INICIATIVA QUE REFORMA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE EXTORSIÓN Y DELITOS COMETIDOS A TRAVÉS DE TECNOLOGÍAS DE LA INFORMACIÓN, SUSCRITA POR LA DIPUTADA JUANITA GUERRA MENA Y EL DIPUTADO MOISÉS IGNACIO MIER VELAZCO, Y SUSCRITA POR LEGISLADORES INTEGRANTES DE LOS GRUPOS PARLAMENTARIOS DE MORENA, DEL PVEM, DEL PT, DEL PRD, DEL PAN Y DE MOVIMIENTO CIUDADANO.

Los suscritos, diputados federales en la LXV Legislatura, con fundamento en los artículos 71 fracción II y 73 fracción XXIII de la Constitución Política de los Estados Unidos Mexicanos; 6o., numeral 1, fracción I, 77 numeral 1 y 78 del Reglamento de la Cámara de Diputados, ponen a consideración de esta honorable Cámara de Diputados la iniciativa con proyecto de decreto por el que se reforma el inciso a), fracción XXI, del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de extorsión y delitos cometidos a través de tecnologías de la información, al tenor de la siguiente

Exposición de Motivos

Regulación constitucional de la extorsión

El uso universal de las tecnologías de la información y las comunicaciones ha traído consigo la posibilidad de una interconexión de las personas con prácticamente todo el mundo que le rodea; actualmente el flujo diario de información y datos por medio de las redes de internet -tanto fijas como portables- equivale a la cantidad de conocimientos que se difundía en toda una década del siglo pasado.

Las redes globales son herramientas poderosas que permiten estrechar vínculos y acortar distancias prácticamente de forma inmediata y por esta razón los gobiernos los grandes corporativos, y la sociedad civil, han orientado recursos importantes en la generación de experiencias digitales que se adapten a las necesidades de los usuarios o gobernados.

Quienes hacemos uso de la tecnología de las comunicaciones lo realizamos como consecuencia de la necesidad de interacción constante, permanente e inmediata; es preciso señalar que nadie pone en duda la gran cantidad de beneficios de estas herramientas, sin embargo, las adopciones de estas nuevas modalidades de interrelación social a gran velocidad traen consigo un número significativo de riesgos y amenazas debido en mayor medida, a la volatilidad, al flujo de información personal expuesta.

Las nuevas tecnologías y modalidades se incorporan a la red y ello ha propiciado que la delincuencia ha adaptado su modus operandi para hacer uso de este tipo de mecanismos para ampliar y diversificar sus actividades ilícitas.

Una de ellas, es el aumento del fenómeno de la extorsión. Las bandas delincuenciales comenzaron a hacer uso de aparatos de comunicación para establecer contacto con sus potenciales víctimas mediante el uso de llamadas telefónicas o los denominados “SMS” o mensajes de texto.

Con la evolución de la infraestructura digital y el surgimiento de las redes de microblogging o redes sociales, los grupos delincuenciales se volvieron en su operatividad más sofisticados e incluso evolucionaron en su forma de operar al utilizar diversas modalidades de extorsión hacia sus víctimas como lo son: la obtención de supuestos premios obtenidos, campañas publicitarias, el otorgamiento de importantes y significativas líneas de crédito bancarias, la donación a fundaciones altruistas o hasta de supuestos beneficios sociales y créditos a la palabra.

El modelo del delito de extorsión se basa preponderantemente en el uso de la violencia psicológica y la manipulación verbal en contra de la víctima, aprovechándose en unos casos de su buena fe, ignorancia o en otros utilizando agresión; en la mayoría de los casos, los delincuentes eligen al azar a la víctima a partir del uso de datos personales y bases de datos obtenidas también de manera ilícita o en ocasiones, proporcionados por familiares o conocidos de la víctima.

En ocasiones, buscan propiciar un diálogo con la persona con el objeto de obtener información para utilizarla en su contra, sin embargo, no solamente restringen su actividad a la modalidad telefónica pues también indagan en las redes sociales de las víctimas, analizando sus imágenes, lo que les permite inferir y conectar a familiares, amigos, sitio de trabajo, su poder adquisitivo y nivel socioeconómico y producto de ello, obtener, número de teléfono celular, ubicación y actividad.

