El que suscribe, **Gustavo Madero Muñoz**, Senador de la República por el Estado de Chihuahua e integrante del Grupo Parlamentario del Partido Acción Nacional, en la LXIV Legislatura del H. Congreso de la Unión con fundamento en lo dispuesto por los artículos 71, fracción II y 72 de la Constitución Política de los Estados Unidos Mexicanos; por los artículos 116, 121, 122 y demás relativos de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, así como por los artículos 55, fracción II, 56 y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someto a la consideración de esta Honorable Asamblea la presente **iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de delitos cibernéticos**, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

El progreso de la sociedad se ha dado gracias, en cierta medida, al avance tecnológico, el cual sin duda forma parte del establecimiento de una política de desarrollo. Se dice entonces, que las nuevas oportunidades de desarrollo pueden ir atadas a los avances tecnológicos que se despliegan por las llamadas revoluciones industriales, las cuales pueden ser consideradas como aquellas que implican un cambio profundo que acelera el ritmo de transformación de la sociedad.[1]

En ese sentido, la historia de la humanidad ha atravesado por más de una revolución industrial o tecnológica, que ha cambiado aspectos como la forma en la que se desarrolla la industria, el transporte y la comunicación, la obtención de energía, la localización y el empleo. Cada uno de estos procesos ha traído consigo grandes invenciones que van desde la maquina de vapor, el tren, los motores de combustión interna y la producción de

[1] INSTITUTO de Energías Renovables, UNAM. El proceso de industrialización: concepto. https://www.ier.unam.mx/~rbb/ERyS2013-1/industrializacion.pdf. Consultado el 02 de febrero de 2021.

automóviles, la producción en serie, la radio y televisión, hasta microelectrónica, la informática y la biotecnología, entre otros.[2]

En ese sentido, el avance tecnológico cambia la forma en la que las economías producen, pero también, modifica y transforma la manera en la que las personas desarrollan sus actividades diarias o laborales, dada la introducción de nuevas tecnologías. Podemos decir que la evolución tecnológica es un proceso complejo, pues cada vez más las tecnologías e innovaciones están interconectadas entre si, generando toda una red con el entorno físico, social e institucional.[3]

Por tanto, la tecnología e innovación no se desarrolla de forma aislada, sino en interdependencia con otras, aprovechando la experiencia y la presencia de proveedores y consumidores, lo que se traduce en una capacidad social para su uso.[4] Hoy en día el mundo ha cambiado, ahora los avances e innovación tecnológica se presentan cada vez de forma más rápida.

En la actualidad, el mundo se encuentra inmerso en una cuarta revolución industrial, la cual ha dado pie al surgimiento de la llamada industria 4.0, a nuevos materiales y software, a la interconexión e interacción de sistemas, la transformación en los modelos de producción y trabajo, el diseño de nuevos productos y servicios, así como la automatización y digitalización de los procesos en un todo integrado. Este nuevo avance tecnológico presupone un cambio estructural y progresivo, principalmente en áreas como la informática y las telecomunicaciones.

Esta nueva etapa contempla la implementación de nuevas herramientas como internet móvil de alta velocidad, el internet de las cosas (IoT), la inteligencia artificial, el machine learning, la realidad aumentada, el análisis

---

[2] INSTITUTO Geográfico Nacional, Ministerio de Fomento del Gobierno de España. Las revoluciones industriales. Consultado el 03 de febrero de 2021.

[3] PÉREZ, Carlota; CEPAL. Cambio tecnológico y oportunidades de desarrollo como blanco móvil. Página 4. https://www.cepal.org/prensa/noticias/comunicados/8/7598/CarlotaPerez.pdf. Consultado el 02 de febrero de 2021; Weller, Jürgen; Gontero, Sonia; Campbell, Susanna; CEPAL. Cambio tecnológico y empleo: una perspectiva latinoamericana. Página 9. https://repositorio.cepal.org/bitstream/handle/11362/44637/1/S1900367_es.pdf. Consultado el 02 de febrero de 2021.

