INICIATIVA QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL, DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y LA LEY DE INSTITUCIONES DE CRÉDITO, SUSCRITA POR LA DIPUTADA ROCÍO ESMERALDA REZA GALLEGOS Y LEGISLADORES INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PAN.

La que suscribe, Rocío Esmeralda Reza Gallegos, y los integrantes del Grupo Parlamentario del Partido Acción Nacional en la LXV Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72, inciso h), de la Constitución Política de los Estados Unidos Mexicanos, así como 6, numeral 1, inciso I, 77, numeral 1, 78 y 102, numeral 2, del Reglamento de la Cámara de Diputados, presentan ante esta soberanía iniciativa con proyecto de decreto que reforma y adiciona diversas disposiciones al Código Penal Federal, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de la Ley de Instituciones de Crédito, a fin de incrementar las sanciones por la comisión de delitos informáticos y cibernéticos, en particular el secuestro de información o acceso ilícito a sistemas y equipos de informática, al tenor de la siguiente

Exposición de Motivos

I . Durante los últimos años, el país ha enfrentado un aumento sin precedentes en los índices delictivos relacionados con ciberataques y amenazas cibernéticas, a grado tal que, en 2021, 74 por ciento de las empresas afirmó haber sido víctima de secuestro de datos.[1] En el sector público, son mundialmente conocidas las lamentables y vergonzosas situaciones por las que han pasado diversas instituciones, órganos y entidades del gobierno mexicano, debido a las constantes intervenciones a sus sistemas informáticos con el propósito de secuestrar información por parte de personas o grupos delictivos expertos en cibernética. Dependencias como el propio Ejército Mexicano, la CFE, Pemex, y hasta la Lotería Nacional, entre muchas, algunas de las cuales se consideran sectores estratégicos al estar definidos dentro de la normativa de protección como infraestructuras críticasdel Estado, y que, por ende, deben tener o contar con sistemas de ciberseguridad de vanguardia.

Por otra parte, el trabajo en casa durante la pandemia disparó el número de ciberataques hacia las empresas, las instituciones gubernamentales y educativas, tanto como a las personas. La Dirección General Científica de la Guardia Nacional indica que de septiembre de 2020 a abril de 2022 atendió 34 mil reportes ciudadanos en materia de ciberseguridad, principalmente relacionados con secuestro de datos bancarios, institucionales o personales.[2]

Los ataques más recurrentes durante la pandemia del Covid-19 fueron las infecciones por código malicioso, virus o *ransomware,* por los que los hackers secuestran información de los dispositivos o de las redes a las que están conectados, por una cantidad de dinero para que el usuario pueda recuperar tal información, aunque en realidad es muy poco probable rescatarla. En el caso de las personas, ha sido común que el ciberataque sea hacia sus cuentas bancarias, su correo electrónico o las cuentas de redes sociales.

II. Los ciberatacantes están un paso adelante y pueden acercarse a las y los usuarios mediante páginas falsas, llamadas telefónicas para solicitar datos o enviando correos electrónicos apócrifos de alguna empresa para confundir a las y los empleados. Entre más

grande sean las instituciones resultan más atractivas para este tipo de ataques. Las empresas pequeñas son más susceptibles a sufrir ciberataques debido a que no cuentan con sistemas de seguridad informática, y los hackers pueden acceder a la información y pedir recompensa económica.

Por supuesto, dicho fenómeno, dada su gravedad y trascendencia, especialmente desde el punto de vista económico, ha permanecido en la agenda pública nacional, sin que hasta el momento haya sido posible revertir la espiral ascendente en la que nos encontramos, a pesar de los diferentes enfoques estratégicos implementados, manteniéndose tal tendencia al alza durante la actual administración federal, así como el descontento ciudadano, por la incapacidad del gobierno para resolverlo.

Ante los múltiples intentos y pocos avances en materia de combate del crimen, la comisión de ilícitos continúa en aumento, tanto en cantidad como en nuevas modalidades delictivas, bajo las cuales pareciera que los delincuentes van a la vanguardia, tomando ventaja no solo respecto de las víctimas del delito, sino respecto de las propias autoridades.