Ahora bien, es menester, desde el Poder Legislativo, actualizar y fortalecer el marco normativo para las sanciones adecuadas de las conductas ilícitas, además de renovar su tipificación, dotando así de las herramientas jurídicas y de actuación idóneas a las autoridades encargadas de la prevención, investigación e impartición de justicia, para afrontar una realidad cada vez más retadora.

No pasa desapercibido que el delito de extorsión ha tenido una evolución acelerada en los últimos años. La más reciente reforma al tipo penal, por este Poder Legislativo, data de hace casi treinta años, por lo que resulta claro que la redacción actual ha quedado superada, obstaculizando a las autoridades encuadrar la conducta al tipo penal vigente, derivado de que existen varias modalidades identificadas de facto, pero que en el texto de la norma jurídica, no se encuentran plasmadas ni tipificadas, imposibilitando el poder contrarrestar eficazmente este delito.

Actualmente, el Código Penal Federal, tipifica al delito de extorsión de la siguiente manera:

“**Artículo 390. Comete el delito de extorsión quien sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, para obtener un lucro para sí o para otro, o causando a alguien un perjuicio patrimonial…”**

El delito de extorsión amerita una pena corporal de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa, ampliándose la pena hasta un tanto más si se realiza por asociación delictuosa, por un servidor público, exservidor público, miembro o ex miembro de alguna corporación policial o de las Fuerzas Armadas.

Respecto de la extorsión, esta se conforma principalmente de dos modalidades en su comisión; en primer término, nos encontramos frente a una modalidad de extorsión de carácter directa, la cual ocurre cuando el delincuente se presenta físicamente en el establecimiento o domicilio particular, para amenazar al propietario o al personal que ahí? labora.

En esta modalidad, también reconocida como “cobro de piso”, el delincuente no tiene empacho en identificarse como integrante de una organización delictiva cuyo objeto es el de realizar un cobro para supuestamente brindar seguridad al establecimiento o lugar o como manera de chantaje para no hacer daño; en su desarrollo, amenaza con privar de la vida a algún familiar o a la probable víctima, así? como causar afectaciones materiales si no se entrega una cantidad periódica de dinero.

Es una forma cínica y al mismo tiempo compleja de regular, en donde, en diversas ocasiones el propio delincuente deja sus datos y la forma en que deberán comunicarse o contactarse con él o ella, para la entrega de los recursos.

Pero la comisión de este delito no se ha detenido ahí. La extorsión hoy es un delito de alto impacto que no solamente atenta contra la seguridad de las personas, sino cada vez de forma más aguda contra el patrimonio de las personas, convirtiéndose en un problema grave y de atención urgente, también, en materia económica.

La delincuencia ha tomado control de negocios y cadenas productivas. Con amenazas, obligan a comerciantes y personas a adquirir bienes de quienes ellos determinan, o bien, limitan su venta dentro de estos mismos criterios. Así, la actividad económica lo es todo, menos libre, y está, como nunca, expuesta a la coerción de la delincuencia.

De principio a fin, las cadenas económicas están capturadas y sometidas, impactando en el encarecimiento y escasez de productos, el cierre de negocios y la fuga de inversiones.

Este delito ha ido ganando terreno. Para facilitar su comisión y seguir abriéndose camino, la delincuencia amenaza también a los servidores públicos, esperando obtener la permisibilidad de las autoridades o incluso su colaboración en estos ilícitos. De esta forma, la delincuencia pretende coaccionar también a nuestras instituciones públicas.

Estos ilícitos, cometidos de forma directa y con la presencia de los delincuentes ante la ciudadanía, los comerciantes y los servidores públicos, encuentra en una segunda modalidad la ruta para reforzar sus amenazas, como también para abrir paso a otro tipo de conductas relacionadas con la extorsión.

Por la vía virtual, telefónica y a través de los distintos medios de comunicación, la delincuencia continúa ejerciendo presión sobre las personas y así lo han identificado las autoridades.

