QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DE LOS CÓDIGOS PENAL FEDERAL, Y FEDERAL DE PROCEDIMIENTOS PENALES, ASÍ COMO DE LAS LEYES GENERAL PARA PREVENIR, SANCIONAR Y ERRADICAR LOS DELITOS EN MATERIA DE TRATA DE PERSONAS Y PARA LA PROTECCIÓN Y ASISTENCIA A LAS VÍCTIMAS DE ESTOS DELITOS, DE LA POLICÍA FEDERAL, Y FEDERAL DE TELECOMUNICACIONES, A CARGO DE CONSUELO ARGÜELLES LOYA Y SUSCRITA POR JOSÉ ALEJANDRO MONTANO GUZMÁN, DIPUTADOS DE LOS GRUPOS PARLAMENTARIO DEL PAN Y DEL PRI, RESPECTIVAMENTE

Exposición de Motivos

El desarrollo dinámico de las tecnologías de la información y comunicaciones a nivel mundial, además de generar importantes ventajas en las actividades cotidianas de las personas y de las autoridades de los Estados, ha propiciado que se considere a la ciberdelincuencia como una amenaza a la seguridad y funcionamiento de los sistemas informáticos, lo que implica una afectación no sólo en la privacidad de las personas y en su patrimonio, sino también en la economía e incluso en la estabilidad y funcionamiento de cualquier país.

La atención de este fenómeno delictivo por parte de las autoridades estatales y organismos internacionales conlleva una alta complejidad, en atención a que en algunos casos las conductas delictivas se llevan a cabo a través de equipos electrónicos situados en algún país que no necesariamente es el mismo en donde se genera el daño o perjuicio. Así, esta nueva modalidad para la comisión de ilícitos permite que los criminales logren sus objetivos sin necesidad de arriesgar su integridad física, basta con que cuenten con un equipo electrónico, red de internet y la capacidad para hacer uso de éstos en la comisión de un delito, prácticamente en cualquier parte del mundo.

De ahí que, diversos países han emitido disposiciones jurídicas que penalizan esas prácticas del mundo virtual, siempre con una perspectiva global y buscando una efectiva cooperación internacional para la persecución y sanción de dichas conductas ilícitas.

En este mismo sentido, diversos organismos internacionales, tales como la Organización de las Naciones Unidas, la Organización para la Cooperación y el Desarrollo Económicos, la Unión Europea, el Consejo de Europa y la Organización de los Estado Americanos, han señalado la necesidad de implementar acciones en los ámbitos técnico, jurídico y de las instituciones del Estado, así como de cooperación multilateral, de investigación, persecución y prevención para el combate a la ciberdelincuencia, principalmente por su carácter transnacional.

En el sistema jurídico mexicano, la figura de delito informático data de poco más de diez años, en comparación con otros sistemas jurídicos, en los que su regulación deviene desde los inicios de la segunda mitad del siglo pasado. Tal es el caso de los Estados Unidos de América con la propuesta del Senador Abraham Ribicoff de 1977 para legislar en materia de ciberdelitos. Posteriormente, en 1983, la Organización para la Cooperación y el Desarrollo Económico designó un comité de expertos para el estudio del tema, quienes emitieron un dictamen en el que recomiendan a los países miembros de tal organización incorporar la regulación de los delitos informáticos en su legislación penal. Asimismo, en 1989, el Consejo de Europa emitió una recomendación en la que se enlistan los delitos mínimos que deberá de agregar a su legislación cada país miembro.

La necesidad de contar con una regulación específica de delitos informáticos también ha sido parte de la agenda en diversos foros internacionales. Ejemplo de ello son el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal, Canadá (1990), el Octavo Congreso Criminal de las Naciones Unidas (1990) y la Conferencia de Wurzburgo, en Alemania (1992).

Todo lo anterior constituyó el antecedente para que la comunidad internacional –interesada por la atención de la ciberdelincuencia en un nivel global–, estableciera en 1996 el denominado Comité Especial de expertos sobre delitos relacionados con el empleo de computadoras, integrado por especialistas en el tema de combate a los delitos cibernéticos, en particular los que se cometen a través de las redes de telecomunicaciones.

Dicho comité se encargó de elaborar un borrador del instrumento jurídico internacional que atendiera ese fenómeno delincuencial. De ahí que, el 23 de noviembre de 2001, el Consejo de Ministros de Europa, compuesto por los Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con los Estados Unidos de América, Sudáfrica, Canadá y Japón, firmaron en Budapest la Convención sobre Delitos Informáticos, hasta ahora la principal directriz para que los Estados parte cuenten en su ámbito interno con una base legal sólida en materia penal y con un sistema estandarizado de instrumentos de investigación, de salvaguardias conexas y de protección a los derechos humanos, además de que procura viabilizar la cooperación internacional en la lucha contra la ciberdelincuencia.

Al efecto, los principales rubros que establece dicho instrumento de corte internacional son:

a) Armonización de las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;

b) Establecimiento de reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de los ciberdelitos, y

c) Establecimiento de un régimen dinámico y efectivo de cooperación internacional en la materia.