III. En el T-MEC se observa que el Estado mexicano ha reconocido que las amenazas a la ciberseguridad menoscaban la confianza, en este caso, en el comercio digital, pero, el sector gubernamental no debe ser ajeno a las amenazas cibernéticas. De tal forma, el Estado debe coadyuvar en el ámbito de su competencia a efecto de desarrollar capacidades y mecanismos de colaboración gubernamentales para tratar rápidamente los incidentes de ciberseguridad, en concordancia con lo establecido en el T-MEC y dada su intervención con el sector comercial establecido en el Estado.

Aunque en México existen avances en materia de regulación de delitos informáticos, no han sido suficientes para contrarrestar los efectos producidos por los mismos, los cuales se han incrementado de manera incontrolable sin que exista un método eficaz para atacar su acelerada proliferación.[3]

En nuestro Código Penal Federal se encuentran tipificadas diversas conductas relacionadas con el acceso ilícito a sistemas y equipos de informática, pero dicha regulación no resulta totalmente aplicable a las diversas conductas ilícitas que son generadas por medio de un ordenador y códigos maliciosos.[4] El *ransomware,* por ejemplo, es un tipo de programa informático que bloquea un sistema hasta que se paga una cantidad de dinero.[5] Los ciberdelincuentes se infiltran en los sistemas informáticos de sus víctimas, encriptan los datos de las empresas y exigen un pago para desbloquearlos.[6] El *ransomware* , también conocido como “secuestro de datos”, se intensificó el año pasado, a pesar de que las empresas aumentaron su presupuesto para el rescate de datos.[7]

El secuestro de datos no se limita al software malicioso, conocido como *ransomware,* que infiltra y roba información para pedir un rescate, sino a un punto central en el que orbita toda la industria del cibercrimen. Los piratas informáticos toman en general el control de los ordenadores aprovechando las fallas de internet. Esto puede pasar porque la víctima consulta una página web ya infectada o porque abre un e-mail que lo invita a entrar en un enlace o a descargar un archivo adjunto, y en unos segundos el programa puede implantarse.[8]

Desde el famoso caso del Wanna Cry, el primer *ransomware* emblemático, los costos del secuestro de datos se han ubicado en promedio en cuatro millones de dólares, pero el año pasado alcanzó su máximo histórico.[9]

IV. La presente iniciativa constituye una propuesta por el futuro de la gobernabilidad, de la seguridad y de la prosperidad económica, política y social en el país; en un camino que no se puede elegir ni detener, pero sí proteger; el camino de la digitalización.

En estos casos, las sanciones actualmente establecidas para este tipo de delitos informáticos o cibernéticos no son del todo proporcionales a la de los hechos antijurídicos y del grado de afectación a los bienes jurídicos protegidos, así como a sus efectos e impactos personales y sociales generados. Aunado a lo anterior, la legislación penal, no considera la retención de información, como es el caso de quienes secuestran datos personales o confidenciales obtenidos mediante coacción o extorción a quien tiene la titularidad de los mismos. Por eso, además de la imperante necesidad de aumentar para ajustar a la realidad la punibilidad de los tipos establecidos, resulta también necesario agregar a ellos la conducta antijurídica por la retención de datos o información obtenida a costa de violencia, coacción o extorsión. De esta manera, a través de la presente iniciativa, se pretende atender una de las manifestaciones de la problemática en cuestión, tomando en consideración que, lamentablemente, ha ido transformándose durante los últimos años, al incrementarse de manera por demás notoria, sostenida e innegable, este tipo de criminales actividades.