En la segunda modalidad, nos encontramos frente a un tipo indirecto de extorsión; siendo identificados por la autoridad hasta el momento seis versiones:

1. La obtención de un premio: La víctima recibe una falsa notificación sobre la obtención de un premio a cambio de un depósito bancario.

2. Secuestro virtual de un familiar: De manera violenta el delincuente indica que tiene secuestrado a un familiar y transmite la voz de una persona, generalmente una mujer o niño llorando, luego exige una cantidad de dinero a cambio de no hacer daño y dejarle en libertad.

3. Familiar detenido: El delincuente se hace pasar por un familiar lejano con quien no se tiene contacto, la retórica utilizada busca que la víctima se emocione, confunda o dude, lo que le permite obtener más información.

4. Amenaza: El delincuente utiliza el tono agresivo y vulgar posible, refiere datos de vivienda, familia, internet o red social, busca provocar temor ante una potencial vigilancia.

5. Amenaza de supuestos funcionarios: El delincuente se hace pasar por autoridad vinculada a un cuerpo de seguridad o procuración de justicia e informa que tiene detenido a un familiar de la víctima y pide dinero a cambio de liberarlo.

6. Deudas y cobranza: Se informa a quien contesta que se tiene una deuda adquirida por el usuario de la línea telefónica y se procederá a una supuesta acción de cobranza inmediata consistente en embargo de bienes, el tono va de amable a agresivo y se dan supuestas alternativas para saldar la deuda como “quitas” o descuentos altos; esta modalidad es realizada por supuestos “despachos de cobranza” que no son más que call centers con personal poco capacitado y con nulo conocimiento de las normas.

Si bien cualquier persona puede ser víctima de este delito, es claro que la delincuencia ha diversificado y optimizado sus mecanismos de operación a fin de hacer de este tipo delictivo un importante nicho de obtención de recursos.

Se trata de un tipo penal cuya modalidad, operatividad, mecanismos de desarrollo y esquema metodológico para su investigación guarda gran similitud con el de otros de alto impacto como el secuestro, trata o desaparición, por lo que es preciso realizar un ajuste normativo de gran envergadura que surja de la propia Constitución Política de los Estados Unidos Mexicanos, que posibilite la emisión de la Ley General en la materia.

El pasado mes de diciembre del 2022, el Observatorio Nacional Ciudadano alertó que las autoridades locales y federales no cuentan con los mecanismos operativos idóneos para enfrentar con eficacia las nuevas modalidades bajo las que se desarrolla el delito de extorsión.[1]

Dicha falta de mecanismos operativos son consecuencia de la ausencia de un marco jurídico de carácter general y especializado, que aborde la problemática delictiva desde una perspectiva transversal, con enfoque en las víctimas y con la implementación de mecanismos de colaboración y coordinación entre los tres órdenes de gobierno.

Ejemplo de ello es, que en el año 2022 este delito creció por arriba del 18 por ciento con respecto al 2021; asimismo, el INEGI[2] refiere que en 2021 se cometieron cerca de 5 millones de extorsiones y de estas solamente 246 mil se denunciaron (5 por ciento).[3]

Asimismo, de los casos denunciados que por su gravedad derivaron en carpetas de investigación, el 60 por ciento no tuvo progresos quedando en trámite solamente el 26 por ciento.[4]

La falta de un mecanismo legal coordinador de acciones, es evidente ante el hecho de que solamente el 2.8 por ciento de los casos derivó en una detención y en solamente el 0.3 por ciento de éstos se logró la reparación del daño.[5]

Se trata de una situación por la que la falta de una mejora legal de carácter sustancial ha impedido un eficaz actuar por parte de las autoridades, que, a pesar de contar con los instrumentos metodológicos, inteligencia policial y recursos tecnológicos, no cuenta con el marco jurídico adecuado para el combate de este delito que no solo afecta a los particulares sino a empresas.[6]

La rentabilidad del delito de extorsión es alta para los grupos delictivos, muestra de ello es su alta incidencia; con datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, en el año 2015, se tuvo una incidencia de 6 mil denuncias, mientras que para los años 2019 y 2020 se reportan 8,734 y 7960, respectivamente y en el año 2022 un reporte que asciende a 10,342 carpetas de investigación, lo que representa un aumento del 30 por ciento en tan solo 9 años y del 18 por ciento en 2022, debido en gran medida a la falta de homologación de penas y a la falta de mecanismos legales de coordinación interinstitucional de los tres niveles de gobierno con el objeto de reducir su incidencia y lograr su eventual erradicación como delito que tiene un alto componente de impacto y que debe considerarse grave dadas las implicaciones en la salud mental y física de las potenciales víctimas.

