Revista Internacional de Investigación e Innovación Tecnológica

Página principal: www.riiit.com.mx

Los retos para proteger los datos del usuario en México

The challenges for protecting user's data in Mexico

Lara-Nino, C.A.[a], Morales-Sandoval, M.[b], Diaz-Pérez. A.[c]

[a] Laboratoire Hubert Curien; Université Jean Monnet, CNRS; C.P. 42000, Saint-Etiene, France.
[b] Unidad Tamaulipas; CINVESTAV; C.P. 87130, Ciudad Victoria, México.
[c] Unidad Guadalajara; CINVESTAV; C.P. 45019, Zapopan, México.
carlos.andres.lara.nino@univ-st-etienne.fr; miguel.morales@cinvestav.mx; adiaz@cinvestav.mx

Innovación tecnológica: Documentación de casos de estudio sobre vulneración de la seguridad de la información de los usuarios en México y su análisis para determinar los principales retos que se deben afrontar en este sentido. Propuesta de soluciones.

Área de aplicación industrial: Seguridad de la información.

Recibido: 06 octubre 2021
Aceptado: 20 enero 2022

Abstract

As users of various information technology services, it is often necessary to provide personal data for different procedures or inquiries. For example, when it comes to requesting a birth certificate, renewing ID, processing the passport, or renewing the driver's license. In addition to providing information to different government agencies as in the previous cases, we also provide personal information to private entities such as when opening a bank account, hiring a telephone service, processing a business benefits card, among others. Providing our personal data has become so usual that it is very common to see micro-businesses that offer the service for the management of official documents obtained through the internet, the above with the consent of the user. Also, it is not out of the ordinary to find copying, scanning, and printing services for documents containing sensitive information that should remain private. There is a mutual understanding that this data belongs only to the user. However, it is increasingly common to see large volumes of personal data being offered for sale on black markets. Clearly, these are illegal activities derived from failures in the data protection mechanisms of the information systems. On the other hand, there are also cases where users, little aware of the risks, directly or indirectly accept terms and conditions to be incorporated into databases that are used for targeted advertising. While this activity is not illegal, its unregulated use has relevant ethical implications. In this document, we review different case studies in order to

identify the vulnerabilities and risks that personal information faces. The risks of using this information for identity theft and why this is important to modern society are also discussed. This work departs from the question: *who protects our information?* Responsibility cannot lie entirely with the government, service providers, or users. However, in this document we focus on users. Because of these recommendations are provided to the reader regarding current privacy policies and government proposals for the handling of our personal information. Behaviors that should be avoided are also emphasized to help preserve the security of personal information.

Keywords: User's information, Mexico, Security, Solutions, Vulnerabilities.

Resumen

Como usuarios, con frecuencia es necesario proporcionar datos personales para diferentes trámites o consultas. Por ejemplo, es lo que generalmente hacemos cuando se trata de solicitar un acta de nacimiento, renovar la credencial de elector, tramitar el pasaporte, o renovar la licencia de conducir. Además de proporcionar información a diferentes organismos gubernamentales como en los casos anteriores, también proporcionamos información personal a entidades particulares como por ejemplo al abrir una cuenta bancaria, contratar un servicio telefónico, tramitar una tarjeta de beneficios comerciales, entre otros. Proporcionar nuestros datos personales es tan usual que es muy común ver micronegocios que ofrecen el servicio para la gestión de documentos oficiales obtenidos mediante internet, lo anterior con el consentimiento del usuario. Asimismo, son comunes los servicios de fotocopiado, escaneo, e impresión de documentos que contienen información sensible y que debería permanecer privada. Hay un entendimiento mutuo de que estos datos pertenecen sólo al usuario. Sin embargo, cada vez es más frecuente ver que grandes volúmenes de datos personales son puestos a la venta en mercados negros. Claramente, éstas son actividades ilícitas derivadas de fallas en los mecanismos de protección de datos que tienen los sistemas de información. Por otra parte, también están los casos en donde usuarios, poco conscientes de los riesgos, de forma directa o indirecta aceptan términos y condiciones para ser incorporados en bases de datos que son usadas para publicidad enfocada. Si bien esta actividad no es ilícita, su uso no regulado tiene implicaciones éticas relevantes. En este documento, hacemos una revisión de diferentes casos de estudio con el objetivo de identificar cuáles son las vulnerabilidades y riesgos que enfrenta la información personal. También se discuten los riesgos que tiene el uso de esta información para el robo de identidad y por qué esto es importante para la sociedad moderna. Este trabajo parte de la pregunta ¿quién protege nuestra información personal recopilada durante la realización de trámites mayormente gubernamentales? Es claro que la responsabilidad no puede recaer totalmente en el gobierno, en los proveedores de servicios, o en los usuarios. Sin embargo, en este documento nos enfocamos en los usuarios. Por ello, se le brindan recomendaciones al lector de cara a las políticas de privacidad actuales y a las propuestas gubernamentales para el manejo de nuestra información personal. Se enfatizan también las conductas que como usuarios debemos evitar para contribuir a preservar la seguridad de muestra información personal.

Palabras clave: Información de usuario, México, Seguridad, Soluciones, Vulnerabilidades.

1. Introducción

En la actualidad, la prevalencia del acceso a internet a través de diversos dispositivos ha facilitado la proliferación de conductas delictivas enfocadas a vulnerar la integridad de las personas en México. Mientras que para algunos las estadísticas pueden evidenciar una carencia del servicio, la realidad es que para el 2016 un 47% de los hogares mexicanos disponía de conexión a internet, 45.6% de los mismos contaba con una computadora, y el 73.6% de los habitantes eran usuarios de telefonía móvil (Martínez Domínguez, 2018). Esto representaba unos 90 millones de puntos de acceso a internet a través de una de las tecnologías de comunicación más vulnerables (Fei y Wang, 2019; Vachhani, 2019). Para enero de 2021, este número se incrementó a 115.4 millones de conexiones móviles, con un total de 92 millones de usuarios de internet (Kemp, 2021). Se ha llegado a mencionar que *"los usuarios publican y comparten más información que en cualquier otro momento de la historia de la humanidad"* (Cortes Martínez, 2016). Así como ha crecido la cobertura de los servicios internet, han aumentado también los ciberdelitos al grado de que para el 2015 México ocupaba el tercer puesto mundial en este rubro (Redacción AN, 2015). En ese momento la suplantación y el robo de identidad ya representaban 68% de los delitos cibernéticos. También de forma alarmante, para 2020 se reportaba a México como el segundo país con más ciberataques en el mundo (Arellano, 2020). Esto indica que no se ha tomado el problema de la protección de los datos personales con seriedad o no se ha hecho lo suficiente para prevenir este tipo de delitos. Un reporte reciente emitido por el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos sobre el estado de la ciberseguridad en América Latina, revela que a pesar de que los usuarios en México tienen un grado de confianza y seguridad en internet *consolidado* para con otros usuarios, gobierno, y sistemas de comercio, su comprensión de la protección de la información personal en línea es apenas *formativa* (Creese, Goldsmith, Weisser Harris, Bund, y Kastelic, 2020). Esto implica que hay carencias en los organismos o en la definición de la problemática. Asimismo, se documenta cómo hay deficiencias en el cumplimiento de los estándares de seguridad de las tecnologías de la información y la comunicación, así como en la calidad del software utilizado para proteger la información. En el mismo sentido, un estudio por la Asociación Mexicana de Internet (AMIPCI, 2017) sobre la protección de datos personales entre usuarios y empresas, documentó como un 81% de las empresas mexicanas almacena algún tipo de dato personal, que pueden incluir datos de identificación (90%), datos patrimoniales (33%), datos de salud (18%), datos biométricos (11%), y otros datos sensibles (9%), mientras que sólo 56% de estas empresas reporta tener conocimiento (44%) o conocimiento pleno (12%) de la legislación vigente para proteger estos datos.