[4] *Op. Cit.* PÉREZ, Carlota; CEPAL. Cambio tecnológico y… Página 6.

y manejo de grandes cantidades de datos (Big Data), la masificación de tecnologías como el blockchain y el cómputo en la nube, la hiperconectividad, entre otras.[5]

Lo anterior, ha permitido una verdadera evolución en el desarrollo e implementación de las Tecnologías de la Información y Comunicación (TICs), por lo que nos encontramos en una época de constante digitalización, donde las personas no solo interactúan con dispositivos como computadoras, celulares y tabletas electrónicas, con fines como la comunicación, obtención de información o la elaboración de documentos, sino, para cumplir con otro tipo de objetivos como una interconexión global, es decir, estar en contacto con personas de otra parte de México o del mundo, no importando la hora o el día, o bien para la elaboración de trámites que requieran de una identificación personal a través del uso de elementos biométricos o firmas electrónicas.

Este avance tecnológico ha permitido modificar la forma en la que se desarrollan nuestras actividades, que como ya mencionamos, no solo se queda en el ámbito nacional, sino pasa a ser un ámbito global. Ahora, estos dispositivos como computadoras o smartphones, son capaces de procesar un gran número de información, pero sobre todo, de albergar plataformas digitales o aplicaciones que facilitan la prestación de servicios como las redes sociales y el entretenimiento, de tal forma que todo se puede hacer en cuestión de minutos.

Un ejemplo de lo anterior es el comercio digital, el cual tiene sus orígenes en el comercio tradicional y los principios de economía clásica como lo son la oferta y la demanda, pero con la posibilidad de realizarse a través de la red y no necesariamente en espacios físicos. Por otro lado, organismos como las instituciones financieras también han adoptado mecanismos para la facilitación de operaciones a través de la red; los usuarios de este tipo de servicios, pueden acceder, desde su computadora o teléfono celular, a

[5] CENTRO de Estudios Sociales y de Opinión Pública; Cámara de Diputados. La industria 4.0: el nuevo paradigma productivo del siglo XXI. Páginas 3 y 4. http://www5.diputados.gob.mx/index.php/esl/content/download/167115/834348/file/CESOP-IL-72-14-Industria4.0-251119.pdf. Consultado el 03 de febrero de 2021; CEPAL. La revolución industrial 4.0 y el advenimiento de una logística 4.0. Página 2. https://repositorio.cepal.org/bitstream/handle/11362/45454/1/S2000009_es.pdf. Consultado

sitios o aplicaciones que les permiten tener, en tiempo real, la información referente a sus cuentas bancarias, realizar operaciones o movimientos, pagos, así como transferencias electrónicas interbancarias.

En 2019, se estimó que México contaba con una población total de 124 millones de personas (actualmente la población total es de 126 millones de mujeres y hombres de todas las edades[6]), de las cuales, alrededor de 113 millones (87.4 millones en zona urbana y 25.6 millones en zona rural) contaron con una edad de 6 años o más, de las cuales el 66% de la población, tuvo acceso a internet, mientras que 62% hace uso de teléfonos inteligentes (smartphones) y el 12% hace uso de telefonía convencional. Las principales actividades realizadas a través de internet son: redes sociales, contenidos audiovisuales gratuitos y de paga, compras y ventas por internet, así como operaciones bancarias.[7]

Sin duda, lo anterior ha generado un incremento en el flujo de información personal, económica, política, social y cultural dentro de la red. Si bien todo esto representa una oportunidad de desarrollo y la facilitación en la oferta y demanda de servicios por parte de los agentes económicos, también se enfrentan retos a cumplir que tienen que ver con la prevención y protección de actos que puedan afectar los intereses de los usuarios de internet.

Es tal la importancia de estos avances en materia digital y sobre todo, en la prevención y protección de los usuarios de estas herramientas contra delitos cibernéticos, que existen tratados internacionales en materia de ciberseguridad, como por ejemplo el Convenio sobre Ciberdelincuencia o Convenio de Budapest que ha sentado las bases para el tratamiento contra las prácticas que vulneran los intereses y derechos de los usuarios de medios digitales.[8] Así como el Reglamento Relativo a la Agencia de la Unión Europea para la Ciberseguridad.