El impacto social del delito de extorsión es muy alto ya que afecta el patrimonio de cualquier persona, así como su tranquilidad y percepción de seguridad, además de inhibir la inversión formal de las pequeñas y medianas empresas como consecuencia de la falta de herramientas de la autoridad para garantizar la seguridad de las y los mexicanos.

Con datos de Coparmex,[7] los principales delitos que han padecido las empresas son el robo (49 por ciento) y en tercer lugar los delitos informáticos y el denominado cobro de piso, (28 por ciento) estos últimos con una importante relación conceptual en los medios comisivos; asimismo, reportan que el 20 por ciento de sus socios han sido víctimas de algún tipo de extorsión y de ellos 7 de cada 10 la han padecido en su modalidad telefónica.[8]

El delito de extorsión afecta lo mismo al comerciante, al emprendedor, al empresario que, al padre o madre de familia, al estudiante y en general a cualquier persona. Se trata de la modalidad delictiva con mayor crecimiento y presencia a nivel nacional, es importante mencionar que, con datos de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (Envipe 2022) el delito de extorsión es el delito más frecuente en 12 entidades federativas, seguido del fraude y del robo.[9]

Por ello, la presente iniciativa consiste en la adecuación del Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos a fin de que en la fracción XXI inciso a), se considere como delito de alto impacto, a la extorsión en todas sus modalidades, como el medio de comisión de delitos en aumento y el mecanismo de diversificación de los medios ilícitos por el cual la delincuencia se allana de recursos financieros para sus operaciones.

La intención de modificar el texto constitucional radica en la necesidad de incorporar de manera expresa la denominación del tipo penal de extorsión, a fin de que el Congreso de la Unión tenga la atribución exclusiva conferida por el constituyente, para desdoblar un mecanismo articulador de acciones de carácter normativo que permita a la autoridad ejecutora y aplicadora de la norma, el pleno y puntual desarrollo de acciones de combate a este nocivo flagelo social.

De esta manera, al incorporar el delito de extorsión en la Carta Magna, se establece por añadidura la posibilidad legal de expedir en el momento procesal oportuno, la correspondiente Ley General en la materia que contenga el sistema de distribución de competencias, las atribuciones de las autoridades para enfrentarlo con eficacia y de manera específica y a partir de un profundo diagnóstico de los elementos del tipo penal, el modus operandi, los medios comisivos y las calificativas, la definición conceptual a fin de que los fiscales del orden federal y de las Entidades Federativas tengan los elementos para determinarlo y clasificarlo con prontitud, expedites y claridad técnica.

Sobre todo, porque, con datos de la Coordinación Nacional Antisecuestro, de un estudio realizado a los 33 Códigos Penales se evidencia una clara disparidad en la definición de los tipos penales y en el establecimiento de sanciones relacionado con el delito de extorsión, mismas que oscilan de 1 a 35 años de prisión y multa de 10 hasta 4 mil Unidades de Medida y Actualización.

Ejemplo de esta delicada disparidad punitiva, es, que mientras el Código Penal Federal establece que la pena aplicable al delito será de 2 a 8 años de prisión, en el Código Penal del Estado de Chihuahua el delito se tasa con una pena de 5 hasta 30 años.

Misma disparidad se encuentra al contrastar los Códigos Penales de distintas Entidades ya que en algunas la penalidad es sumamente baja, como el caso de Yucatán donde la sanción es de 1 a 6 años y en Tamaulipas el delito se equipara al de robo.

El aumento en la comisión de este delito debe ser tomado con seriedad y con responsabilidad por parte de las y los legisladores; para nosotros desde este órgano colegiado no es ajeno el hecho de que el propio Sistema Nacional de Seguridad Pública reporte en el mes de marzo del 2023, que el delito de extorsión tiene un significativo aumento del 18.4 por ciento de incidencia nacional con respecto al año 2019.[10]

Regulación constitucional de los delitos cibernéticos

Otro mecanismo en el que el crimen ha diversificado sus modalidades para delinquir, son los delitos cibernéticos.