Entre los llamados ciberdelitos podemos identificar aquellos orientados a desarrollar actividades delictivas a través del internet, como pueden ser el comercio ilegal de bienes y servicios, la explotación infantil, trata de personas, y delitos electorales; otros enfocados en defraudar a personas físicas o morales con el fin de obtener recompensas monetarias o en especie; y aquellos cuyo intento es vulnerar la integridad de las personas físicas, como lo son el acoso, la negación de acceso a internet, el robo de información, y en su última instancia la suplantación de identidad. Evidentemente, todos estos agravios tienen consecuencias negativas para la sociedad y es necesario analizarlos a detalle. No obstante, para ser concisos, este trabajo se enfoca en preservar la seguridad de la información de los usuarios con el objetivo final de prevenir el robo o

suplantación de identidad. Según el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, en lo subsecuente), para 2015 México ya ocupaba el octavo lugar mundial y el segundo en América Latina en la comisión de este delito (INAI, 2021). De acuerdo con El Economista, en un 67% de los casos el mecanismo usado por los criminales para cometer el delito estaba asociado con la pérdida de documentos físicos, 63% tenía relación con el robo de carteras y portafolios, y en un 53% de los casos la información era tomada directamente de una tarjeta bancaria (Santa Rita, 2013). Según un estudio de la fecha, se encontró que hasta un 86% de los participantes solía portar la credencial electoral en la cartera, documento que como revisaremos contiene suficiente información para acceder a grandes volúmenes de datos del usuario. En años subsecuentes, este delito pasó del mundo físico al ciberespacio gracias a la disponibilidad de puntos de acceso tanto como para usuarios legítimos como para actores maliciosos. Hoy en día, Forbes califica al robo de identidad digital como el delito de mayor crecimiento en México y en el mundo (Islas Maldonado, 2020).

En la actualidad es frecuente diferenciar entre robo de identidad y robo de identidad digital. No obstante, es necesario aclarar que, a pesar de las diferencias en el mecanismo para la comisión del delito, el objetivo es el mismo. Según el INAI, se define al robo de identidad como *"la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre"*. Lo cual implica, entre otras conductas, *"la obtención y uso no autorizado e ilegal de datos personales"*. En este documento revisaremos cómo mediante diversas técnicas, esta apropiación puede darse mediante medios físicos o digitales. Si bien los métodos difieren, demostraremos cómo el acceso a las tecnologías de la información facilita tanto la obtención de los datos personales como su uso no autorizado. Subsecuentemente, analizaremos las medidas actuales que buscan proteger la información de los usuarios para identificar vulnerabilidades potenciales. Finalmente, se presentan recomendaciones para sociedad y organizaciones con el fin de mitigar los riesgos que fomentan la comisión del robo de identidad.

2. Métodos

Según observaciones de los autores, existen tres factores principales tras el aumento en los casos de robo de identidad en años recientes. El primero está asociado con el incremento en la confianza en las nuevas tecnologías, particularmente los sistemas móviles. El segundo, con la disponibilidad de los datos de usuario en distintos sitios de internet, tanto de origen legítimo como sitios de gobierno como a través de la compra de bases de datos creadas mediante actividades ilícitas. Y tercero, el auge en el uso de documentos digitales para realizar trámites en línea o en persona. Este último factor ha sido exacerbado por las restricciones de movilidad y necesidad de usar recursos digitales, como consecuencia de la pandemia SARS-CoV-2.

Si bien se puede dar el robo de identidad a través de mecanismos convencionales como el robo de documentos físicos a la víctima, estos procesos no se abordan en esta sección para dar cabida a una discusión sobre mecanismos emergentes que, entre otras características, no alertan a la víctima de forma inmediata.

En este documento se presenta una revisión de casos donde se pueden identificar situaciones de riesgo para el usuario, con el fin de identificar conductas que pueden evitarse y deben prevenirse. Esto para mitigar que los datos del usuario puedan llegar a ser utilizados en la comisión de distintos delitos,

entre ellos el robo o suplantación de identidad. Los casos de estudio fueron recuperados a partir de una revisión cuidadosa de distintas fuentes hemerográficas. Para su selección se tomó en cuenta la disponibilidad de detalles concretos, así como la disponibilidad de recursos en línea que permitan respaldar los sucesos descritos. Por ejemplo, si una publicación en un medio de circulación nacional no tenía forma de ser consultada a través de un portal de internet hemos optado por no revisarla en aras de preservar la transparencia de los datos.

2.1 Apropiación ilícita de los datos

A medida que se populariza el uso de teléfonos inteligentes, los usuarios tienen menos reservas respecto al uso de nuevas tecnologías como son las aplicaciones móviles, las redes sociales, y los servicios de comunicación por internet.

En referente a las primeras, no es inusual que se soliciten permisos de acceso al hardware (cámaras, micrófono, ubicación) o al software del dispositivo (contactos, mensajes, llamadas); cuando se hace el uso correcto de estos sistemas es posible crear aplicaciones que ofrecen servicios de mayor calidad, no obstante, puede darse el caso de que la información recopilada se use con fines adversos a los intereses del usuario (Nguyen, McDonald, y Glisson, 2017). Estudios han mostrado que menos del 20% de los usuarios presta suficiente atención a los permisos solicitados al momento de instalar aplicaciones (Felt y cols., 2012).

Las redes sociales son una herramienta de gran utilidad ya que pueden propiciar la distribución oportuna de información emergente (Chan, Nickson, Rudolph, Lee, y Joynt, 2020) y la diseminación del conocimiento (Labinaz y Sabisa, 2021). Asimismo, permiten crear comunidades de usuarios con intereses afines más allá de las limitaciones geográficas (Piselli, 2007). No obstante, estos sistemas traen consigo riesgos dado que se carece de certeza en la información transmitida (Torres, Gerhart, y Negahban, 2018) y la identidad real de los usuarios (Fire, Kagan, Elyashar, y Elovici, 2014). Estos riesgos pueden materializarse en ataques contra la integridad del usuario al propiciar la toma de decisiones basada en información falsa, o ataques contra la privacidad al compartir datos sensibles con usuarios fraudulentos.

En cuanto al uso del internet como medio de comunicación, estudios revelan que apenas un 37% de los usuarios de sistemas móviles hacen uso del correo electrónico de forma habitual (Pacheco, 2018). Esto nos da indicios de que pocos usuarios son conscientes de las actividades delictivas cometidas a través de este servicio, en contraste con la familiaridad respecto a las estafas telefónicas o por mensaje de texto. De este modo, es posible explicar que México ocupe el séptimo lugar a nivel mundial y primero en América Latina en la recepción de correos electrónicos maliciosos (Garduño, 2021). Los objetivos de este tipo de ataques son o bien comprometer el dispositivo de la víctima mediante archivos adjuntos infectados con virus informáticos o llevar al usuario a proporcionar datos personales a través de sitios de internet apócrifos, técnica conocida como *phishing*. Ganar acceso al dispositivo de cómputo puede a su vez tener como metas extraer información confidencial o secuestrar el sistema mediante *ramsonware*. Para incrementar la efectividad de estas estrategias, los atacantes hacen uso de ingeniería social (enfocado a un usuario en particular) y *spoofing*, que buscan hacer pasar correos apócrifos como verdaderos. Cabe mencionar que existen distintos métodos de *spoofing*, pero en este trabajo nos enfocamos en su implementación mediante los servicios de correo electrónico.