En este contexto y derivado de la constante evolución de la ciberdelincuencia y de las amenazas a los sistemas informáticos, se advierte la necesidad de contar con un marco jurídico efectivo para la persecución y sanción de los ciberdelitos, en el que se contemplen los requerimientos mínimos establecidos o recomendados por instrumentos jurídicos de carácter internacional, a fin de estar en condiciones de formar parte de los esquemas de coordinación y cooperación con los demás Estados y organismos internacionales, conforme a los cuales se establezcan mecanismos de asistencia jurídica mutua a nivel regional y mundial para la prevención y, en su caso, investigación y sanción de esos delitos.

Adicionalmente, resulta relevante y de especial importancia el impacto del cibercrimen en la estabilidad y gobernabilidad de un Estado, toda vez que mediante ataques informáticos masivos se puede llegar a obtener información relacionada con áreas estratégicas o simplemente hacer uso de la red de Internet para difundir mensajes, imágenes o videos que tengan por objeto infundir terror o temor en la sociedad, y con ello atentar contra la seguridad nacional o el normal funcionamiento de las autoridades del Estado.

En este sentido, actualmente es posible que grupos de la delincuencia organizada, grupos terroristas o incluso una persona en lo individual puedan llegar a desarrollar en la red de telecomunicaciones o en sistemas electrónicos, diversas actividades relacionadas con actos terroristas, como la identificación de víctimas, el diseño de planes de ataque, la obtención de información en páginas gubernamentales, de partidos políticos, del sector privado, o bien difundir y promover sus postulados u objetivos para impulsar su agenda y ampliar su base social.

En estas circunstancias, se advierte la necesidad de sancionar los actos terroristas que se lleven a cabo a través de la red de telecomunicaciones o de sistemas electrónicos, en virtud del vacío legal al respecto y del impacto que los mismos pueden tener en la integridad, estabilidad o permanencia de los Estados.

El impacto de los ciberdelitos en los ámbitos nacional e internacional

La ciberdelincuencia ha sido objeto de análisis por parte de las autoridades de los Estados, de organismos internacionales y de la propia iniciativa privada, dado que la afectación de las conductas delictivas tiene impacto tanto en el sector público como en el privado, y un alcance global en algunos supuestos.

De ahí que, se han publicado diversos reportes o informes con estadísticas que reflejan el nivel que ha alcanzado el fenómeno de la ciberdelincuencia a nivel nacional e internacional, así como la vulnerabilidad de los sistemas informáticos de las autoridades y de los particulares.

En este sentido, la empresa Symantec llevó a cabo una encuesta a más de 7 mil adultos de 14 países –Australia, Brasil, Canadá, China, Francia, Alemania, India, Italia, Japón, Nueva Zelanda, España, Suecia, Reino Unido y los Estados Unidos de América–, de la que publicó el Informe de delitos cibernéticos de Norton 2011, en el que se advierten los alcances de los ciberdelitos, los costos que representan, así como la falta de justicia que manifiestan las víctimas.

El informe señala que cerca del 65 por ciento de adultos en el mundo han sido víctimas de algún tipo de ciberdelito, tales como estafas *online*, ataques de *phishing*, actividades de piratas informáticos en perfiles de redes sociales y fraudes con tarjetas de crédito. En cuanto a los responsables de estas conductas ilícitas, un 56 por ciento son delincuentes anónimos y un 21 por ciento grupos organizados.

Por lo que hace a la solicitud de ayuda cuando se es víctima de un ciberdelito, el reporte identificó que el 48 por ciento de las víctimas llaman a sus instituciones financieras, el 44 por ciento a la policía y sólo el 34 por ciento contactan al propietario de un sitio web o al proveedor de correo electrónico.

En cuanto al daño económico que representa la comisión de un ciberdelito, la encuesta señala que el monto por las actividades de la ciberdelincuencia que han erogado las víctimas supera los 388 mil millones de dólares. Asimismo, destaca que se gastaron directamente 114 mil millones de dólares debido al dinero robado por los delincuentes, o bien, al monto gastado en resolver los ataques cibernéticos. Igualmente, se determina que el gasto equivalente al tiempo perdido valuado por las víctimas, se estima en 274 mil millones de dólares.

En este mismo tenor, a principios de 2012 la Agenda de Seguridad y Defensa (SDA, por sus siglas en inglés),+++1+++ publicó el informe sobre "Seguridad Cibernética: la controvertida cuestión de reglas globales",+++2+++ en el que se concluyó que a pesar de que el gobierno de México ha desarrollado acciones de lucha contra el narcotráfico, las organizaciones delictivas cuentan con tecnología avanzada, lo que las coloca en ventaja frente a las acciones gubernamentales para su combate.

Al respecto, en septiembre de 2011 se confirmó la vulnerabilidad de los portales oficiales del gobierno mexicano, en virtud de los ataques del grupo de *hackers* denominado "Anonymous", lo que generó mayor interés para atender dicha problemática de corte internacional, así como la necesidad de contar con un marco jurídico en materia de delitos cibernéticos y con los recursos tecnológicos que permitan hacer frente a ese fenómeno criminal.

Adicionalmente, el gobierno de México ha registrado incidencias sobre delitos cibernéticos (3.8 casos por día) y a fin de atender esta problemática, ha conformado un grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos (DC- México), cuyas acciones se han centrado en hacer frente a organizaciones criminales.