No hay una definición universalmente aceptada de ciberdelincuencia. No obstante, la Oficina de Naciones Unidas Contra la Droga y el Delito la define de la siguiente manera: “La ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito…La ciberdelincuencia se diferencia de los delitos comunes en que no tiene barreras físicas o geográficas, y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes”.

La Agencia de la Unión Europea para la Cooperación Policial distingue la ciberdelincuencia en delitos dependientes de los medios informáticos (es decir, todo delito que puede cometerse sólo usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación) y delitos propiciados por los medios informáticos (es decir, delitos comunes facilitados por Internet y las tecnologías digitales). La distinción principal entre estas categorías de ciberdelincuencia es el papel de las TIC en el delito, ya sea como el objetivo del delito o como parte del modus operandi del delincuente. Cuando las TIC son el blanco del delito, este ciberdelito afecta de forma negativa la confidencialidad, integridad o accesibilidad de los sistemas y datos informáticos. La confidencialidad, integridad y accesibilidad forman la conocida como “Triada CIA”: en palabras simples, la información privada debe permanecer privada, no se debe cambiar sin el permiso del dueño y este debe tener accesibilidad a los datos, servicios y sistemas en todo momento. Cuando las TIC forman parte del modus operandi, la ciberdelincuencia entraña un delito común (por ejemplo, un fraude o robo) que el Internet o las tecnologías digitales facilitan de alguna forma.

El Convenio de Budapest, aunque no define la ciberdelincuencia, sí establece que los ciberdelitos son aquellos actos que ponen en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, y hace la tipificación como delito de dichos actos, clasificándolos de la siguiente manera:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

  1. Acceso ilícito;

  2. Interceptación ilícita;

  3. Ataques a la integridad de los datos;

  4. Ataques a la integridad del sistema; y

  5. Abuso de los dispositivos.

- Delitos Informáticos

  1. Falsificación Informática; y

2. Fraude Informático.

- Delitos relacionados con el contenido

1. Delitos relacionados con la pornografía infantil; y

2. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

De acuerdo con un informe publicado por la Interpol el 4 de agosto de 2020 sobre las repercusiones del Covid-19 en la ciberdelincuencia, se ha puesto de manifiesto un cambio sustancial en los objetivos de los ataques, que antes eran hacía particulares y pequeñas empresas y ahora los ataques tienden a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales.

Entre las constataciones principales que pone de relieve la evaluación de la Interpol sobre el panorama de la ciberdelincuencia en relación con la pandemia de Covid-19 destacan

• Las estafas por internet y el phishing: Los autores de las amenazas han revisado sus métodos habituales en materia de estafas por Internet y phishing. Ahora, los ciberdelincuentes, a menudo haciéndose pasar por autoridades gubernamentales y sanitarias, envían a sus víctimas correos electrónicos de phishing sobre el Covid-19 en los que las incitan a facilitar datos personales y a descargar contenidos maliciosos.

• Malware disruptivos (ransomware y DDoS): Alentados por la probabilidad de causar graves problemas y obtener sustanciosas ganancias, los ciberdelincuentes están multiplicando el número de ataques con malware disruptivos contra las infraestructuras esenciales y las instituciones sanitarias. Los ataques con ransomware perpetrados por distintos grupos delictivos, que en meses anteriores se habían mantenido relativamente latentes, alcanzaron su punto álgido en las dos primeras semanas de abril de 2020. Las investigaciones de las fuerzas del orden muestran que la mayoría de los atacantes calculaban con bastante exactitud la cantidad máxima que podían solicitar como rescate a las organizaciones víctimas de sus ataques.

• Malware destinados a obtener datos: En el ámbito de la ciberdelincuencia también están en auge los ataques de malware para obtener datos, como los troyanos de acceso a distancia, los ladrones de información, los spyware (programas espía) o los troyanos bancarios, entre otros. Los autores de las amenazas utilizan información relacionada con el Covid-19 como señuelo para infiltrarse en los sistemas e infectar redes, sustraer datos, desviar fondos y crear botnets.