De tal forma, se propone incluir en la tipificación de este tipo de delitos, sanciones mayormente contundentes, para actualizar su marco legal y, con ello, dar debida respuesta al sustancial incremento registrado últimamente. Para tales efectos se plantea reformar el Código Penal Federal con la finalidad de endurecer las penas que actualmente castigan los delitos informáticos y cibernéticos. En el caso de los delitos por el acceso ilícito a sistemas y equipos de informática, lo que se proyecta es modificar los artículos 211 Bis 1 a 211 Bis 5 del ordenamiento en mención para incrementar un tercio las penas, considerando que el actual artículo 211 Bis 7 dispone que las penas previstas en dicho capítulo aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno, lo cual sucede en la mayoría de los casos. Así que se considera adecuado el ajuste, partiendo de la coincidencia y el conocimiento de que las multas y sanciones que establece estas normas deben ser particularmente altas para inhibir las conductas.

Además, se añade a los tipos penales de los artículos 211 Bis 1, 211 Bis 2, 211 Bis 4 y 211 Bis 5, la conducta sancionable por retener dicha información, además de las de ya establecidas: modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática; ya que usualmente los ciberatacantes al ingresar indebidamente a estos sistemas sólo impiden, paralizan, u obstruyen la información, es decir, la secuestran, sin modificarla, destruirla o perderla. Por lo que se considera agregar la retención de información a la descripción de los tipos penales de dichos artículos.

La adición que se propone respecto a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares por los Delitos en materia del Tratamiento Indebido de Datos Personales consiste en el artículo 68 Bis para sancionar con prisión de dos años seis meses a veinticinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales

obtenidos mediante violencia, extorsión o coacción al titular, o a la persona autorizada para transmitirlos. Lo cual ha estado sucediendo reiteradamente.

En el caso de la Ley de Instituciones de Crédito, se propone modificar el artículo 112 Quáter, para sancionar con prisión de quince a cuarenta y cinco años y de ciento cincuenta mil a un millón quinientos días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

A su vez, la modificación del artículo 113 Bis, para quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito o de los recursos o valores de estas últimas, se propone aplicar una sanción de veinticinco a setenta y cinco años de prisión y multa de dos mil quinientos a un millón quinientos mil días de salario. Si quienes cometen el delito descrito son funcionarios o empleados de las instituciones de crédito o terceros ajenos pero con acceso autorizado por éstas a los sistemas de las mismas, la sanción será de treinta y cinco a setenta y cinco años de prisión y multa de cinco mil a doscientos cincuenta mil días de salario.

El porcentaje de incremento general que se propone a las sanciones que se establecen en las normas objeto de modificaciones descritas es de un tercio.

V. El ciberespacio es real, y las amenazas cibernéticas también tienen un impacto en el mundo físico. En el centro de todo ello están las sociedades, las empresas, los gobiernos, la ciudadanía, las y los niños y adolescentes, sus derechos, sus interacciones y sus logros, etcétera.

Aunque el incremento de los índices delictivos se ha convertido en un tema tan alarmante como común para nuestra sociedad, las amenazas cibernéticas son cada vez más frecuentes, complejas y destructivas, al atentar contra bienes y derechos jurídicamente tutelados, como la vida, la integridad, la salud, el patrimonio, los activos de información, la privacidad, la reputación, etcétera. Incluso inciden en la opinión pública a través de información falsa, lo que crea desinformación, perjudicando a niñas, niños, personas adultas, empresas, instituciones gubernamentales y hasta relaciones internacionales.

La dependencia tecnológica y los beneficios de su adopción para los gobiernos, empresas y sociedad son hechos notorios ampliamente comprobados, lo que exacerba los riesgos que representan las amenazas cibernéticas, las cuales constituyen un mercado global emergente, en consolidación y ampliamente lucrativo.

Hoy resulta complejo medir y cuantificar las consecuencias directas e indirectas que puede tener un ataque cibernético a todas las actividades y servicios gubernamentales, sean infraestructuras críticas o servicios esenciales o no, lo que constituye a las instituciones gubernamentales del país, prioridad en su protección, en virtud de los servicios de gobierno

que prestan a la ciudadanía, a través de los Poderes Ejecutivo, Legislativo y Judicial y órganos autónomos.