Estos mecanismos novedosos para obtener información de los usuarios se suman a las técnicas ya conocidas donde a través de la actividad ilícita, se puede acceder a grandes volúmenes de datos. Tan sólo en 2020, se reportaron 12 incidentes de seguridad en instituciones públicas de México (MILENIO, 2021). Entre las organizaciones afectadas destacaron la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el Banco de México (Banxico), el Servicio de Administración Tributaria (SAT), y la Secretaría de la Función Pública (SFP).

En este último caso se reportó que fueron expuestas las declaraciones patrimoniales de 830 mil servidores públicos (Soto Galindo, 2020). Además de los datos propios de las declaraciones, se expuso información como cuentas bancarias, domicilios particulares, y Claves Únicas de Registro de Población (CURPs). Hemos de hacer notar que este incidente no se suscitó a raíz de un actor malicioso, sino de la deficiencia en los procedimientos de la SFP para salvaguardar los datos, aunado a la falta de visión de la institución que, tras la revelación de los hechos, declaró que la información expuesta *"es de naturaleza pública y forma parte de los trabajos de interconexión con la Plataforma Digital Nacional, los datos que contiene pueden consultarse en el sitio: https://servidorespublicos.gob.mx/*". No obstante, las declaraciones disponibles en el sitio no muestran al público todos los datos expuestos en la filtración de 2020.

Investigaciones subsecuentes por parte del INAI revelaron que en realidad 1.6 millones de servidores públicos se vieron afectados a raíz de este suceso, cifra registrada en el expediente INAI.3S.07.01.005/2020. La actitud de negligencia y encubrimiento por parte de la SFP queda expuesta al revisar el historial del caso. De acuerdo con (Soto Galindo, 2020), fue el analista de seguridad Bob Diachenko quien encontró la base de datos expuesta a través del motor de búsqueda *Sodhan* y alertó a la SFP el 30 de junio de 2020. Para ese entonces los datos llevaban en línea más de un mes, desde el 6 de mayo de 2020. No obstante, como muestra el expediente INAI.3S.07.01.004/2020, a través del comunicado DGTGA/120/109/2020 emitido el 6 de octubre de 2020, la SFP narra cómo "*A pesar de* [las medidas de seguridad de la base de datos], *el incidente ocurrió debido a que un agente externo, utilizando software especializado, detectó una IP pública (200.33.31.87) que respondía a peticiones del protocolo HTTP*" y que "*Posteriormente utilizó conocimiento especializado acerca de la base de datos Elasticsearch para acceder a su contenido*". Si bien este recuento de los hechos no es falso, se hace omisión de las circunstancias bajo las cuales se dio la filtración. Es claro que la SFP ha tratado de verter la responsabilidad en un agente externo cuando en realidad los datos estuvieron abiertos al público por un periodo de tiempo prolongado. Lo más probable es que no se tiene registro de la cantidad de accesos a la información durante este lapso. Además, hasta la fecha no se tiene conocimiento de sanciones imputadas contra algún responsable interno.

Si bien el caso de la filtración de datos en la SFP afecta a un número reducido de mexicanos, existen otros ejemplos donde la cantidad de usuarios perjudicados es mucho mayor. El Instituto Nacional Electoral (INE), antes llamado Instituto Federal Electoral (IFE), es el órgano encargado de conducir los procesos electorales y salvaguardar los datos personales de todos los votantes. Más allá de servir en la elección de representantes populares, la credencial de elector es el documento de identificación por excelencia en México. En su última revisión (Modelo G), este documento contiene a simple vista el nombre del elector, opcionalmente su domicilio, clave de elector, CURP, y fecha de

nacimiento, entre otros. En el anverso, códigos QR con tecnología propietaria del INE resguardan todos estos datos más información privada. Toda la información de los votantes se agrupa en el llamado padrón electoral o lista nominal, un instrumento que es utilizado en el proceso electoral para corroborar la identidad de los electores y la vigencia de sus credenciales. Por mecánicas del proceso, el INE debe otorgar una copia del padrón a cada partido registrado, previo a la realización de una elección. Dada la importancia de estos documentos, se podría esperar que existan candados que impiden la filtración de los datos. No obstante, lo único que separa al padrón electoral del mercado negro es, aparentemente, la buena voluntad de sus custodios.

Desde el 2003, el entonces IFE sufrió la primera filtración de los datos a manos de un actor interno (EL PAÍS, 2003). En esa ocasión, se filtraron los datos de 58 millones de votantes y se cotizaron en 200,000 MXN. Los datos comprometidos incluían nombre, fecha de nacimiento, dirección, y teléfono de los electores. A pesar de identificar al responsable, un ciudadano particular, no se le imputó delito alguno. Versiones actualizadas de este registro fueron subsecuentemente filtradas en 2006, 2010, y dos veces en 2012 (González, 2016). En estos últimos casos, los datos fueron encontrados a la venta en la conocida zona de Tepito por 12,000 USD y 15,000 USD. En 2013 ocurrió de nueva cuenta la filtración de la lista nominal, esta vez a manos del partido político *Convergencia* (hoy *Movimiento Ciudadano*). Como consecuencia de este hecho, el INE sancionó al partido en cuestión por la suma de 76 millones de pesos. La multa fue impugnada y el caso nunca se resolvió al punto de que el partido político responsable, como tal ya no existe. Para ese entonces el número de electores afectados superaba ya los 80 millones. De nueva cuenta, en 2016 se vulneró la privacidad de los datos a manos de un partido político (González, 2016). Los datos fueron encontrados nada menos que en el sitio de almacenamiento de *Amazon*. En esta ocasión el INE ni siquiera se molestó en señalar a los responsables *"para no entorpecer la investigación"*. Nuevamente, en 2018 se dio a conocer que se encontró a la venta el listado nominal de 2015 (INE, 2018). Tan común parecía ya la noticia que no se proporcionaron detalles del caso. A raíz de todos estos eventos se introdujeron mecanismos de control en el proceso de distribución de los datos. Se redujo la cantidad de registros por copia, se acotó la información incluida, y se agregaron huellas digitales para identificar a cada copia. Sin embargo, nada parece desalentar a los actores maliciosos quienes apenas este año lograron de nuevo vulnerar la privacidad de los datos de 91 millones de electores (EL ECONOMISTA, 2021). Para este punto debe resultar evidente que en México la noción de información privada es meramente un espejismo.

Ahora bien, no siempre se trata de procesos complicados mediante los cuales actores maliciosos pueden ganar acceso a nuestra información a cambio de grandes sumas monetarias. En muchas ocasiones, simples aplicaciones de ingeniería social pueden derivar en la vulneración de la privacidad de las y los ciudadanos. Es observación de los autores, que eventos fuera de lo ordinario relajan nuestra percepción sobre conductas fuera de lo ordinario. Tomando como ejemplo la reciente consulta popular concretada en México, es de notarse que un evento de esta naturaleza no es común. Entre el revuelo causado por las diferentes partes, se dio a conocer en la Ciudad de México (CDMX) que supuestos promotores del voto pedían información personal, tan sólo a unos metros del Palacio Nacional, la ahora sede del poder ejecutivo en México (Villa y Caña, 2021). Se reporta que los supuestos funcionarios, además de las firmas de los transeúntes,

solicitaban claves de elector, sección electoral, números telefónicos, nombres, y direcciones con el argumento de que "*son firmas que está pidiendo el INE previo al día de la consulta*". Esto apenas a dos días de esa fecha. A muchos les parecería extraño este proceso, mientras que otros serían indudablemente estafados. Sin embargo, a todos nos queda la duda sobre quién está realmente tras estas actividades. No es posible discernir si se trata de un intento oficial por inflar las urnas, o simplemente de criminales ultrajando de sus datos a personas vulnerables. Cuando las conductas delictivas se dan en frente de la autoridad, simplemente no se puede argumentar entre una alternativa o la otra.