• Dominios malignos: Se ha producido un aumento considerable del número de ciberdelincuentes que, aprovechando el incremento de la demanda de productos médicos e información sobre el Covid-19, registran nombres de dominio que contienen palabras clave como “coronavirus” o “Covid”. Se trata de sitios web fraudulentos que sustentan una amplia variedad de actividades malignas.

• Desinformación: La información no contrastada, las amenazas mal entendidas y las teorías de la conspiración han fomentado la ansiedad de la población y, en algunos casos, facilitado la ejecución de ciberataques. Cerca de 30 por ciento de los países que contestaron a la encuesta mundial sobre ciberdelincuencia confirmaron la circulación de información falsa sobre el Covid-19. En el plazo de un mes, un país informó de 290 publicaciones, la mayoría de las cuales ocultaba malware. También se comunicaron casos de desinformación vinculada al comercio ilegal de productos médicos fraudulentos. Otros casos de desinformación guardaban relación con estafas a través de mensajes de texto que presentaban ofertas demasiado buenas para ser ciertas, por ejemplo, alimentos gratuitos, ventajas especiales, o grandes descuentos en supermercados.

El informe de la Interpol destaca que es altamente probable que la ciberdelincuencia siga aumentando a corto plazo. Debido a las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener mayores ganancias, los ciberdelincuentes seguirán ampliando sus actividades y concebirán unos modus operandi más avanzados y complejos.

Señala que también es probable que, para aprovechar la preocupación de la ciudadanía por la pandemia, los autores de amenazas continúen propagando estafas por Internet y campañas de tipo phishing relacionadas con el coronavirus; que aumenten las estafas a empresas por e- mail mediante suplantación de identidad, como consecuencia de la recesión económica y los cambios que se han producido en el panorama empresarial, lo que generará nuevas oportunidades para la comisión de delitos; entre otros.

Del 25 al 29 de noviembre de 2019 se llevó a cabo la quinta Semana Nacional de la Ciberseguridad en México, organizada por la División Científica de la Secretaría de Seguridad y Protección Ciudadana de la Guardia Nacional. La cual tiene la finalidad de concientizar a la sociedad en general sobre la importancia del uso responsable de las nuevas tecnologías de la información a través de la difusión de contenidos preventivos y de concientización sobre los riesgos del ciberespacio a fin de disminuir la incidencia ocasionada por conductas antisociales e ilícitas y promover la denuncia de delitos cibernéticos.

En ella participó la Oficina de las Naciones Unidas contra la Droga y el Delito: presentó su Programa Global de Ciberdelito, el cual acompaña el esfuerzo de los Estados miembros en la lucha contra esta clase de crímenes, a través de asistencia técnica especializada y fortalecimiento de capacidades.

Este programa enfatiza la relevancia de la coordinación nacional, la recopilación de datos y la necesidad de marcos legales efectivos que lleven a una respuesta sostenible, en un marco sólido de derechos humanos.

De acuerdo con el secretario general de la Organización de las Naciones Unidas, António Guterres, se estima que la ciberdelincuencia genera ingresos por alrededor de 1.5 trillones de dólares al año, así como la mayoría de los crímenes afecta a las personas en mayor situación de vulnerabilidad.

Se estima que México es el noveno país más afectado por el crimen cibernético. En América Latina es superado sólo por Brasil.

No obstante, México no cuenta con una ley dedicada a los delitos cibernéticos, únicamente el Código Penal Federal contiene un título dedicado a la revelación de secretos y acceso ilícito a sistemas y equipos informáticos. Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen.

De acuerdo con datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, en 2017 cada hora se cometían 463 fraudes cibernéticos en operaciones por comercio electrónico y banca móvil. En 2018, las pérdidas por este delito sumaron 4 mil 412 millones de pesos.

El Banco Interamericano de Desarrollo y la Organización de Estados Americanos revelan que se pierden alrededor de 9 mil millones de dólares anuales por delitos cibernéticos. Incluso, los propios sitios del gobierno federal como Pemex; las Secretarías de Economía, de Hacienda, y del Trabajo y Previsión Social han sufrido ataques.