---

[6] INEGI. Población Total. https://www.inegi.org.mx/temas/estructura/. Consultado el 03 de febrero de 2021.

[7] *Op. Cit.* INSTITUTO Federal de Telecomunicaciones. Uso de las TIC y… Páginas 16 y 17.

[8] BIBLIOTECA del Congreso Nacional de Chile. Convenio sobre ciberdelincuencia: convenio de Budapest. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf. Consultado el 02 de febrero de 2021.

Si bien México no se ha adherido al convenio de Budapest, si cuenta con instrumentos internacionales, tal como el Tratado entre México, Estados Unidos y Canadá (T-MEC), que comprometen a nuestra nación a implementar medidas de ciberseguridad.

El Capítulo 19 "Comercio Digital" del T-MEC, reconoce la importancia de esta modalidad del comercio para el crecimiento y desarrollo de los Estados miembro, por ello, busca que los países implementen medidas para evitar obstáculos innecesarios para su implementación, pero también, para la generación en la confianza de los usuarios respecto del entorno digital. Por ello, a lo largo del articulado de este capítulo, se cuenta con disposiciones en materia de transacciones electrónicas, autenticación y firmas electrónicas, protección al consumidor en línea, protección de información personal, principios obre acceso y uso del internet para comercio digital, así como en materia de ciberseguridad, entre otras.[9]

En el artículo 19.15 "Ciberseguridad" del capítulo mencionado en el párrafo anterior, se reconoce que las amenazas a la ciberseguridad menoscaban la confianza de los usuarios de medios digitales, por ello, esta disposición busca que los Estados parte desarrollen las capacidades para la respuesta a incidentes de ciberseguridad, así como, fortalezcan los mecanismos de cooperación en materia de identificación y mitigación de intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad, así como para el intercambio de información para el conocimiento y las mejores prácticas.[10]

Cabe señalar que, de acuerdo con la Unión Internacional de Telecomunicaciones, se puede considerar a la Ciberseguridad como[11]:

---

[9] SECRETARÍA de Economía; Gobierno de México. Textos finales del T-MEC; Capítulo 19 "Comercio Digital". https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf. Consultado el 02 de febrero de 2021.

[10] SECRETARÍA de Economía; Gobierno de México. Textos finales del T-MEC; Capítulo 19…

[11] UNIÓN Internacional de Telecomunicaciones. Aspectos generales de la ciberseguridad (versión en español). Página3. https://www.itu.int/rec/T-REC-X.1205-200804-I/es. Consultado el 03 de febrero de 2021.

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios[12] *en el ciberentorno…*

En ese sentido, la ciberseguridad debe garantizar las propiedades de seguridad contra los riesgos correspondientes al entorno digital.

Por su parte, la ciberseguridad también puede ser considerada como[13]:

…el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos…

Por otro lado, se debe mencionar que México ya ha incursionado en temas de ciberseguridad, a través de la Estrategia Nacional de Ciberseguridad, cuyo objetivo se ha centrado en identificar y establecer las acciones aplicables en la materia en el ámbito social, económico y político, de tal manera que la población y organizaciones públicas y privadas, puedan gozar del uso y aprovechamiento responsable de las Tecnologías de la Información y Comunicación. Por lo tanto, con estas medidas, se han considerado a cinco objetivos estratégicos: sociedad y derechos; economía e innovación; instituciones públicas; seguridad pública, y seguridad nacional[14].

---

[12] Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

[13] AMERICAN Chamber Mexico. Estrategia de Ciberseguridad en México: por un futuro ciberseguro. Página 2. https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20(1).pdf. Consultado el 02 de febrero de 2021.

[14] GOBIERNO de México. Estrategia Nacional de Ciberseguridad. Página 3. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf. Consultado el 02 de febrero de 2021.