Otro ejemplo se suscitó a raíz de la pandemia por coronavirus y la campaña de vacunación implementada por el gobierno mexicano. Al 20 de agosto de 2021 se reportaba que EE. UU. había aplicado 360 millones de dosis, con un 51% de su población completamente vacunada (Holder, 2021). Alemania, el líder en la Unión Europea en este rubro, contaba ya con 99 millones de dosis aplicadas, con un 59% de su población inmunizada. Para ese entonces México reportaba la aplicación de 79 millones de dosis, lo que representaba apenas el 24% de la población teniendo el esquema completo. A partir de esta diferencia en las tasas de vacunación, diferentes países llegaron a establecer restricciones para los viajeros que llegaban de México y no contaban con un esquema de vacunación completo (sin mencionar que no todas las vacunas que han sido aplicadas en México son reconocidas en el extranjero). Esto generó que algunos ciudadanos se vieran en la necesidad de obtener un certificado de vacunación completo para viajar al extranjero, a pesar de que no había campañas de vacunación a la vista. De la demanda nace la oferta. Para octubre de 2021 se reportaba ya que en la plaza de Santo Domingo de la CDMX era posible encontrar quienes ofrecen la emisión de certificados de vacunación apócrifos por tan solo 600 MXN (Vargas, 2021). Más allá de la naturaleza ilícita de estas transacciones, hay detalles relevantes para el tema que se aborda en este trabajo. Se ha detallado que a quienes están interesados se les solicitan datos como nombre, edad, dirección, CURP, dirección correo electrónico, e incluso cuentas bancarias, toda vez que un certificado de vacunación auténtico sólo incluye la CURP, el nombre de la persona, así como las fechas de aplicación, marcas, y lotes de las vacunas recibidas. Evidentemente nos encontramos ante una operación delictiva que tiene dos objetivos: primero lucrar con la emisión de documentos falsos, delito por el cual el gobierno mexicano sanciona tanto a la parte emisora como a la solicitante, y segundo, apoderarse de la información personal de objetivos potenciales para el robo de identidad.

El robo de identidad se puede dar ya sea por oportunidad, al contar con la información de una víctima potencial, o premeditado, al buscar obtener la información de una víctima en específico. En meses recientes se han reportado diversos casos donde políticos mexicanos prominentes han sufrido del robo de identidad a través de los sistemas de telefonía móvil (EXPANSIÓN política, 2021). En estas instancias se han hecho uso de mecanismos no divulgados para apoderarse de las cuentas de *WhatsApp* de las personas afectadas. A través de esta aplicación se enviaron mensajes a otras víctimas solicitando la transferencia de recursos económicos a cuentas de particulares. Lo interesante del caso, es que, a pesar de la sofisticación del delito, al momento de solicitar las transferencias bancarias los actores maliciosos sin mayor reserva proporcionaron a las víctimas nombres y números de cuenta bancaria. Resta averiguar si estos datos fueron a la vez robados de otras víctimas. Es indudable que resulta complicado esclarecer esquemas

complejos donde un actor malicioso puede hacer uso de la identidad de múltiples personas para cometer una cadena de delitos. Esto refleja la importancia de comprender las diferentes fuentes mediante las cuales se pueden obtener los datos de usuario.

Mas allá de aquellas instancias donde terceros buscan obtener los datos de los usuarios por distintos motivos, en México se han documentado también casos donde se presume que los perpetradores son aquellos quienes deberían protegernos (García Argueta, 2021). En años recientes, el famoso caso *Pegasus* ha levantado polémica con relación al uso de tecnologías de espionaje por parte del gobierno mexicano contra sus ciudadanos. Entre 2015 y 2017, diferentes actores de la sociedad civil, periodistas, e investigadores, fueron el blanco de una campaña para infectar sus dispositivos móviles mediante el envío de un mensaje de texto. No resulta claro en cuantos casos el ataque se desarrolló de manera exitosa, pero los indicios apuntan a que provenían del gobierno federal vigente en ese entonces. El software espía *Pegasus* fue desarrollado por la empresa israelí *NSO Group* como una herramienta para brindar *"tecnologías que permiten a los gobiernos autorizados combatir el terrorismo y el crimen*" (Pegg y Cutler, 2021). Una vez instalado en un dispositivo móvil, permite al atacante acceder a los mensajes y fotografías del dispositivo, acceder a la ubicación y activar las cámaras o micrófonos para grabar a la víctima, todo esto de forma secreta. Inicialmente, se requería que el objetivo hiciera clic en un enlace malicioso para instalar el programa malicioso. Sin embargo, se han reportado casos donde mediante vulnerabilidades del sistema operativo es posible infectar distintos dispositivos sin la intervención del usuario. Claramente, estamos ante una pieza de tecnología que puede resultar conveniente si se usa de forma adecuada, pero qué pasa cuando se malversa su función. ¿Podría una actualización de la legislatura vigente, con el fin de regular el uso de herramientas como *Pegasus*, mitigar el riesgo de que sean usadas con malas intenciones?

2.2 El uso no autorizado de los datos

Una vez analizados diversos mecanismos mediante los cuales un atacante puede apoderarse de información sensible para el usuario, podemos proceder con la discusión sobre qué fin pueden llegar a tener estos datos, cómo pueden beneficiar a los actores maliciosos y qué tanta información es en realidad necesaria para apoderarse de la identidad de una persona en México.

Gracias a la modernización de la infraestructura de gobierno, hoy en día es posible realizar diversos trámites a través del internet ante distintas dependencias. Esto reduce tiempos de espera y traslados innecesarios de personas. Uno de los servicios más utilizados es la consulta de la CURP a través del sitio www.gob.mx/curp. Esta plataforma permite realizar la búsqueda de cualquier CURP utilizando ya sea la cadena del documento, o algunos datos del usuario. En el segundo caso, solo se requiere el nombre de la persona, su primer apellido, fecha de nacimiento, sexo y estado de nacimiento. Suponiendo que una persona no autorizada tratase de recuperar la CURP de una persona en particular, si contara con su nombre y primer apellido, podría hacer algunas estimaciones sobre su edad, sexo y estado de nacimiento. Sólo serían necesarios 366 intentos por año para explorar todas las posibles fechas de nacimiento. En 24 horas sería posible explorar casi 4 años de registros, suponiendo una tasa de una consulta por minuto dado el uso de *captchas*. Una vez que se tiene acceso al documento, el atacante gana acceso a la CURP, el nombre completo de la persona, la entidad de nacimiento, registro y el municipio de registro.

Otro de los servicios disponibles en las páginas del gobierno es la expedición de actas de nacimiento a través de la plataforma www.gob.mx/ActaNacimiento. Del mismo modo que con el caso de la CURP, se requiere o bien ese dato o información personal para realizar la búsqueda. El escenario hipotético que planteamos para la búsqueda exhaustiva de la CURP también se puede aplicar para obtener el acta de nacimiento de una persona. En caso de encontrar un registro, además se debe proporcionar el nombre de uno de los padres, por lo que llevar a cabo primero la búsqueda exhaustiva de la CURP puede resultar más atractivo para un actor malicioso. Para obtener el acta es necesario realizar un pago por el servicio que puede hacerse en línea o mediante un formato bancario. Dado que el pago en línea dejaría algún indicio de la consulta, presumimos que el formato bancario es más factible para un actor malicioso. Dependiendo de la entidad federativa de registro, se requieren algunos datos para generar estos formatos de pago, pero en la mayoría de los casos los datos son opcionales o no se validan por lo que de nuevo se puede usar información ilegítima.