La Secretaría de Seguridad Pública en su Cuarto Informe de Labores (Septiembre de 2009-julio de 2010) refiere que en México las principales conductas delictivas en Internet registradas son el *hackeo, phreaking,* asesinatos a sueldo, venta de droga, ciberterrorismo, así como programación de virus y códigos maliciosos. En dicho informe se destaca el incremento importante en la propagación de estos últimos, ya que en el 2008 se tuvo un registro de 1 millón 691 mil 323 y en 2009 de 2 millones 895 mil 802 casos.

En un quinto Informe de Labores (Septiembre de 2010-julio de 2011) de la misma dependencia, a través de la División Científica de la Policía Federal, se señala que se realizaron acciones para prevenir, investigar y combatir los delitos cibernéticos, mediante la atención y asesoría a la ciudadanía con base en un monitoreo permanente a la red pública de internet. De ello, derivaron 5 mil 582 denuncias ciudadanas, las cuales fueron recibidas a través de diferentes medios de captación, a saber: 3 mil 389 vía correo electrónico, 1 mil 432 mediante el Centro Nacional de Atención a la Denuncia Ciudadana de la Policía Federal y 761 por teléfono. Al respecto, las conductas que presentaron un mayor índice de denuncias fueron el fraude al comercio electrónico y *phishing.*

Si se atiende a las principales conductas delictivas que se suscitan en nuestro país, conforme a lo referido por los reportes de la Secretaría de Seguridad Pública, es propio considerar que en materia de delitos informáticos se han

afectado diversos bienes jurídicos como el patrimonio, la intimidad, la información, la propiedad e incluso la seguridad nacional.

Asimismo, de acuerdo al sexto Informe de Labores de esa secretaría, las acciones realizadas por la Policía Federal, a través de la División Científica para Combatir el Delito Cibernético, de junio de 2011 a septiembre de 2012 se detectaron 13 mil 133 incidentes en materia de ciberdelitos, entre los cuales han imperado el *phishing,* la negación de servicio, la alteración de contenido *(hacking),* la infección por código malicioso, la propagación de malware y los accesos no autorizados. Al mismo tiempo se registró que el promedio de denuncias sobre ciberdelitos, comparado con el periodo de septiembre de 2010 a junio de 2011, se incrementó en un 135 por ciento, ya que pasó de 18 a 44 denuncias por día aproximadamente.

Frente a este escenario, en el que la globalización del espacio cibernético ha producido el incremento en la comisión de delitos, resulta imperioso que México cuente con una regulación jurídica adecuada, que desde una perspectiva integral que atienda los aspectos de prevención, persecución y sanción de los ciberdelitos como un asunto prioritario en la política de seguridad de la información de las instituciones de gobierno y, al mismo tiempo, lo dote de criterios que lo posicionen en el ámbito internacional como un Estado comprometido con los estándares internacionales de seguridad y de regulación jurídica efectiva en materia de ciberdelincuencia.

Marco jurídico nacional vigente en materia de ciberdelincuencia

En atención a las recomendaciones emitidas en el ámbito internacional, el primer tratamiento de los ciberdelitos en México ha sido resultado de la labor legislativa publicada en el Diario Oficial de la Federación el 17 de mayo de 1999, misma que incorporó una serie de delitos al Código Penal Federal en el Título Noveno, denominado "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática", distribuidos, hasta la fecha, en dos capítulos que integran diez artículos (210 al 211 Bis 7), que se refieren, principalmente, a la alteración o pérdida de información de los sistemas informáticos, así como a la copia y/o uso de la información no autorizada y en los que además la principal agravante de las penas se prevé para el caso de que el sujeto pasivo de la conducta sea el Estado.

Con esto es claro que México no cuenta con una ley específica en materia de ciberdelitos. No obstante, aunque existen disposiciones en la materia que se encuentran dispersas dentro del marco jurídico nacional, ha sido insuficiente para combatir conductas delictivas en medios cibernéticos. Si bien la tecnología ha generado grandes beneficios económicos, al mismo tiempo ha facilitado el aumento del crimen cibernético.

De ahí la necesidad de incluir y actualizar el catálogo de los delitos previstos en nuestro marco jurídico penal, a fin de adecuarlo para tipificar otras conductas delictivas llevadas a cabo a través de Internet.

Cabe señalar que el Poder Legislativo ha manifestado su interés en la atención del fenómeno de la ciberdelincuencia, a través de la presentación de diversas iniciativas y, en concreto, mediante la emisión de un punto de acuerdo de la Comisión Permanente del Senado de la República[3] , en el que se exhorta al Ejecutivo Federal para que México se adhiera formalmente a la Convención de Budapest, y se destaca que éste es un mecanismo bien articulado, vasto en sus concepciones, explícito en sus medios y fines, así como respetuoso de la soberanía y de los sistemas judiciales de los países adherentes, a los que concede un notable campo de acción a nivel internacional en la investigación, persecución y sanción de los delitos cibernéticos.

Por todo lo anterior, se advierte la importancia de una mayor regulación de los delitos cibernéticos en el orden jurídico nacional, a fin de fortalecer los esquemas de coordinación y cooperación del Estado mexicano con la comunidad internacional, a través de la implementación de instrumentos legales que agilicen la asistencia para la cooperación en la investigación de delitos a nivel regional y mundial.