Han surgido nuevos retos en materia de riesgos y amenazas a los derechos humanos, la protección de datos personales, el patrimonio de las personas e instituciones, hasta los peligros latentes para la seguridad nacional e infraestructuras críticas del país. Por lo que debemos garantizar la seguridad cibernética de las instituciones gubernamentales, como un asunto de seguridad pública que no puede postergarse más. El Congreso de la Unión debe hacer un esfuerzo sin precedentes para contar con legislación eficiente en materia de ciberseguridad. Como hemos constatado, las amenazas cibernéticas no se detienen cada periodo electoral.

Como vemos, hay mucho que trabajar y los ordenamientos deben ser congruentes con la protección a los derechos inherentes a cualquier persona, cualquier organización y cualquier país.

En un gobierno que se jacta de orden transformador, el desarrollo de una política de seguridad nacional es fundamental. Los procesos a escala mundial son un elemento activo en las sociedades modernas y el fenómeno informático es ingrediente fundamental en la consecución de sus fines. Sin embargo, no podemos dejar las ventanas abiertas; el gobierno federal debe garantizar seguridad jurídica frente a las tecnologías de la información y de la comunicación, así como seguridad en las tecnologías de la información y comunicación, mediante estrategias que generen confianza en el uso de tecnologías.

Por lo expuesto y fundado sometemos a consideración de esta soberanía el siguiente proyecto de

Decreto

Primero. Se **modifican** los artículos 211 Bis 1 a 211 Bis 5; todos, del Código Penal Federal, para quedar de la siguiente manera:

Título Noveno
Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática

[...]

Capítulo IIAcceso Ilícito a Sistemas y Equipos de Informática

Artículo 211 Bis 1. Al que sin autorización modifique, destruya**, retenga** o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de **ocho** meses a dos años **y ocho meses** de prisión y de**ciento treinta y tres** a **cuatrocientos** días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se impondrán de **cuatro** meses a un año **y tres meses** de prisión**,** y de **sesenta y seis** a **doscientos** días multa**.**

Artículo 211 bis 2 .- Al que sin autorización modifique, destruya**, retenga** o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **un año y tres meses** a **cinco** años **y tres meses** de prisión y de doscientos **sesenta y seis** a **ochocientos** 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 **ocho** meses a dos años **y ocho meses** de prisión y de **ciento treinta y tres** a **cuatrocientos** 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 **cinco años y tres meses** a **trece** años de prisión y multa de **seiscientos sesenta y seis** a **mil trescientos tres y tres** 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 3. 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 años y ocho meses** a **diez** años **y seis meses** de prisión y de **cuatrocientos** a **mil doscientos** 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 **un año y tres meses** a **cinco** años **y tres meses** de prisión y de **doscientos** a **quinientos treinta y tres** 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 **cinco años y tres meses** a **trece** años de prisión y multa de **seiscientos sesenta y seis** a **mil trescientos tres y tres** 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 4. Al que sin autorización modifique, destruya**, retenga** 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 **ocho** seis meses a **cinco años y tres meses** de prisión y de **cientos treinta y tres** a **ochocientos** 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 **cuatro** meses a **dos años y seis meses** de prisión y de **sesenta y seis** a **cuatrocientos** días multa.

Artículo 211 Bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya**, retenga** o provoque pérdida de información que contengan, se le impondrán de **ocho** meses a **cinco** años **y tres meses** de prisión y de **ciento treinta y tres** a **ochocientos** 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 **cuatro** meses a dos años **y ocho meses** de prisión y de **sesenta y seis** a **cuatrocientos** 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.

Segundo. Se **adiciona** el artículo 68 Bis a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para quedar de la siguiente manera:

Capítulo XIDe los Delitos en materia del Tratamiento Indebido de Datos Personales

[…]

Artículo 68 Bis. Se sancionará con prisión de un años y seis meses a diez años al que, con el fin de alcanzar un lucro indebido, trate datos personales obtenidos mediante violencia, extorsión o coacción al titular, o a la persona autorizada para transmitirlos.