Hoy en día, esta realidad del uso de la tecnología digital se hace más presente, por ejemplo, con la situación que se vive por la propagación del virus SARS-CoV2 (COVID-19).

Como es bien conocido, la pandemia por COVID-19 ha provocado que los diferentes países implementen medidas para la mitigación de los efectos generados. En México se puso en marcha la jornada de "sana distancia", la suspensión de eventos masivos y el cierre de negocios no esenciales. Con ello, la vida cambió, potencializando el uso de plataformas digitales para el desarrollo de actividades como la compra y venta de bienes o servicios, operaciones bancarias, entretenimiento, la educación y empleo.

De acuerdo con la CEPAL, las tecnologías digitales han sido esenciales para el funcionamiento económico y social durante la crisis que se está enfrentando. La concurrencia de población en tiendas de alimentos y farmacias disminuyó un 51%, gracias a la existencia de aplicaciones donde los usuarios pueden hacer sus pedidos y recibirlos en casa; así mismo, la concurrencia en establecimientos de productos no esenciales y de esparcimiento se redujo cerca de un 75%.[15]

Por otro lado, de acuerdo con este organismo internacional, entre el primer y segundo trimestre de 2020, la soluciones para el teletrabajo y la educación a distancia incrementaron en 324% y 60% respectivamente, esto gracias a la implementación de plataformas de videoconferencias.[16] Además, se estima que durante el segundo trimestre de 2020, el uso de aplicaciones de compra en México incrementó en 90%, mientras que el consumo de plataformas de entreteniendo (streaming) incrementó en un 32%, el uso de redes sociales en 42% y el uso de aplicaciones fintech creció en 50%.[17]

---

[15] CEPAL. Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19. Página 1. https://repositorio.cepal.org/bitstream/handle/11362/45938/4/S2000550_es.pdf. Consultado el 04 de febrero de 2021.

[16] *Op. Cit.* CEPAL. Universalizar el acceso a las tecnologías…

[17] FORBES. En tres meses aumentó 90% el uso de aplicaciones de compras en México. https://www.forbes.com.mx/tecnologia-3-meses-aumento-90-uso-apps-de-compras-mexico/; Statista. Variación porcentual del consumo de plataformas de streaming durante la cuarentena por el coronavirus en países seleccionados a fecha de marzo de 2020. https://es.statista.com/estadisticas/1108893/covid-19-aumento-del-uso-de-plataformas-de-

Con todo esto, se vislumbra y reitera la importancia de la implementación de políticas de ciberseguridad que salvaguarden los derechos, privacidad y propiedad de los usuarios del entorno digital y que a su vez incremente la confianza en la implementación de plataformas digitales y aplicaciones.

No obstante lo anterior, nuestro país no ha continuado con una estrategia intergral de ciberseguridad, desafortunadamente el Plan Nacional de Desarrollo 2019-2024 no contiene referencias sobre la importancia de impulsar una estrategia nacional de ciberseguirdad, la única referencia al respecto, se encuentra en Apartado 3. Economía, línea 7: "*Cobertura de Internet para todo el país. Mediante la instalación de Internet inalámbrico en todo el país se ofrecerá a toda la población conexión en carreteras, plazas públicas, centros de salud , hospitales, escuelas y espacios comunitarios . Será fundamental para combatir la marginación y la pobreza y para la integración de las zonas deprimidas a las actividades productivas*."

De acuerdo con la literatura, México ha mostrado tener un buen modelo de madurez de la capacidad de ciberseguridad, la cual se divide en 5 dimensiones: a) política y estrategia de ciberseguridad; b)) cultura cibernética y sociedad; c) educación, capacitación y habilidades en ciberseguridad; d) marcos legales y regulatorios; y e) estándares, organizaciones y tecnologías.[18]

Como se ha mencionado anteriormente, el Convenio sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y que entro en vigor el 01 de julio de 2004, es el primer tratado internacional que busca abordar los delitos informáticos y de Internet para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones. Es decir, es el primer instrumento multilateral jurídicamente vinculante para regular el ciberdelito.