Contenido de la iniciativa

Las líneas cardinales de la presente iniciativa de reformas en materia penal son el reflejo del interés del Estado Mexicano de regular ilícitos que, además de no ser privativos de nuestro entorno actual, constituyen un grave problema frente a la evolución en la tecnología.

Lo anterior, en virtud de que los delitos cibernéticos además de ser una expresión negativa de la globalización, su nulo o inadecuado tratamiento jurídico puede llegar a interrumpir el esquema de seguridad de la información de la nación y, por ende, rebasar a las estructuras de contención, control y vigilancia implementadas por parte del gobierno para tales efectos.

En su contenido, se propone adicionar y reformar diversos preceptos jurídicos del Código Penal Federal, de la Ley General para prevenir, sancionar y erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, del Código Federal de Procedimientos Penales, de la Ley de la Policía Federal y de la Ley Federal de Telecomunicaciones. Ello, con la finalidad de alinear las disposiciones del orden jurídico nacional a las exigencias que impone el avance tecnológico y la condición social actual de nuestro país en materia de delitos cibernéticos.

Características y justificación de las reformas que se proponen

En virtud de las deficiencias, limitaciones y omisiones señaladas en el marco legal, se propone adicionar y reformar el Código Penal Federal, la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, el Código Federal de Procedimientos Penales, la Ley de la Policía Federal y la Ley Federal de Telecomunicaciones, conforme a lo siguiente:

Adiciones y reformas al Código Penal Federal

1. Artículo 139, se considera necesario adicionar como medio para la comisión del delito de terrorismo los sistemas de informática y la red de telecomunicaciones, en virtud del uso que en los últimos años se ha dado al ciberespacio para producir alarma, temor o terror en la población o en un grupo o sector de ella, a fin de atentar en contra de la seguridad nacional o presionar a la autoridad para que tome una determinación. Al efecto, se entenderá por red de telecomunicaciones al sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario, de conformidad con el artículo 3, fracción VIII de la Ley Federal de Telecomunicaciones.

2. Artículo 178 Bis, se propone incluir como sujeto de la conducta delictiva a las comercializadoras de servicios de telecomunicaciones o del concesionario de comunicación vía satélite, al ser ellos quien en un momento dado proporcionan directamente el servicio. Asimismo, se incluyen los delitos contemplados en el Capítulo II del Título Noveno referentes al acceso ilícito a sistemas y equipos de informática, en los cuales hay modificaciones, añadiéndose nuevos tipos penales.

Finalmente, se determina la misma sanción para quienes incumplan de forma inmediata las obligaciones de conservación de tráfico de datos, que se refieren a la duración, fecha, hora, origen y destino de los datos; y de contenido, es decir, la información que se envía. Lo anterior no excluye las sanciones que correspondan por la violación a la secrecía.

3. Artículo 211 Bis 2 y 211 Bis 3, se considera necesario sancionar a quien sin autorización, o contando con ésta, pero de manera indebida, conozca, obtenga, copie o utilice información contenida en sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad nacional, por lo que se adiciona esta hipótesis a la que se encuentra vigente en los artículos en cita con respecto a la información de seguridad pública, toda vez que se trata de bienes jurídicamente tutelados análogos. En consecuencia, se propone adicionar la sanción de inhabilitación o

destitución, según corresponda, para quienes cometan esos delitos y sean o hayan sido servidores públicos de alguna instancia de seguridad nacional.

4. Artículo 211 Bis 7, se propone crear un tipo penal que sancione el simple acceso a un sistema de informática, entendiéndose esto, como el conjunto de actos cometidos en forma dolosa para ingresar a una parte o a la totalidad de una red de telecomunicaciones, sistemas o equipo de informática sin tener la autorización de los legítimos propietarios y/o usuarios.

5. Los actos tipificados deben ser de carácter doloso, pues pueden existir ingresos no autorizados por error, además debe considerarse como agravante el que se realice de manera reiterada.

Los bienes jurídicos tutelados deben ser la violación a los derechos de las personas, a la propiedad privada y a la privacidad.

Adicionalmente, se propone sancionar a quien obtenga un beneficio o lucro indebidos, o bien, perjudique a un tercero, con el uso de información contenida en una red de telecomunicaciones, sistema o equipo de informática, esto es, no sólo prever como delito un acceso indebido a éstos, sino además un mal uso que se dé a la información en ellos contenida.

6. Artículo 211 Bis 8, se considera necesario crear un tipo penal que sancione la interceptación ilícita de datos informáticos, toda vez que en el orden jurídico nacional únicamente se sanciona la intervención de comunicaciones privadas y administrativamente la interceptación de información transmitida por redes públicas de telecomunicaciones. El objeto de esta disposición es proteger el derecho de privacidad de la comunicación de datos.

7. Artículo 211 Bis 9, es necesario crear un tipo penal que sancione los ataques al funcionamiento de sistemas informáticos, cuyo objeto sea tipificar la deliberada afectación de la utilización ilícita de dichos sistemas, toda vez que el Código Penal Federal únicamente sanciona los ataques a la información más no el funcionamiento en sistemas informáticos.

El delito debe ser doloso, ya que el autor debe tener la intención de afectar seriamente el funcionamiento de los sistemas de referencia.