Tercero. Se **modifican** el primer párrafo del artículo 112 Quáter y el 113 Bis de la Ley de Instituciones de Crédito, para quedar redactados de la siguiente manera:

Capítulo IVDe los Delitos

[…]

Artículo 112 Quáter. Se sancionará con prisión de **cuatro** a **doce** años y de **cuarenta** mil a **cuatrocientos** días multa al que sin causa legítima o sin consentimiento de quien esté facultado para ello

I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o

II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Artículo 113 Bis. A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito o de los recursos o valores de estas últimas, se le aplicará una sanción de **seis años y seis meses** a **veinte** años de prisión y multa de **seis cientos sesenta y seis** a **cuarenta** mil días de salario.

Si quienes cometen el delito que se describe en el párrafo anterior son funcionarios o empleados de las instituciones de crédito o terceros ajenos pero con acceso autorizado por éstas a los sistemas de las mismas, la sanción será de **nueve años y seis meses** a **veinte** años de prisión y multa de **mil ciento treinta y tres** a **sesenta y seis** mil días de salario.

Transitorios

Primero. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Segundo. Se derogan todas las disposiciones que se opongan al presente decreto.

Notas

1 “Tech: Ransomware: ¿Qué es el secuestro de datos? Esto dicen los especialistas”, en *El Financiero,* 22 de septiembre de 2022, https://www.elfinanciero.com.mx/tech/2022/09/22/ransomware-que-es-el-secuestro-de-datos-esto-dicen-los-especialistas/

2 “Ciberataques en México aumentaron durante la pandemia”. Universidad de Guadalajara. Red Universitaria de Jalisco, 12 de septiembre de 2022, https://www.udg.mx/es/noticia/ciberataques-en-mexico-aumentaron-durante-la-pandemia

3 *Penalización de los delitos informáticos,* tesis para obtener el grado de maestro en derecho que presenta el licenciado Óscar Manuel Vences Sánchez. Universidad Autónoma del Estado de Morelos. Facultad de Derecho y Ciencias Sociales. División de Estudios Superiores de Posgrado. Maestría en derecho con Acreditación Pnpc (002478). Cuernavaca, Morelos. Diciembre de 2019, http://riaa.uaem.mx/xmlui/bitstream/handle/20.500.12055/2675/VESONS06T.pdf?sequence=1&isAllowed=y

4 Ídem.

5 “Estados Unidos desmantela una red internacional de secuestro de datos en internet. La banda, conocida como *Hive,* habría extorsionado a víctimas estadounidenses y de otras partes del mundo”. Escrito en Mundo el 27 de enero de 2023, https://mvsnoticias.com/mundo/2023/1/27/estados-unidos-desmantela-una-red-internacional-de-secuestro-de-datos-en-internet-581107.html

6 “El FBI *hackea* a los *hackers* responsables del secuestro de datos empresariales”, en *France 24,* 26 de enero de 2023, https://www.france24.com/es/ee-uu-y-canad%C3%A1/20230126-el-fbi-hackea-a-los-hackers-responsables-del-secuestro-de-datos-empresariales

7 “Lento avance en ciberseguridad cuestiona preocupación en México por atender secuestro de datos”, en *Arena Pública,* 24 de enero de 2023, https://m.arenapublica.com/tecnologias/lento-avance-en-ciberseguridad-cuestiona-preocupacion-en-mexico-por-atender-secuestro-de-datos

8 “Ransomware: ¿Qué es el secuestro de datos? Esto dicen los especialistas. En 2021, 74 por ciento de las empresas afirmó haber sido víctima de secuestro de datos en México”, 22 de septiembre de 2022, https://www.elfinanciero.com.mx/tech/2022/09/22/ransomware-que-es-el-secuestro-de-datos-esto-dicen-los-especialistas/

9 “Secuestro de datos cuesta 4.24 millones de dólares a empresas. Durante 2021 el *ransomware* afectó a 68 por ciento de las compañías, la cifra más alta de la historia, y para 2025 podría elevarse a 10 billones de dólares”, 13 de julio de 2022, https://wradio.com.mx/radio/2022/07/13/nacional/1657731605_800821.html

Palacio Legislativo de San Lázaro, a 18 de abril de 2023.

Diputada Rocío Esmeralda Reza Gallegos (rúbrica)