---

streaming-por-pais/; El Financiero. COVID-19 le da un 'subidón' de 42% al uso de las redes sociales: Nielsen IBOPE. https://www.elfinanciero.com.mx/economia/covid-19-le-da-un-subidon-de-42-al-uso-de-las-redes-sociales-nielsen-ibope, y Forbes. Las aplicaciones de fintech crecen 50% en México y 20% a nivel mundial. https://www.forbes.com.mx/tecnologia-fintech-apps-mexico-crecimiento/. Consultado el 04 de febrero de 2021.

[18] FORO Jurídico. El estatus de México y el Convenio de ciberdelincuencia de Budapest. https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

Este convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos como la búsqueda de redes informáticas y la interceptación. Su principal objetivo, establecido en el preámbulo, es aplicar una política penal común destinada a la protección de la sociedad contra el ciberdelito, especialmente mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

En el caso de México, de acuerdo al artículo 1 de la Constitución Federal (CPEUM), todas las personas gozarán de los derechos humanos reconocidas en la misma y en los tratados internacionales de los que el Estado Mexicano sea parte, y en el mismo sentido el artículo 133 dicta que la Constitución, leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República con aprobación del Senado, serán la Ley Suprema.

Actualmente México se encuentra como observador del Convenio de Budapest y de manera formal ha sido invitado a ascender y adherirse a al mismo. Este convenio de Budapest, a pesar de ser un vehículo internacional vinculante, debe estudiarse también desde su naturaleza, ya que la teoría estipula que existen tratados internacionales autoejecutables, en inglés *self-executing*, y no autoejecutables, en inglés non *self-executing*; los primeros son aquellos que su aplicabilidad puede ser sin necesidad de medidas normativas posteriores, o sea de transformación en los ordenamientos legales locales, pues estos pueden aplicarse de manera inmediata y directa desde que cuente con eficacia en el país y que claramente el tratado entre en vigencia, puede ser susceptible de pedirse su ejecución en los temas de justicia. En segundo término, tenemos los no autoejecutables, que al igual que los autoejecutables, cuentan con el procedimiento de ratificación, aprobación, publicación respetando su debida entrada en vigor del tratado, pero que no otorgan un derecho exigible de inmediato, se requiere la adopción o modificación de leyes y disposiciones a nivel nacional que complementen y desarrollen por medio de un actuar legislativo y

reglamentario para que así estos tratados sean de efecto obligatorio. El Convenio sobre la Ciberdelincuencia de Budapest de 2001 en su artículo 2 infiere que este convenio no se ejecuta por sí mismo, toda vez que menciona los siguiente:

> *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".*

En conclusión, actualmente 65 estados son miembros del Convenio de Budapest, incluso algunos de Latinoamérica y el Caribe como Colombia, Costa Rica, Panamá, República Dominicana, Perú, Paraguay, Chile y Argentina. México se encuentra como observador pero no se ha adherido, empero lamentablemente México ha tenido poca reacción de ratificación ante los instrumentos internacionales, tal es el caso del Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales aperturado desde el año 1981, y que México recientemente lo ratificó hasta el 28 de junio de 2018.

La urgencia de un marco regulatorio, que tipifique, persiga y sancione las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red, responde al incremento que estos delitos han tenido durante la pandemia. Casos como uso indebido de la información, ya sea sensible o privilegiada, intrusiones en equipos, redes, sistemas, nubes, sitios web, ataques en redes sociales, son denuncias que constantemente registran los sectores públicos y privados.

Hay que recordar que México es el segundo país con más intentos de ciberataques a negocios, esto según cifras correspondientes a América Latina dadas a conocer por la empresa de ciberseguridad Kaspersky[19]. La

[19] EL Universal. México el segundo país con más ciberataques a negocios. https://www.eluniversal.com.mx/techbit/mexico-es-el-segundo-pais-con-mas-ciberataques-negocios-kaspersky

empresa señala que, durante los primeros nueve meses del 2020, se registraron más de 37.2 millones de intentos de ataques contra negocios. De ellos, 56.25% se registraron en Brasil; 22.81%, en México; 10.20%, en Colombia; 4.22%, en Perú; 3.27%, en Chile y 3.25% en Argentina.