8. Artículo 211 Bis 10, se propone tipificar la posesión, producción, comercialización, importación, difusión, distribución, obtención de un dispositivo o programa informático que no tenga otro propósito que servir para cometer delitos informáticos, el bien jurídico que se busca tutelar es la seguridad pública en general y en particular la informática frente a la creación de instrumentos que solo sirven para amenazar o vulnerar los derechos a la propiedad.

Sin embargo, esta conducta no será punible cuando sea para fines de pruebas autorizadas que en algunas ocasiones se realizan para verificar la vulnerabilidad de un sistema, o de la protección de un sistema informático.

9. Artículo 211 Bis 11, se propone tipificar la falsificación de datos almacenados del usuario sin su consentimiento, con la finalidad de obtener un beneficio o lucro indebido en detrimento de un tercero. Con lo que se busca proteger la seguridad y fiabilidad de los datos electrónicos.

10. Artículo 211 Bis 12, se propone tipificar la producción, reproducción o suplantación de páginas electrónicas, sistema de informática o red de telecomunicaciones con la finalidad de recabar datos personales o del usuario sin consentimiento, la entrada no autorizada provoca una situación que corresponde a la elaboración de un documento falso.

11. Artículo 211 Bis 13, el orden jurídico nacional prevé el tipo penal de fraude informático únicamente en operaciones con instituciones de crédito, según lo establece el artículo 400 Bis por lo que se considera necesario la

creación de un tipo penal que sancione de manera genérica el fraude informático cuyo objetivo es tipificar como delito cualquier manipulación indebida en el curso de tratamiento de datos con la intención de efectuar una transferencia ilegal de la propiedad.

Las manipulaciones en el fraude informático se tipifican como delito cuando se produce una pérdida económica directa o posesión de la propiedad de otra persona y el autor actuó con la intención de obtener una ganancia.

12. Artículo 211 Bis 14, se señalan las reglas aplicables al Capítulo II del Título Noveno, así mismo, define lo que es un sistema de informática, siendo todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí cuya función o la de alguno de sus elementos, sea el tratamiento automatizado de datos de ejecución de un programa.

De igual forma, define que se entiende por datos informáticos, es toda representación de hechos, actos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema de informática ejecute una función.

Finalmente, establece la forma en que se tratará a las personas morales en la comisión de los delitos comprendidos en este Capítulo.

Reforma a la Ley General para prevenir, sancionar y erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos

1. Artículo 17, se propone sancionar penalmente la simple posesión de material de pornografía infantil, en atención al vacío legal al respecto, así como ante la ilicitud justificada de dicha conducta. De igual forma, se propone eliminar de la descripción de la conducta de referencia al arrendamiento, en virtud de que se considera que ya se encuentra incluido en el concepto de adquisición para un tercero.

Adiciones y reformas al Código Federal de Procedimientos Penales

1. Artículo 133 Quáter, brinda el sustento para la obtención de datos informáticos por parte de las empresas concesionarias y permisionarias así como comercializadoras o a los concesionarios de comunicación vía satélite del servicio de telecomunicaciones o de Internet. Además, se considera necesario adicionar a este precepto legal que las investigaciones también abarcan los delitos previstos en el Capítulo II del Titulo Noveno del Código Penal Federal y que la localización geográfica en tiempo real contempla a los datos de tráfico asociados a las comunicaciones vinculadas con la investigación de los delitos contemplados en este artículo.

Incorpora la necesidad de que la solicitud de localización geográfica sea ratificada por un juez federal con posterioridad a la solicitud de la autoridad investigadora.

2. Artículo 278 Ter, es necesario incluir a los delitos informáticos previstos en el Capítulo II del Título Noveno del Código Penal Federal dentro de los supuestos de autorización para la intervención de comunicaciones privadas por parte de la autoridad judicial.

3. Artículo 278 Quáter, los datos históricos del tráfico no están disponibles ya que a menudo el intruso cambia la ruta de comunicación, por lo que la obtención en tiempo real de los mismos es una medida de investigación importante, por lo que se sugiere adicionar este precepto, señalando que la conservación inmediata de datos de tráfico o datos de contenido de alguna comunicación, será por un tiempo máximo de noventa días a partir de la solicitud. Se establecen formalidades que deben observarse en la solicitud.

Asimismo, en un término máximo de doce horas posteriores a la notificación de dicho requerimiento, se deberá presentar una solicitud formal a la autoridad judicial, debidamente fundada y motivada, a efecto de que se determine su procedencia en un tiempo no mayor a veinticuatro horas.

Adiciones y reformas a la Ley de la Policía Federal

1. Artículo 8, fracción XXVIII, en la investigación preventiva como en la instruida por el Ministerio Público, es procedente que el Comisionado General de la Policía Federal o en quienes delegue esta facultad puedan solicitar datos de tráfico y georreferenciación. En la reforma se está delimitando la información que puede solicitar a estos dos aspectos y se faculta expresamente al Comisionado General.

2. Artículo 51, fracción I, inciso o), en la investigación preventiva de los delitos y conforme al marco jurídico vigente procede solicitar una autorización judicial para la intervención de comunicaciones privadas de los delitos informáticos, previstos en el Capítulo II del Título Noveno del Código Penal Federal.