Si se tiene conocimiento del domicilio de la persona de interés, es posible ganar acceso a información como número de RFC, reportes de crédito y número de seguridad social (para inscritos al IMSS). Todo esto desde la comodidad de un escritorio. Si un actor malicioso realmente tratara de conseguir los datos de una persona podría usar esta información obtenida a través de medios oficiales para generar documentos apócrifos. Idealmente, se presume que buscaría ganar acceso a un documento de identidad, por ejemplo, la credencial para votar. El INE solicita tres documentos de identidad para quienes estén interesados en tramitar este documento: acta de nacimiento, identificación con fotografía y comprobante de domicilio. El caso del acta de nacimiento ya se ha abordado, los comprobantes de domicilio se pueden obtener sin mayor problema dada la práctica de las empresas paraestatales de dejar los recibos de pago a plena vista en el domicilio. En cuanto a la identificación con fotografía, el INE admite documentos de escuelas públicas o privadas con un máximo de 10 años de haber sido expedidos. En la plaza de Santo Domingo, CDMX es posible encontrar quienes ofrecen tales documentos por tan solo 4,000 MXN (Mendoza, 2016). Si se quiere suplantar la identidad de alguien sólo resta que el actor malicioso consiga un actor de rasgos similares a la víctima. Dado que las credenciales de elector tienen una vigencia de 10 años, esto no resulta sumamente complicado. Aún más, como se ha reportado en (Silva-Peña, 2021), los mecanismos usualmente utilizados para verificar la autenticidad de estos documentos son poco eficaces y prones a error. Alternativamente, falsificar el Modelo G de la credencial de elector tiene un costo de tan sólo 1,800 MXN y requiere apenas 24 horas de espera (Colín, 2018). Como punto de referencia, al INE le toma una semana emitir este documento de forma legítima.

A pesar de que algunos de estos ataques no pueden ser aplicados a grandes volúmenes de usuarios, dado que se requiere un grado elevado de ingeniería social y búsqueda de información, su severidad puede llegar a ser mayor que otros esquemas donde lo que se busca es simplemente la información. En este sentido, el robo de datos de objetivos específicos pudiera asemejarse al secuestro pues no se busca tener muchas víctimas sino algunos objetivos de interés.

2.3 El uso no ético de los datos

Los ejemplos propuestos hasta ahora muestran algunas conductas delictivas que son sancionadas por la autoridad con penas económicas e incluso encarcelamiento. No obstante, los datos de usuario pueden ser

usados con fines no éticos que escapan el rigor de la ley. En estos casos se engaña u orienta al usuario para ceder su información de manera voluntaria y autorizar su uso con fines generalmente comerciales.

En la experiencia de los autores, uno de estos casos se presenta al tiempo de abrir cuentas bancarias. Cuando se firman los contratos con las distintas cláusulas, los bancos suelen incluir secciones dedicadas a la autorización del uso de los datos para fines comerciales. Esto generalmente es usar los patrones financieros de los clientes para ofrecerle productos y servicios. Normalmente, un cliente puede rechazar firmar estas secciones del contrato con lo que sus datos quedan resguardados ante tales prácticas, en principio. Sin embargo, hace apenas unos años se presentó el caso con *BBVA Bancomer*, donde modernizaron el sistema de forma de contratos y ahora todo se realiza mediante una terminal electrónica. Al momento de la firma del acuerdo de uso de los datos para fines comerciales, la aplicación simplemente no permitía proceder sin que el cliente accediera a firmar esta sección, o por lo menos eso expresaban los ejecutivos del banco en cuestión. En cualquiera de los casos, o se está forzando al cliente a ceder el acceso a los datos con tal de entrar en un acuerdo comercial con el banco, o simplemente se le está engañando.
A finales del 2020 la filial española de este banco, *BBVA*, recibió una sanción de 5 millones EUR por hacer uso no autorizado de los datos de sus clientes con fines publicitarios (Pérez, 2020). Mientras que en México se desconoce si esta práctica sigue vigente, pero no ha sido causante de sanciones.

Las empresas detrás de distintas redes sociales también se han visto involucradas en escenarios donde recopilan información de los usuarios y la venden a distintas empresas con el fin de crear campañas de publicidad enfocada. Entre los infractores resalta *Facebook* que ha recibido sanciones por 1.2 millones EUR en España (Fernández, 2017), 5,000 millones USD en EE. UU. (FTC, 2019) y 7 millones EUR en Italia (EFE, 2021). Con anterioridad, esta empresa ya se había visto involucrada en polémicas relacionadas con el tratamiento ético de los datos. Entre 2013 y 2016, la empresa británica *Cambridge Analytica* empleó esta red social para recolectar información de millones de usuarios y utilizarla en campañas políticas, entre ellas, la elección de Donald Trump como presidente de EE. UU. en 2016. Según reportes (EL PAÍS, 2018), esta empresa habría conducido operaciones también en México, más nunca se dieron a conocer detalles o se llevó a cabo una investigación al respecto.

Otra conducta que se presta para hacer un uso no ético de los datos del usuario es mediante la instalación de *cookies*. Estos son archivos que las páginas web pueden almacenar en el navegador del usuario como un registro de eventos. Diversos países han implementado regulaciones orientadas a regular el tipo de datos que se pueden recolectar y su uso. Por ejemplo, en sitios con base en la Unión Europea los usuarios deben previamente aceptar el uso de estas *cookies*. Por infringir sus propias regulaciones en este sentido, en 2020 el gobierno francés impuso multas a *Google* por 100 millones EUR (CNIL, 2020) y *Amazon* por 35 millones EUR (Schechner, 2020). En México las páginas web deben informar a los usuarios sobre la recolección de datos, más no se les obliga a pedir una autorización previa.

3. Discusión

En esta Sección presentamos una revisión actual de los mecanismos que permiten garantizar la seguridad de los datos de usuario en México. Se busca con ello profundizar en el discurso sobre el estado de la

infraestructura gubernamental disponible para esta tarea y proponer recomendaciones tanto para el gobierno como para los ciudadanos de forma que puedan tener conciencia sobre la relevancia de esta información y las consecuencias de su uso indebido.

La legislación principal en materia de protección de datos en México es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), promulgada el 5 de julio de 2010. En ese documento se detallan los procedimientos mediante los cuales se puede acceder a la información del usuario, procesarla y resguardarla, así como sanciones para quienes incumplan con lo estipulado.

Según esta Ley, el principal requisito para que un particular pueda recopilar y hacer uso de datos de usuario es presentar un aviso de privacidad, que es un documento donde se identifica al responsable de recabar los datos, la finalidad de su tratamiento, las opciones y medios para limitar su uso o divulgación, medios para ejercer los derechos de acceso, rectificación, cancelación, u oposición del uso de los datos, en su caso la transferencia y los mecanismos mediante los cuales se reportaran los cambios en el aviso de privacidad. La mayoría de las y los mexicanos tendrá alguna memoria de enlaces en distintos sitios con la leyenda "*Consulte nuestro aviso de privacidad*," dado que ésta es la estrategia preferida para notificar a los usuarios de que sus datos están siendo recopilados con alguna finalidad. Sin embargo, ¿cuántas personas realmente se toman el tiempo de leer estos documentos? En este tema, la Ley establece que quien recopila los datos debe permitir al usuario solicitar que éstos no sean usados o almacenados, es decir, el espíritu de la Ley no es en realidad proteger al usuario, sino reglamentar el uso de los datos personales.