Con relación a usuarios de hogar, la empresa dijo que en lo que va del año han registrado 20.5 millones de ataques en la región. De ellos, 55.97% fueron en Brasil; 27.86%, en México; 7.33%, en Colombia; 5.36%, en Perú; 1.87%, en Argentina y; 1.62%, en Chile. La organización acotó que los ciberdelincuentes están usando temas de la pandemia para vulnerar, por ejemplo, herramientas de acceso remoto y así acceder y recolectar datos bancarios que, incluso, pueden burlar tokens y la doble autenticación establecida por los bancos.

Durante 2020, varias empresas que realizan operaciones en México fueron blanco de diversos ciberataques, por ejemplo, los clientes de la fintech mexicana *Yo Te Presto* (1.4 millones al momento del incidente) vieron expuestos sus correos electrónicos gracias a un acceso no autorizado a los sistemas de la compañía. De acuerdo con el director de esta empresa de financiamiento colectivo, la vulneración no afectó la información personal de sus usuarios, debido a que sólo se había difundido su correo electrónico, y que tampoco habían sufrido afectaciones financieras en sus cuentas dentro de la institución.

A finales de octubre de 2020, los datos de 4.7 millones de usuarios de la *fintech Clip* fueron puestos en venta en un foro en internet. Los datos incluían correo electrónico y número telefónico de los usuarios de la fintech, información que se solicita cuando una persona paga mediante la terminal creada por esta compañía fintech con el fin de recibir un recibo. La respuesta de la compañía ante este incidente fue que los datos expuestos no contenían información financiera de sus clientes ni usuarios y que continuaría trabajando con las autoridades correspondientes sobre este tema[20].

[20] EL Economista. 2020, en 12 hackeos o incidentes de ciberseguridad en México. https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

También en julio se reveló que dos servidores de Gentera, holding financiera mexicana dueña de empresas como Compartamos Banco, Compartamos Financiera, Compartamos SA, Yastás, Aterna y Fiinlab, estaban abiertos sin ninguna protección en internet. La compañía de ciberseguridad que hizo este descubrimiento, aseguró haber verificado 140,000 registros de clientes del banco, los cuales incluían nombres de las cuentas de usuario, nombres completos, correos electrónicos, sexo, fecha de nacimiento, CURP, RFC, dirección y teléfono, estaban alojados en estos dos servidores. Gentera aseguró que los datos eran muestras falsas o dummies que habían sido utilizadas por su laboratorio de investigación financiera Fiinlab y que la información de sus clientes no había sido comprometida.

Pero no solamente, el sector privado es vulnerable a los ataques cibernéticos instituciones públicas también fueron blaco de ciberataques e incidentes de seguridad que en muchos casos pusieron en riesgo o en franca vulnerabilidad la información de cientos de miles de personas. La mayoría de las veces, los afectados por la vulneración de datos personales poco pueden hacer para proteger su información.

Entre el 5 y el 11 de julio, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el Banco de México (Banxico) y el Sistema de Administración Tributaria (SAT) sufrieron afectaciones en sus respectivas páginas de internet. La más afectada fue la Condusef, cuyo portal se vio completamente intervenido por varias horas por los ciberatacantes. Tanto Banxico como el SAT apenas vivieron intermitencias debido a la robustez de sus sistemas de seguridad.

Entre mayo y junio de 2020, la Secretaría de la Función Pública sufrió un incidente de seguridad que expuso las declaraciones patrimoniales de 830,000 funcionarios públicos, una cifra que representa a más de la mitad de los empleados de la Administración Pública Federal. La información vulnerada contenía las claves de identificación fiscal (RFC) y de registro de población (CURP), además del sexo de los funcionarios afectados.

Ante lo ocurrido el INAI, determinó en noviembre de 2020 que la SFP había fallado al no proteger la confidencialidad y la seguridad de los datos, además de vulnerar varios principios establecidos en la ley mexicana de

datos personales, esto pese a que la secretaría de Estado reservó como clasificados por un año los detalles de esta vulneración.