Adiciones y reformas a la Ley Federal de Telecomunicaciones

1. Artículo 40 Bis, se considera necesario contar con una disposición que obligue a los concesionarios de comunicación vía satélite a la conservación de "datos de tráfico de comunicaciones distintas a las telefónicas", incluyendo a los delitos previstos Capítulo II del Título Noveno del Código Penal Federal. Se establece la necesidad de que medie una autorización por parte de una autoridad judicial federal para la procedencia de la medida.

2. Artículo 44 fracciones XIII, XII Bis y XXI, incluye la obligación del concesionario de redes públicas de telecomunicaciones a conservar de forma inmediata datos de contenido de redes públicas, sistemas o equipos de informática hasta por un tiempo máximo de noventa días cuando sea solicitado por el Procurador General de la República o los servidores públicos en quienes delegue la facultad; conservar un registro de datos sobre el tráfico por un periodo de veinticuatro meses; y entregar los datos conservados de los delitos informáticos previstos en el Capítulo II del Título Noveno del Código Penal Federal.

Por lo expuesto, la suscrita diputada Consuelo Argüelles Loya, integrante del Grupo Parlamentario del Partido Acción Nacional, someto a esta honorable Cámara de Diputados en su LXII Legislatura con fundamento en lo dispuesto en los artículos 71, fracción II, y 73, fracción XXI, de la Constitución Política de los Estados Unidos Mexicanos; 55, fracción II, 56 y demás relativos del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos; así como 77 y 78 del Reglamento de la Cámara de Diputados, la siguiente iniciativa con proyecto de

Decreto que adiciona y reforma diversas disposiciones del Código Penal Federal; del Código Federal de Procedimientos Penales; de la Ley General para prevenir, sancionar y erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos; de la Ley de la Policía Federal y de la Ley Federal de Telecomunicaciones, en materia de ciberdelitos

Artículo Primero. Se reforman los artículos **139, 178 Bis, 211 Bis 2 y 211 Bis 3,** se adicionan los artículos**211 Bis 7 al 211 Bis 13,** y se recorre el artículo **211 Bis 7 al 211 Bis 14** y se le adiciona un párrafo, del**Código Penal Federal;** para quedar como sigue:

Artículo 139. Se impondrá pena de prisión de seis a cuarenta años y hasta mil doscientos días multa, sin perjuicio de las penas que correspondan por los delitos que resulten, al que utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, instrumentos que emitan radiaciones, explosivos, armas de fuego; por incendio, inundación o cualquier otro medio violento, realice actos en contra de las personas, las cosas o servicios públicos, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad para que tome una determinación.

...

A quien realice cualquiera de los actos señalados en el primer párrafo de este artículo utilizando sistemas de informática o redes de telecomunicaciones se le impondrá una pena de prisión de seis a veinte años y hasta mil doscientos días multa, sin perjuicio de las penas que correspondan por los delitos que resulten.

Artículo 178 Bis. Al responsable operativo del concesionario, permisionario **o comercializadora** de servicios de telecomunicaciones **o del concesionario de comunicación vía satélite,** que tenga asignada la función de colaborar con las autoridades en la localización geográfica, en tiempo real de los equipos de comunicación, que estén relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas **o cualquiera de los previstos en el Capítulo II del Título Noveno del Código Penal Federal** y que se rehusare a hacerlo de forma dolosa, se le impondrán de doscientos cincuenta a dos mil quinientos días multa.

La misma sanción se impondrá cuando se incumplan las obligaciones de conservación de datos de tráfico o de contenido de forma inmediata, independientemente de la que le corresponda por la violación a la secrecía.

Artículo 211 Bis 2. ...

...

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública **o nacional,** 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 **o nacional,** se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión públicos.

Artículo 211 Bis 3. ...

...

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública o nacional, 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 **o nacional,** 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 7. Al que acceda de manera dolosa y sin autorización a una red de telecomunicaciones, sistema o equipo de informática, se le impondrá una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Cuando el acceso a qué se refiere el párrafo anterior se realice de manera reiterada o en agravio de las instituciones del Estado, la pena se incrementará hasta en una mitad.

Al que sin autorización utilice información contenida en una red de telecomunicaciones, sistema o equipo de informática para la obtención de un beneficio o lucro indebido o para perjudicar a un tercero, se le impondrá una pena de un año a cinco años de prisión y de trescientos a setecientos días multa."

Artículo 211 Bis 8. Al que de manera dolosa por cualquier medio intercepte datos informáticos, se le impondrá una pena de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Cuando la intercepción a que se refiere el párrafo anterior se realice de manera reiterada o en agravio de las instituciones del Estado, la pena se incrementará hasta en una mitad.

Artículo 211 Bis 9. Al que afecte dolosamente por cualquier medio el funcionamiento de un sistema de informática se le impondrá una pena de seis meses a dos años de prisión y de cien a trescientos días multa.

Cuando la afectación a que se refiere el párrafo anterior se realice de manera reiterada o en agravio de las instituciones del Estado, la pena se incrementará hasta en una mitad.

Cuando de la comisión del delito a que se refiere el párrafo anterior resultaren otros delitos, se estará a las reglas del concurso.