Para ejemplificar las deficiencias en este sistema, basta con revisar el aviso de privacidad proporcionado al consultar un recibo de la Comisión Federal de Electricidad (CFE) a través de su portal de internet. Primero, se debe notar que para consultar este documento es necesario proporcionar el nombre y número del servicio, un teléfono fijo y un correo electrónico. En este punto debe causar cierto asombro que se soliciten medios de contacto, toda vez que el documento se emite inmediatamente a través de la plataforma. Al revisar el aviso de privacidad, salta a la vista que uno de los motivos expresos para el uso de datos es "*Para las gestiones de Cobranza*" además de "*Promover los productos y servicios que ofrecemos*" y "*Publicidad*". El primer caso se entiende hasta cierto punto, pero realmente no tiene sentido que una empresa paraestatal sin competencia haga campañas publicitarias u ofrezca algún servicio nuevo a sus clientes. Los datos que se declaran a utilizar son nombre completo, RFC, CURP, domicilio, teléfonos, correo electrónico, datos de identificación, datos de contacto. Note cómo algunos de estos datos no mantienen relación alguna con los datos proporcionados al realizar la consulta de la base de datos. Finalmente, CFE notifica a los usuarios que comparten los datos personales *dentro y fuera del país* con diferentes personas y organizaciones, entre las que destacan:

- Instituciones de crédito en México, para realizar el cobro de servicios con tarjeta bancaria.
- *Antad*, "*Apps*," y "*aplicaciones informáticas*" en México "*para realizar la gestión de cobranza y abrir más canales de pago para la atención de los clientes*".
- "*Gestores de cobranza*" en México, "*para realizar la gestión de cobro en clientes con adeudos*".

En efecto, la CFE está facultada para compartir nuestros datos con instituciones de crédito, tiendas, aplicaciones y gestores de cobranza. Luego, a pesar de los fines declarados, la LFPDPPP faculta a estas instituciones para usar nuestros datos con los usos estipulados en el aviso de privacidad emitido por la CFE (Artículo 36). De este modo, instituciones de crédito, tiendas, aplicaciones y gestores de cobranza, no sólo tienen acceso a nuestros datos, sino que pueden utilizarlos para "*Promover los productos y servicios que ofrecemos*" y "*Publicidad*" de forma legal.

Por datos personales, la Ley define a "*cualquier información concerniente a una persona física identificada o identificable*". Esto deja ver vacíos adicionales en potencia. Primero, es posible argumentar que toda persona es identificable si se cuenta con suficientes datos disponibles (Hauk, 2021). Además, como se evidencia en el mismo reporte, se podría discutir que los datos no conciernen a una persona física, sino a un ordenador que es propiedad de la persona. Este tipo de definiciones que carecen de precisión pueden dar pie a la defensa de actividades ilícitas.

A pesar de que el Artículo 8 de la Ley requiere el consentimiento del titular de los datos para su tratamiento, se declaran excepciones que pueden dar pie a vacíos legales. Primero, se entiende que hay un consentimiento expreso cuando la voluntad del usuario se manifieste "*verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos*". Aquí de nuevo basta con recurrir a la memoria de aquellos sitios en internet con la leyenda "*Al permanecer en esta página acepta nuestros términos y condiciones*". Realmente no hay un requerimiento estricto de que los terceros soliciten de forma expresa el consentimiento del usuario para recopilar y procesar sus datos. El mismo Artículo estipula "*Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición*". De nuevo, se entiende que los terceros tienen derecho a recopilar y tratar la información del usuario a menos que éste a) consulte el aviso de privacidad y b) siga los mecanismos definidos para manifestar su oposición.

El Artículo 10 de la LFPDPPP menciona que "*no será necesario el consentimiento para el tratamiento de los datos personales cuando: […] Los datos figuren en fuentes de acceso público*", las cuales están definidas como "*Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación*". Esto da entrada a vacíos adicionales. Recordemos el caso de la consulta de una CURP, estos documentos forman parte de una base de datos pública, según lo estipulado en la Ley. No obstante, para consultar la base de datos es necesario utilizar información privada del usuario. Pero de acuerdo con lo reglamentado, una vez que el usuario proporciona estos datos a un tercero, está por defecto proporcionando acceso a todos sus datos disponibles en otras bases de datos públicas. La realidad es que la disposición actual no beneficia en absoluto al usuario, sino que faculta a terceros para hacer uso de información adicional que puede entrar dentro de los vacíos legales.

El Artículo 63 de la misma Ley identifica las infracciones que se le pueden atribuir al responsable del manejo de los datos. Se contemplan entre otros:

- *No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;*

- *Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;*
- *Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;*
- *Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;*
- *Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;*

Según el Artículo 64, son atribuibles de sanciones económicas de 100 a 160,000 días de salario mínimo. Así como también:

- *Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;*
- *Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;*
- *Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;*
- *Recabar datos en forma engañosa y fraudulenta;*
- *Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.*

Infracciones que se castigan con multas que van de los 200 a 320,000 días de salario mínimo. En cuanto a responsabilidades penales, se consideran delitos en materia del tratamiento indebido de datos personales:

- *Artículo 67.- Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.*
- *Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.*

La Ley es suficientemente clara en materia de sanciones, sin embargo, existe el componente de impunidad generalizado en México. Como hemos documentado, en la mayoría de los casos no se encuentran culpables o se imputan sanciones a los responsables.

El segundo componente de interés en cuanto a legislación vigente está relacionado con el robo de identidad, que puede llegar a considerarse como el caso extremo en el uso no autorizado de los datos personales. Actualmente, el Código Penal Federal no tipifica al robo o suplantación de identidad como delito. No obstante, los estados de Baja California, Baja California Sur, Colima, Chihuahua, Ciudad de México, Durango, Guanajuato, Jalisco, Estado de México, Nuevo León, Oaxaca, Quintana Roo, Sinaloa, Tamaulipas, Tlaxcala y Zacatecas si tienen definiciones en esta materia y sancionan la comisión del delito. Es de resaltarse, sólo el 50% de las entidades federativas están facultadas para intervenir en el caso donde se suplante la identidad de sus ciudadanos.

En 2018, se presentó en el Senado una iniciativa con proyecto de decreto para adicionar un capítulo denominado Robo de Identidad al Código Penal Federal. Este proyecto contempla como definición: "*Comete el delito de robo de identidad el que adquiera por cualquier medio, información personal y financiera, con la intención de suplantar la identidad de un tercero, con el*

fin de cometer conductas ofensivas, obtener recursos monetarios o beneficios financieros a su favor, o cometer cualquier otro delito". Y busca aplicar sanciones a los responsables con penas de nueve años de prisión y de setecientos días de multa. Sin embargo, tres años después, el acuerdo aún se encuentra pendiente de dictamen por la Cámara de Senadores. Contar con esta legislación es de suma importancia para cubrir la totalidad del territorio nacional y homogeneizar las definiciones y sanciones en la materia.

4. Conclusiones

En este documento se ha presentado un amplio estudio de casos referentes a situaciones de riesgo para la seguridad de los datos personales de los usuarios en México. Se ha puesto énfasis en el análisis de los mecanismos emergentes mediante los cuales actores maliciosos pueden ganar acceso a la información. Subsecuentemente, se han discutido los usos delictivos que estos actores pueden dar a los datos de usuario. Finalmente, se ha realizado una revisión del marco legal vigente y las áreas de oportunidad existentes.