De la misma forma, datos sensibles de al menos 551 asegurados del ISSSTE estuvieron expuestos en internet sin ningún tipo de protección durante un lapso que permanece indeterminado. Los primeros enlaces a estos informes de procedimientos de pacientes del ISSSTE aparecieron en los principales buscadores de internet (Google, Bing y Yahoo) en abril de 2020. Los datos revelados en estos informes incluían el nombre completo, sexo y edad de los pacientes, pero sobre todo datos sensibles, como el diagnóstico que recibió cada uno y el procedimiento quirúrgico al que fue sometido; además de datos personales de los médicos que atendieron a estos pacientes.

En México, el costo de un hackeo en 2018 fue de 2.5 millones de pesos, sin embargo, en 2019 esta cifra alcanzó los 6.5 millones de pesos, de acuerdo cifras de la empresa de ciberseguridad Sophos. De conformididad con la empresa uno de los vectores de ataque con mayor éxito recientemente en México son las vulneraciones por ransomware y por phishing. Datos de la compañía ESET revelan que si bien entre 2017 y 2019 se redujo 50% la cantidad de ataques de ransomware en México, de 12.53% a 9.29%, los que han tomado como blanco al país han tenido más éxito, como el ciberataque a Pemex, sucedido en noviembre de 2019.

Asimismo, de acuerdo con expertos en ciberseguridad de MIT Analytics en Cambridge Massachusetts, nuestro país se encuentra muy rezagado en el área de ciberseguridad, por lo que en la "deep web" y "dark web" se vende la información de tarjetas de crédito y robo de identidad. Se destaca que con la pandemia de COVID-19, los fraudes y robos de información clasificada mediante ciberataques se han incrementado de forma exponencial hasta en un 9 mil por ciento en México.

Con la pandemia por COVID-19, aumentó no sólo el uso de dispositivos electrónicos con el teletrabajo, sino, consecuentemente, los ciberataques, ya que los empleados, al trabajar desde sus hogares, son más susceptibles de ser hackeados, porque no cuentan con las barreras de protección que sí tienen en las oficinas de sus empresas.

Por todo lo anterior, se puede concluir que los delitos informáticos o cibernéticos, son un objetivo prioritario en las agendas de diversos países y un pilar fundamental para custodiar las economías digitales, por lo que la legislación debe encontrar el equlibrio entre y garantizar el despliegue de la tecnología para un funcionamiento correcto, sin llegar a violar los derechos fundamentales como la libertad de expresión y autodeterminación informativa, pero persiguiendo y sancionando las conductas delictivas descritas con anterioridad.

En nuestro país, la piedra angular del andamiaje jurídico en materia de delitos informáticos surgió tras la reforma del 17 de mayo de 1999, la cual adicionaba en el Código Penal Federal el capítulo Acceso ilícito a sistemas y equipos de informática, comprendida de los artículos 211 bis 1 al 211 bis 7. Desde ese momento se han perfeccionado tal catálogo de delitos con reformas del 24 junio de 2009, y 17 junio de 2016. No obstante, es necesario establecer tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea, por lo que la presente iniciativa tiene como finalidad establecer y actualizar el catálogo de delitos cibernéticos, los cuales son conductas que se cometen en Internet tales como la infiltración en los sistemas de información para alterar la información, dañarla, eliminarla, obstaculizar su acceso, que puede o no implicar una extorción.

Por lo anteriormente expuesto, someto a la consideración de esta Soberanía la siguiente Iniciativa con proyecto de:

DECRETO POR EL QUE SE REFORMA Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE DELITOS CIBERNÉTICOS.

Artículo Único. – Se reforman los artículos 211 bis 1 a 211 bis 7 y se adicionan los artículos 211 bis 8 a 211 bis 13 del Código Penal Federal, en materia de delitos cibernéticos, para quedar como sigue:

CAPITULO II
Acceso ilícito a sistemas y equipos de informática.

