INICIATIVA QUE REFORMA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, A CARGO DE LA DIPUTADA JUANITA GUERRA MENA, DEL GRUPO PARLAMENTARIO DE MORENA.

La suscrita, Juanita Guerra Mena, integrante del Grupo Parlamentario de Morena 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; y 6, numeral 1, fracción I, 77, numeral 1, y 78 del Reglamento de la Cámara de Diputados, pone a consideración de la Cámara de Diputados iniciativa con proyecto de decreto por el que se adiciona la fracción XXIII Ter del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de ciberdelincuencia, al tenor de la siguiente

Exposición de Motivos

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, Antônio 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.

Por lo expuesto es fundamental dotar al Congreso de la Unión de la facultad para expedir las normas de carácter general en materia de ciberdelincuencia y cibercrimen, que contengan mecanismos de coordinación entre autoridades de los tres órdenes de gobierno y el diseño de una estrategia nacional de inteligencia cibernética y policial.

Proyecto de Decreto

Único. Se **adiciona** la fracción XXIII Ter al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Constitución Política de los Estados Unidos Mexicanos

Artículo 73. El Congreso tiene facultad

I. a **XXIII Bis.** ...

XXIII Ter. Para expedir las normas de carácter general en materia de ciberdelincuencia y cibercrimen, que contengan los mecanismos de coordinación entre autoridades de los tres órdenes de gobierno y el diseño de una estrategia nacional de inteligencia cibernética y policial;

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.

Tercero. El Congreso de la Unión deberá emitir, en un plazo que no exceda de 180 días naturales a partir del siguiente a la entrada en vigor del presente decreto, la Ley General contra la Ciberdelincuencia y el Cibercrimen.

Cuarto. Las legislaturas de las entidades federativas deberán expedir la Ley de Coordinación contra el Cibercrimen y el Ciberdelito en un término improrrogable de 90 días naturales a partir de la entrada en vigor de la Ley General en la materia a la que se refiere el Artículo 73 fracción XXIII Ter del presente Decreto, así como para armonizar lo conducente en la legislación aplicable en materia de Seguridad Pública y Ciudadana.

Palacio Legislativo de San Lázaro, a 23 de septiembre de 2021.

Diputada Juanita Guerra Mena (rúbrica)