Como conclusión, es necesario presentar recomendaciones para los usuarios de modo que puedan proteger sus datos ante un escenario de riesgo creciente donde por un lado los procesos delictivos son cada vez más sofisticados y por el otro la legislación queda rebasada a medida que surgen nuevas tecnologías. Es necesario considerar:

- Evitar proporcionar datos personales a través de sitios de internet o medios electrónicos a menos que sean absolutamente necesarios.
- Evitar exponer documentos con información sensible a través de basura, correspondencia no atendida, servicios de papelería, entre otros.
- Evitar hacer uso de plataformas digitales que carecen de autenticidad, así como aplicaciones móviles que solicitan acceso a servicios que realmente no necesitan.
- Conocer los derechos con los que goza el usuario ante las políticas de recolección y tratamiento de los datos por terceros, así como los medios de revocación de autorización.

Para las autoridades, podemos recomendar también la toma de decisiones orientada a mejorar el estado de protección de los datos de la ciudadanía. Es importante cambiar de paradigma y priorizar la seguridad de los individuos sobre los intereses de las corporaciones:

- Revisar las políticas actuales en cuanto a la recolección, tratamiento, y uso de los datos a través de las tecnologías digitales, de manera que se dé prioridad a la protección de los datos y se requiera no sólo un *clic*, sino el pleno acuerdo de la persona para hacer uso de su información.
- Tipificar la alteración y uso indebido de datos personales como delito a nivel federal, así como designar la emisión y uso de documentos apócrifos con la misma severidad que delitos como la falsificación de moneda.
- Definir la identidad digital como un derecho inalienable de los ciudadanos, de manera que se puedan establecer derechos y obligaciones relacionados con el uso de los sistemas de información. Esto de cara a un mundo cada vez más integrado con el ciberespacio.

Otras recomendaciones que pueden tomarse en cuenta, según (EL ECONOMISTA, 2020), incluyen protecciones físicas como mantener seguros los documentos que almacenamos en nuestras casas, proteger nuestra correspondencia, limitar el número de documentos personales con los que nos

desplazamos cotidianamente, y revisar nuestros estados financieros con regularidad. Así como también protecciones al hacer uso del internet como evitar el uso de computadoras públicas, cambiar regularmente nuestras contraseñas, y borrar los datos del navegador al terminar una sesión.

En años recientes, el uso de herramientas digitales para coadyuvar en la protección de los datos de usuario se ha incrementado. Esto puede tener una explicación en el crecimiento exponencial del volumen de datos. Simplemente no es razonable la expectativa de que una persona por organización pueda hacerse cargo del diseño y manejo de políticas de seguridad. Algunos ejemplos de tales herramientas son *SisVal* para verificar la autenticidad de credenciales de elector (Silva-Peña, 2021), *FAD* (https://fad.firmaautografa.com) y *DocuSign* (https://www.docusign.com) que permiten verificar la autenticidad de firmas electrónicas, y *VeriDoc* (https://sumamexico.com/en/veridocid/) que permite auditar la autenticidad de diversos documentos oficiales. Estas nuevas herramientas pueden contribuir significativamente a reducir el indicie de delitos más es necesario que puedan ser auditadas para verificar su correcto funcionamiento.

Finalmente, a pesar de la necesidad de actualizar tanto la legislación como la tecnología para brindar mayores protecciones a los ciudadanos, también hay que reconocer la necesidad de concientizar a los usuarios sobre la importancia de resguardar sus datos y sobre las potenciales consecuencias que conlleva su mal uso. Hoy en día, cuando nos vemos rodeados de medios digitales pareciera que la tecnología nos ha rebasado. Por ello es necesario permanecer vigilantes ante las distintas amenazas que se nos pueden presentar.

5. Referencias

Martínez Domínguez, M. (2018). “Acceso y uso de tecnologías de la información y comunicación en México: factores determinantes”. *Paakat: Revista de Tecnología y Sociedad*, 8(14), 1-18. doi: 10.32870/Pk.a8n14.316

Fei, T., y Wang, W. (2019). *LTE is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks*. En 2019 IEEE Global Communications Conference (p.1-6). doi: 10.1109/GLOBECOM38437.2019.9013397

Vachhani, K. (2019). *Security Threats Against LTE Networks: A Survey*. En S. M. Thampi, S. Madria, G. Wang, D. B. Rawat, y J. M. Alcaraz Calero (Eds.), Security in computing and communications (pp. 242-256). Singapore: Springer Singapore.

Kemp, S. (2021, 9 de feb.). *Digital 2021: Mexico*. DataReportal - Global Digital Insights. Disponible en https://datareportal.com/reports/digital-2021-mexico

Cortez Martínez, F., Herrera Candelaria, A.D., Ramírez Lozano, M.A., Rodríguez Zúñiga, A.R. Martínez Peláez, R., y Parra Michel, J.R. (2016). “Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México”. *Revista lbérica de Sistemas y Tecnologías de Información* (21) 115-128. doi: 10.17013/risti.21.115–128

Redacción AN. (2015, 24 de jul.). *México tercer lugar mundial en ciberdelitos; China y Sudáfrica lo superan*. Aristegui noticias. Disponible en https://aristeguinoticias.com/2407/mexico/mexico-tercer-lugar-mundial-en-ciberdelitos-china-y-sudafrica-lo-superan/

Arellano, S. (2020, 9 de oct.). *México, segundo país con más ciberataques en el mundo*. MILENIO. Disponible en https://www.milenio.com/politica/comunidad/mexico-es-el-segundo-pais-con-mas-ciberataques-en-el-mundo

Creese, S., Goldsmith, M., Weisser-Harris, C., Bund, J., y Kastelic, A. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe* (Reporte no. 1). Washington, D.C. USA: BID/OEA/University of Oxford.

AMIPCI (2017, 8 de ago.). *Estudio de Protección de Datos Personales entre Usuarios y Empresas*. Disponible en https://www.asociaciondeinternet.org.mx/es/component/remository/Proteccion-de-Datos-Personales

INAI. (2021). *Datos de interés*. Micrositio sobre robo de identidad. Disponible en https://micrositios.inai.org.mx/identidadsegura/?pageid=45

Santa Rita, I. (2013, 7 de feb.). *Evite llevar toda su identidad en la cartera*. EL ECONOMISTA. Disponible en https://www.eleconomista.com.mx/finanzaspersonales/Evite-llevar-toda-su-identidad-en-la-cartera-20130207-0024.html

Islas Maldonado, G. (2020, 10 de jun.). *El robo de identidad digital en México*. Forbes. Disponible en https://www.forbes.com.mx/el-robo-de-identidad-digital-en-mexico/

Nguyen, T., McDonald, J. T., y Glisson, W. B. (2017). *Exploitation and Detection of a Malicious Mobile Application*. En T. Bui (Ed.), Proceedings of the 50th Hawaii International Conference on System Sciences (pp. 6181-6190). Hawaii, USA: AIS Electronic Library (AISeL). doi: 10.24251/HICSS.2017.747

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., y Wagner, D. (2012). *Android Permissions: User Attention, Comprehension, and Behavior*. En L. Faith Cranor (Ed.), Proceedings of the Eighth Symposium on Usable Privacy and Security. New York, USA: Association for Computing Machinery. doi: 10.1145/2335356.2335360

Chan, A. K. M., Nickson, C. P., Rudolph, J. W., Lee, A., y Joynt, G. M. (2020). "Social media for rapid knowledge dissemination: early experience from the COVID-19 pandemic". *Anaesthesia*, 75(12), 1579-1582. doi: 10.1111/anae.15057

Labinaz, P., y Sabisa, M. (2021). *Speech acts and the dissemination of knowledge in social networks*. En C. Xie, F. Yus, y H. Haberland (Eds.), Approaches to Internet Pragmatics: Theory and Practice (pp. 145-174). Amsterdam, Netherlands: John Benjamins Publishing Company. doi: 10.1075/pbns.318.05lab

Piselli, F. (2007). "Communities, places, and social networks". *American Behavioral Scientist*, 50 (7), 867{878. doi: 10.1177/0002764206298312