Artículo 211 Bis 10. Al que posea, produzca, comercialice, obtenga para su utilización, importe, difunda, distribuya o por cualquier otro medio ponga a disposición, un dispositivo, un programa informático diseñado o adaptado para cometer cualquiera de los delitos tipificados en los artículos 211 Bis 7 a 211 Bis 10 de este Código, o bien, una contraseña, código de acceso o datos informáticos similares que permitan acceder a un sistema de informática, se le impondrá una pena de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Las conductas que se señalan en el párrafo anterior no serán punibles cuando sean para fines de pruebas legítimamente autorizadas o de protección de un sistema de informática.

Artículo 211 Bis 11. Al que genere o introduzca datos falsos en sistemas de informática con la finalidad de que se tengan por auténticos para la obtención de un beneficio o lucro indebido o para perjudicar a un tercero, se le impondrá una pena de dos a cinco años de prisión y de trescientos a setecientos días multa."

Artículo 211 Bis 12. Al que produzca, reproduzca o suplante una página electrónica, sistema de informática o red de telecomunicaciones, con la intención de obtener ilícitamente datos personales o del usuario, se le impondrá una pena de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Artículo 211 Bis 13. Al que valiéndose de cualquier equipo, sistema de informática o red de telecomunicaciones, introduzca, altere, borre o suprima datos informáticos, u obstaculice por cualquier medio el funcionamiento de un sistema de informática para obtener un lucro indebido, se le impondrán las penas previstas en el artículo 386 del presente código.

Artículo 211 Bis 14. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Para efectos del presente capítulo, por sistema de informática se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Para efectos del presente capítulo, por datos informáticos se entenderá toda representación de hechos, actos, información o conceptos expresados de cualquier forma que se preste a tratamiento en un sistema de informática, incluidos los programas diseñados para que un sistema de informática ejecute una función.

Cuando en la comisión de los delitos comprendidos en este capítulo concurran las circunstancias previstas en el artículo 11 de este Código, el juez impondrá a la persona moral de doscientos a cien mil días multa y podrá decretar su suspensión o disolución, tomando en consideración el grado de conocimiento de los órganos de administración respecto de la comisión de alguno de dichos delitos y el daño causado o el beneficio obtenido por la persona moral.

Artículo Segundo. Se reforma el **artículo 17** de la **Ley General para prevenir, sancionar y erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos,** para quedar como sigue:

Artículo 17. Se impondrá pena de 5 a 15 años de prisión y de un mil a 20 mil días multa al que posea, almacene o adquiera para sí o para un tercero, el material a que se refiere el artículo anterior, sin fines de comercialización o distribución.

Artículo Tercero. Se reforman los artículos **133 Quáter y 278 Ter** y se adiciona el artículo **278 Quáter** del**Código Federal de Procedimientos Penales,** para quedar como sigue:

Artículo 133 Quáter. Tratándose de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas **o cualquiera de los previstos en el Capítulo II del Título Noveno del Código Penal Federal,** el Procurador General de la República o el Comisionado General de la Policía Federal, o los servidores públicos en quienes deleguen esta facultad, solicitarán por simple oficio o medios electrónicos a los concesionarios, permisionarios **o comercializadoras** de servicios de telecomunicaciones **o a los concesionarios de comunicación vía satélite,** la localización geográfica, en tiempo real, de los equipos de comunicación, que se encuentren relacionados.

En un término máximo de doce horas posteriores a la notificación de dicho requerimiento, se deberá presentar una solicitud formal ante una autoridad judicial federal, debidamente fundada y motivada, a efecto de que se determine su procedencia en un tiempo no mayor a veinticuatro horas. La autoridad judicial podrá decretar la legalidad de la medida, modificarla o desestimarla de plano, lo que deberá notificarse a los concesionarios, permisionarios o comercializadoras de servicios de telecomunicaciones, o a los concesionarios de comunicación vía satélite para que se continúe o, en su caso, se suspenda su ejecución.

...

...

...

Artículo 278 Ter. Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el procurador general de la República o los servidores públicos en quienes delegue la facultad, la autoridad judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves **o de los delitos previstos en el Capítulo II del Título Noveno del Código Penal Federal.**

...

...

...

...

...

Artículo 278 Quáter. Tratándose de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas o cualquiera de los previstos en el Capítulo II del Título Noveno del Código Penal Federal, el Procurador General de la República o los servidores públicos en quienes delegue la facultad, solicitarán por simple oficio o medios electrónicos a los concesionarios, permisionarios o comercializadoras de servicios de comunicaciones, o a los concesionarios de comunicación vía satélite, la

conservación inmediata de datos de contenido de redes, sistemas o equipos de informática, estando a partir de ese momento obligados a conservarlos hasta por un tiempo máximo de noventa días contados a partir de dicha solicitud. En el oficio de solicitud se deberá indicar específicamente el tipo de datos de contenido que se deberán conservar, la persona o personas a quienes se investiga y el objeto de la medida.

En un término máximo de doce horas posteriores a la notificación de dicho requerimiento, se deberá presentar una solicitud formal a la autoridad judicial, debidamente fundada y motivada, a efecto de que se determine su procedencia en un tiempo no mayor a veinticuatro horas. La autoridad judicial podrá decretar la legalidad de la medida, modificarla o desestimarla de plano, lo que deberá notificarse a los concesionarios, permisionarios o comercializadoras de servicios de telecomunicaciones, o a los concesionarios de comunicación vía satélite para que se continúe o, en su caso, se suspenda su ejecución.