Entre enero y junio de 2020 se registraron 3.1 millones de intentos de ciberataque. De acuerdo con la Dirección General Científica de la Guardia Nacional, la actividad maliciosa en internet disminuyó en 12 por ciento en el periodo diciembre de 2019-febrero de 2020. Sin embargo, esta cifra se incrementó en 14 por ciento en marzo y abril, periodo correspondiente a la emergencia sanitaria. En cuanto a la pornografía infantil, la Guardia Nacional calculó un incremento de 73 por ciento durante el mismo periodo. Casi 80 por ciento fueron relacionados con la red social Facebook.

De acuerdo con la Guardia Nacional entre las principales amenazas a la población en internet está la vulneración en la seguridad de la información, el robo de datos, fraudes, suplantación de identidad, el acceso lógico no autorizado, así como la infección por el código malicioso.

Para esta Cámara de Diputados, resulta primordial impulsar una reforma al texto de la Carta Magna a fin de que en el Artículo 73 fracción XXI inciso a) se incorpore a la extorsión y a los delitos cometidos a través de tecnologías de la información como modalidades delictivas de las que resulte imperativo expedir su respectiva norma de carácter general, que permita la homologación de criterios, modelos homologados de capacitación, de abordaje desde la autoridad y sobre todo, la posibilidad de que en un solo momento procesal parlamentario se emitan los debidos criterios para que las autoridades Federal y de las Entidades Federativas, actúen en consecuencia sin el obstáculo que representa la dispersión de criterios punitivo normativos actual.

Así las cosas, es clara la necesidad de impulsar esta valiosa modificación a fin de restituir la paz y la tranquilidad de comunidades enteras de mexicanas y mexicanos que han padecido o se encuentran en potencial situación de padecer este grave delito.

Delitos relacionados con el uso de las tecnologías

Por lo anteriormente expuesto sometemos a consideración de esta H. Cámara de Diputados la siguiente iniciativa con proyecto de

Decreto

Único. Se **reforma** el inciso a) de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Constitución Política de los Estados Unidos Mexicanos

Artículo 73.- ...

I. a **XX.** ...

XXI. Para expedir:

a) Las leyes generales que establezcan como mínimo, los tipos penales y sus sanciones en las materias de secuestro, desaparición forzada de personas, otras formas de privación de la libertad contrarias a la ley, **extorsión, los delitos cometidos a través de tecnologías de la información** , trata de personas, tortura, y otros tratos o penas crueles, inhumanos o degradantes, así como electoral.

b) y **c)** ...

...

...

XXII. a **XXXI.** ...

Artículos Transitorios

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

Segundo. El Congreso de la Unión deberá expedir la Ley General en materia de delitos de extorsión en un término de 180 días hábiles contados a partir del día siguiente al de la entrada en vigor del presente decreto.

Notas

1 La extorsión bajo el caleidoscopio: muchas modalidades y pocas políticas públicas. Observatorio Nacional Ciudadano. 2022.

2 Instituto Nacional de Estadística y Geografía

3 IB Ídem.

4 Ídem.

5 Ídem.

6 De acuerdo con el Observatorio Nacional Ciudadano, en 2021 cerca de 1.2 millones de empresas fueron víctimas de algún delito, siendo la extorsión (28.9 por ciento), la más frecuente.

7 Confederación Patronal de la República Mexicana.

8 Fuente: Encuesta a socios Coparmex, tercer cuatrimestre 2022.

9 Envipe 2022. Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2022. Fuente: Inegi.

10 Fuente: Coordinación Nacional Antisecuestro con datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública del mes de marzo del 2023.

Dado en el Palacio Legislativo de San Lázaro, a 26 de abril de 2023.

Diputados: Valeria Santiago Barrientos, Marisela Garduño Garduño, Moisés Ignacio Mier Velazco, María Guadalupe Román Ávila, Juanita Guerra Mena, Román Cifuentes Negrete, Armando Corona Arvizu, Rocío Reza Gallegos, Francisco Javier Huacus Esquivel, Carlos Puente Salas, Reginaldo Sandoval Flores.