Torres, R., Gerhart, N., y Negahban, A. (2018). *Combating Fake News: An Investigation of Information Verification Behaviors on Social Networking Sites*. En T. Bui (Ed.), Proceedings of the 51st Hawaii International Conference on System Sciences (pp. 3976-3985). Hawaii, USA: AIS Electronic Library (AISeL). doi: 10.24251/HICSS.2018.499

Fire, M., Kagan, D., Elyashar, A., y Elovici, Y. (2014). "Friend or foe? Fake profile identification in online social networks". *Social Network Analysis and Mining*, 4 (194). doi: 10.1007/s13278-014-0194-4

Pacheco, M. (2018, 23 de feb.). *El 89% de las personas con internet en México lo usan principalmente para WhatsApp*. Xataka México. Disponible en https://www.xataka.com.mx/servicios/el-89-de-las-personas-con-internet-en-mexico-lo-usan-principalmente-para-whatsapp

Garduño, M. (2021, 24 de feb.). *México es el séptimo país a nivel mundial amenazado por correos maliciosos*. Forbes. Disponible en https://www.forbes.com.mx/tecnologia-mexico-septimo-pais-correos-maliciosos/

MILENIO. (2021, 19 de jul.). *Crimen organizado vulnera seguridad de datos personales en internet: INAI*. Disponible en https://www.milenio.com/politica/inai-crimen-organizado-vulnera-datos-personales-internet

Soto Galindo, J. (2020, 4 de jul.). *Función Pública expuso la declaración patrimonial de 830,000 funcionarios públicos*. EL ECONOMISTA. Disponible en https://www.eleconomista.com.mx/politica/Funcion-Publica-expuso-la-declaracion-patrimonial-de-830000-funcionarios-publicos-20200704-0009.html

EL PAÍS. (2003, 20 de may.). *Un ladrón roba el padrón de México y se lo vende a una empresa de EE UU por 16.500 euros*. Disponible en https://elpais.com/internacional/2003/05/20/actualidad/1053381607_850215.html

González, M. E. (2016, 23 de abr.). *Roban padrón electoral; lo "subieron" a Amazon*. El Sol de México. Disponible en https://www.elsoldemexico.com.mx/mexico/Roban-padr%C3%B3n-electoral-lo-%E2%80%9Csubieron%E2%80%9D-a-Amazon-170547.html

INE. (2018, 7 de oct.). *INE interpone denuncia por uso indebido de la Lista Nominal; aseguran base de datos y se impide su comercialización*. Central Electoral. Disponible en https://centralelectoral.ine.mx/2018/10/07/ine-interpone-denuncia-uso-indebido-la-lista-nominal-aseguran-base-datos-se-impide-comercializacion/

EL ECONOMISTA. (2021, 19 de jul.). *INE investiga presunta venta de datos del Padrón Electoral*. Disponible en https://www.eleconomista.com.mx/politica/INE-investiga-presunta-venta-de-datos-del-Padron-Electoral-20210719-0082.html

Vargas, M. (2021, 8 de ago.). *Robo de identidad, el precio por un certificado falso de vacunación en CDMX*. Publimetro. Disponible en https://www.publimetro.com.mx/mx/noticias/2021/08/08/robo-de-identidad-el-precio-por-un-certificado-falso-de-vacunacion-en-cdmx.html

Villa y Caña, P. (2021, 25 de jul.). *Piden información personal promotores de consulta popular*. EL UNIVERSAL. Disponible en https://www.eluniversal.com.mx/nacion/piden-informacion-personal-promotores-de-consulta-popular

Holder, J. (2021, 20 de ago.). *Tracking Coronavirus Vaccinations Around the World*. The New York Times. Disponible en https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html

EXPANSION política. (2021, 2 de ago.). *Zavala, Anaya y Cordero denuncian el hackeo de sus cuentas de WhatsApp*. Disponible en https://politica.expansion.mx/mexico/2021/08/02/zavala-anaya-y-cordero-denuncian-el-hackeo-de-sus-cuentas-de-whatsapp

García Argueta, I. (2021). *Caso Pegasus: El espionaje en México*. Centro de Investigación

y Docencia Económicas (CIDE). Tesis de licenciatura. Disponible en http://repositorio-digital.cide.edu/bitstream/handle/11651/4493/TESIS_IGA.pdf

Pegg, D. y Cutler, S. (2021, 18 de jul.). *What is Pegasus spyware and how does it hack phones?* The Guardian. Disponible en https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

Mendoza, A. (2016, 21 de ago.). *Puede venir Peña y nosotros le sacamos su título*. VICE. Disponible en https://www.vice.com/es/article/7byz4a/puede-venir-pena-y-nosotros-le-sacamos-su-titulo-0000305-v7n1

Silva-Peña, A.V., Aviña-Luna, J.C., Meléndez-Sánchez, U., Rodríguez-González, L., Muñoz-González, E.D., Parra-Michel, J.R., y Martínez-Peláez, R. (2021). "SisVal: prototipo de sistema de validación de identidad para trámites personales en México". *Revista Internacional de Investigación e Innovación Tecnológica* 52(9), 32-49.

Colín, B. (2018, 3 de sept.). *Licencias, INE, tarjetones... todos falsos y en una hora, por $1,600*. CRONICA. Disponible en https://www.cronica.com.mx/notas/2018/1092592.html

Pérez, E. (2020, 15 de dic.). *La Agencia de Protección de Datos se pone seria: multa récord al BBVA de 5 millones de euros por el uso de datos sin consentimiento*. Xataka. Disponible en https://www.xataka.com/legislacion-y-derechos/agencia-proteccion-datos-se-pone-seria-multa-record-al-bbva-5-millones-euros-uso-datos-consentimiento

Fernández, Y. (2017, 12 de sept.). *Multa de 1,2 millones de euros a Facebook: Protección de Datos carga contra sus perfiles en la sombra*. Xataka. Disponible en https://www.xataka.com/servicios/multa-de-1-2-millones-de-euros-a-facebook-proteccion-de-datos-carga-contra-sus-perfiles-en-la-sombra

EFE. (2021, 17 de feb.). *Multa Italia a Facebook con 7 mde por uso indebido de datos*. MILENIO. Disponible en https://www.milenio.com/negocios/multa-italia-facebook-7-mde-indebido-datos

FTC. (2019, 24 de jul.). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Press release. Disponible en https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

EL PAÍS. (2018, 21 de mar.). *La huella mexicana de Cambridge Analytica*. Disponible en https://elpais.com/internacional/2018/03/21/mexico/1521592636_991451.html

CNIL. (2020, 10 de dic.). *Cookies: sanction de 60 millions d'euros à l'encontre de GOOGLE LLC et de 40 millions d'euros à l'encontre de GOOGLE IRELAND LIMITED*. Press release. Disponible en https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-google-llc-et-de-40-millions-deuros-lencontre-de

Schechner, S. (2020, 10 de dec.). *Google, Amazon Fined $163 Million as France Takes Hard Line on Privacy*. The Wall Street Journal. Disponible en https://www.wsj.com/articles/google-amazon-fined-163-million-as-france-takes-hard-line-on-privacy-11607601278

Hauk, C. (2021, 27 de jul.). *Browser Fingerprinting: What Is It and What Should You Do About It?* Pixelprivacy. Disponible en

https://pixelprivacy.com/resources/browser-fingerprinting/

EL ECONOMISTA. (2020, 13 de oct.). *Manténgase seguro y evite el robo de identidad*. Disponible en https://www.eleconomista.com.mx/finanzaspersonales/Mantengase-seguro-y-evite-el-robo-de-identidad-20201013-0090.html