Artículo 211 bis 1.- Para los efectos de este capítulo se entenderá por:

I. Ciberseguridad: toda acción tendiente a proteger las redes de telecomunicaciones, redes públicas de telecomunicaciones y sistemas de información, de los usuarios de tales sistemas, sean públicos o privados, afectadas por las ciberamenazas;

II. Ciberamenaza: cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar las redes de telecomunicaciones, redes públicas de telecomunicaciones y los sistemas de información, a los usuarios de tales sistemas;

III. Ciberataque: cualquier acto u omisión cuyo objetivo sea infiltrar, sin autorización, redes de telecomunicaciones, redes públicas de telecomunicaciones, sistemas de información o equipos informáticos;

IV. Internet: lo que establece el artículo 3, fracción XXXII de la Ley Federal de Telecomunicaciones y Radiodifusión;

V. Redes de telecomunicaciones: lo que establece el artículo 3, fracción LVII de la Ley Federal de Telecomunicaciones y Radiodifusión;

VI. Redes públicas de telecomunicaciones: lo que establece el artículo 3, fracción LVIII de la Ley Federal de Telecomunicaciones y Radiodifusión, y

VII. Sistema de información: todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.

Artículo 211 bis 2.- Comete el delito de ciberataque quien realice actos tendientes a acceder de manera ilegítima, vulnerar, inhabilitar, robar información, intervenir, destruir o afectar redes de telecomunicaciones, redes públicas de telecomunicaciones y sistemas de información, a quien se le impondrán de ocho a doce años de prisión y multa que hasta tres mil veces la unidad de medida y actualización vigente al momento de la realización de la conducta.

Artículo 211 bis 3.- A quien, sin derecho, acceda, intervenga u obstaculice total o parcialmente los servicios prestados por internet, se le impondrán de diez a quince años de prisión y multa hasta de tres mil veces la unidad de medida y actualización vigentes al momento de la realización de la conducta.

Artículo 211 bis 4.- A quien, sin autorización, obtenga datos o información referente al tráfico de datos, actividad en internet o mensajes digitales del titular del equipo o de algún otro usuario autorizado por este a utilizarlo, se le impondrán de tres a siete años de prisión y una multa hasta mil veces la unidad de medida y actualización.

Artículo 211 bis 5.- Comete el delito de ciberamenaza quien, sin autorización ni derecho, acceda a un sistema informático con el fin de copiar, modifique, limitar el acceso, corrompa o destruya datos o información contenida en dicho sistema o realice exija al titular de la información dar, hacer o no hacer algo para permitir el acceso a dicho dato o sistema. Quien comenta el delito descrito en el presente artículo, se le impondrán de seis a ocho años de prisión y multa hasta mil veces la unidad de medida y actualización.

Artículo 211 bis 6.- Comete el delito de ciberataque quien, sin autorización infiltre de forma masiva redes de telecomunicaciones, redes públicas de telecomunicaciones o sistemas informáticos con la finalidad de obstaculizar los servicios prestados en internet. Quien cometa el delito descrito en el presente artículo, se le impondrá de diez a doce años de prisión y multa de mil quinientas veces la unidad de medida y actualización.

Artículo 211 bis 7.- Comete el delito de robo de identidad el que adquiera, por cualquier medio, información personal y financiera, con la intención de suplantar a un tercero, con el fin de cometer conductas ofensivas, obtener recursos monetarios o beneficios financieros a su favor, o cometer cualquier otro delito, dicha conducta se castigará de cinco a diez años de prisión y multa hasta ochocientas veces la unidad de medida y actualización.

Artículo 211 bis 8.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 9.- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución

e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 10.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 11.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 12.- Para los efectos de los artículos **211 Bis 10 y 211 Bis 11** anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 13.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno**, o la realice un servidor público**.

TRANSITORIO

ÚNICO. – El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Dado en la Ciudad de México a dieciséis días del mes de febrero de dos mil veintiuno.

SEN. GUSTAVO MADERO MUÑOZ