Los concesionarios permisionarios o comercializadoras de servicios de telecomunicaciones o los concesionarios de comunicación vía satélite, tendrán la obligación de guardar en total secrecía la medida requerida.

Artículo Cuarto. Se reforma la **fracción XXVIII del artículo 8** y se adiciona **el inciso o) a la fracción I del artículo 51 de la Ley de la Policía Federal,** para quedar como sigue:

Artículo 8. La Policía Federal tendrá las atribuciones y obligaciones siguientes:

I. a XXVII. ...

XXVIII. **El comisionado general de la Policía Federal, o en quien delegue esa función;** podrá solicitar por escrito, previa autorización de un juez a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones de sistemas de comunicación vía satélite, **los datos de tráfico** con que cuenten, así como georreferenciación, de los equipos de comunicación móvil en tiempo real **y de las direcciones de protocolos de Internet,** para el cumplimiento de sus fines de prevención, **persecución y combate de los delitos.** La autoridad judicial competente, deberá acordar la solicitud en un plazo no mayor de doce horas a partir de su presentación;

Artículo 51. La intervención preventiva de comunicaciones a que se refiere esta Ley, se autorizará únicamente en los delitos previstos en los ordenamientos legales que a continuación se enlistan:

I. Del Código Penal Federal:

...

o) Capítulo II del Título Noveno del Código Penal Federal

II. a V. ...

Artículo Quinto. Se reforman los artículos **40 Bis, 44, fracción XIII,** y se adicionan **las fracciones XIII Bis y XXI del artículo 44 de la Ley Federal de Telecomunicaciones,** para quedar como sigue: **Artículo 40 Bis.**Los concesionarios, permisionarios o comercializadoras de servicios de telecomunicaciones, y los concesionarios de comunicación vía satélite, están obligados a colaborar con las autoridades en la localización geográfica, en tiempo real, de los equipos de comunicación, y a la conservación inmediata de datos de tráfico o datos de contenido que se encuentren relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas o cualquiera de los previstos en el Capítulo II del Título Noveno del Código Penal Federal, o de los mencionados en el artículo 51 de la Ley de la Policía Federal, a solicitud del Procurador General de la República, Comisionado General de la Policía Federal, , de los procuradores de las entidades federativas o de los servidores públicos en quienes deleguen esta facultad, de conformidad con las leyes correspondientes.. Dicha

medida deberá ser decretada como legal con posterioridad por una autoridad judicial, de conformidad con las leyes correspondientes mediante oficio que notificarán a su vez a los sujetos obligados.

...

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

I. a **XII.** ...

XIII. Entregar los datos conservados, al Procurador General de la República o Procuradores Generales de Justicia de las entidades federativas, cuando realicen funciones de investigación de los delitos de extorsión, amenazas, secuestro, en cualquiera de sus modalidades, **cualquiera de los previstos en el capítulo II del Título Noveno del Código Penal Federal,** o de algún delito grave o relacionado con la delincuencia organizada, en sus respectivas competencias.

...

...

...

XIII Bis. Conservar un registro de datos sobre el tráfico por un periodo de veinticuatro meses, contados a partir de la fecha en que se haya establecido la conexión.

Para efectos de la presente fracción, por datos sobre el tráfico se entenderá todos los datos relativos a una conexión o comunicación electrónica realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación o conexión y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

XIV. a XX. ...

XXI. Conservar de forma inmediata datos de contenido de redes públicas, sistemas o equipos de informática hasta por un tiempo máximo de noventa días cuando sea solicitado por el Procurador General de la República o los servidores públicos en quienes delegue la facultad.

Transitorios

Primero. El presente decreto entrará en vigor 90 días después de su publicación en el Diario Oficial de la Federación.

Segundo. Todas las disposiciones que contravengan la presente deberán reformarse en un plazo no mayor a 60 días después de su publicación.

Notas

1 Fundada en el año 2002 como un punto de encuentro neutral para especialistas en seguridad y defensa de la Organización del Tratado del Atlántico Norte y la Unión Europea. Desde entonces se ha convertido en un importante foro para la discusión de políticas de seguridad y defensa, con el objeto de generar la reflexión de los gobiernos para la previsión de una agenda política que atienda los retos relacionados con dichos temas en sus Estados. Entre otras actividades, ha desarrollado consultas de opinión a nivel mundial sobre temas de seguridad.

2 Publicado en Bruselas el 31 de enero de 2012, basado en entrevistas con expertos y políticos de instituciones de la Unión Europea, la Organización del Tratado del Atlántico Norte, gobiernos nacionales, industria, medios de

comunicación, *think-tanks* , universidades y organizaciones no gubernamentales, participantes y responsables de políticas en la materia.

3 Punto de acuerdo propuesto por el diputado Rodrigo Pérez-Alonso, del Partido Verde Ecologista de México y publicado en la Gaceta número 10 del Senado de la República, el 7 de julio de 2010.

México, Distrito Federal, Palacio Legislativo de San Lázaro, a 16 de abril de 2013.

Diputados: Consuelo Argüelles Loya (rúbrica), José Alejandro Montano Guzmán