CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

Gaceta Parlamentaria

Año XXI	Palacio Legislativo de San Lázaro, jueves 26 de abril de 2018	Número 5013-XXII

CONTENIDO

Anexo XII

Jueves 26 de abril

DICTAMEN DE LA COMISIÓN DE JUSTICIA, A LA INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL Y DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES

HONORABLE ASAMBLEA:

A la Comisión de Justicia de la Cámara de Diputados del H. Congreso de la Unión de la LXIII Legislatura, le fue turnada una iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, presentada por la Diputada Sofía González Torres, integrante del Grupo Parlamentario del Partido Verde Ecologista de México y el Diputado Waldo Fernández González del Grupo Parlamentario del Partido de la Revolución Democrática.

Con fundamento en los artículos 71 y 72 de la Constitución Política de los Estados Unidos Mexicanos, 39; 43, 44, y 45 numeral 6, incisos e) y f) de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; 80, 81, 82, 84, 85 y 157 numeral 1, fracción I, 158 numeral 1, fracción IV y 167 del Reglamento de la Cámara de Diputados, los miembros de esta Comisión de Justicia sometemos a consideración del Pleno de esta Honorable Asamblea el presente dictamen al tenor de la siguiente:

M E T O D O L O G Í A

Esta Comisión, desarrolló los trabajos correspondientes conforme al procedimiento que a continuación se describe:

I. En el apartado **"ANTECEDENTES"** se indica la fecha de recepción en el Pleno de la Cámara de Diputados y del turno recibido en la Comisión de Justicia para su análisis y dictaminación.

II. En el apartado denominado **"CONTENIDO DE LA INICIATIVA"** se resume el objetivo de la iniciativa que nos ocupa.

III. En el apartado **"CONSIDERACIONES"**, las y los integrantes de esta Comisión dictaminadora, expresamos los razonamientos y argumentos con base en los cuales se sustenta el sentido del presente dictamen.

I. ANTECEDENTES

1. Con fecha 14 de noviembre de 2017, la Diputada Sofía González Torres, integrante del Grupo Parlamentario del Partido Verde Ecologista de México y el Diputado Waldo Fernández González del Grupo Parlamentario del Partido de la Revolución Democrática, presentaron una Iniciativa con proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, la cual fue suscrita por los Diputados integrantes del Grupo Parlamentario del Partido Verde Ecologista de México, así como de los Diputados Martha Sofía Tamayo Morales, Alfredo Anaya Orozco, Armando Luna Canales, Francisco Saracho Navarro, Adolfo Mota Hernández y Felipe Cervera Hernández, del Grupo Parlamentario del Partido Revolucionario Institucional; Hernán Cortés Berumen, José Máximo García López, Kathia María Bolio Pinelo, Juan Corral Mier,

Víctor Ernesto Ibarra Montoya y Luis Agustín Rodríguez Torres, del Grupo Parlamentario del Partido Acción Nacional; y Sara Paola Gálico Félix Díaz del Grupo Parlamentario de Movimiento Regeneración Nacional.

En la misma fecha, para su estudio, análisis y dictamen correspondiente, la Presidencia de la Mesa Directiva de la Cámara de Diputados, determinó el turno de la Iniciativa de referencia a la Comisión de Justicia para dictamen y a la Comisión Especial de Tecnologías de Información y Comunicación para opinión.

2. Con fecha __ de Diciembre de 2017, la Comisión Especial de Tecnologías de la Información y Comunicación entregó a esta Comisión de Justicia, la Opinión en Sentido Positivo respecto a la Iniciativa materia del presente Dictamen, misma que se anexa copia, dando cumplimiento a lo dispuesto por el numeral 5 del artículo 69 del Reglamento de la Cámara de Diputados.

II. CONTENIDO DE LA INICIATIVA

La Iniciativa presentada por los Diputados Sofía González Torres y Waldo Fernández González para reformar y adicionar diversas disposiciones al Código Penal Federal y Código Nacional de Procedimientos Penales, consiste en fortalecer el andamiaje jurídico en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, misma que sustentan bajo la siguiente argumentación:

Los Iniciantes destacan la importancia que trae consigo el avance tecnológico en la vida cotidiana del ser humano, marcada por el encuentro de diferentes desarrollos y su transversalidad, la Cuarta Revolución Industrial representa un cambio de paradigmas. Sus principales motores son la digitalización, la robótica, el internet de las cosas y la conexión entre dispositivos, así como la creación de redes de datos y

sistemas que se encuentran cada vez más integradas entre sí y con los usuarios, a través de un sin fin de dispositivos.

Exponen que gracias a esta Revolución Digital se han establecido nuevos sistemas en torno a casi cualquier aspecto de la vida cotidiana, se crean nuevos sistemas de negocios como la economía colaborativa, el internet de las cosas, los sistemas ciberfísicos, el "cloud computing" o "nube". Esta revolución es tan importante, que fue el centro de las conferencias del Foro Económico Mundial en enero de 2017.

A la par de estas trasformaciones, los Diputados proponentes destacan que el aspecto de derechos humanos juega un papel fundamental en el desarrollo de una política de Estado en materia de ciberseguridad y concretamente en materia de combate a los cibercrímenes. En los umbrales de las sociedades de la información, en donde las tecnologías de la información y la comunicación juegan un papel de primer orden, el acceso a las mismas es reconocido ya como un derecho fundamental por diversos Estados, formando una suerte de *Soft Law* dentro de la Comunidad Internacional de Naciones. Nuestra propia Constitución Política también reconoce este derecho, colocándolo, junto con la reforma constitucional de derechos humanos de 2011, a la vanguardia regional e internacional en materia de derechos humanos.

Mencionan que en la teoría de los derechos fundamentales todo ejercicio de un derecho conlleva responsabilidades. Por ejemplo, es importante garantizar que con dicho ejercicio no se afecte injustificadamente la esfera normativa de otro sujeto. A lo anterior deben sumarse los grandes riesgos que un uso no compatible con los derechos humanos de las tecnologías de la información y comunicación puede tener y que se ha visto continuamente en casos como los que se están regulando a través de esta iniciativa.

La Diputada González Torres argumenta que, conforme a nuestra Constitución y los Tratados Internacionales en la materia, determinados derechos fundamentales pueden ser objeto de una atenuación en sus modalidades de ejercicio y ello con el único propósito de tutelar otro derecho fundamental o un valor que se estima de gran intensidad dentro de un Estado constitucional y democrático de derecho que, ante el caso concreto, sólo puede asegurarse su protección mediante la toma de medidas inmediatas que, incluso, pueden interferir con el pleno ejercicio de otros derechos. Para garantizar lo anterior, cuando el ejercicio de un derecho humano interfiere en la esfera jurídica de otros derechos de orden primordial de otros sujetos, se requiere la adopción de medidas dirigidas al logro de un equilibrio, de un balance (balancing, según lo llama la tradición anglosajona) a fin de que todos puedan disfrutar del ejercicio pleno de dichos derechos.

Para fundamentar la creación de estos tipos penales los legisladores hacen referencia a que, comprendiendo los alcances y retos de un mundo interconectado, a principios de este siglo la Unión Europea puso en marcha una serie de políticas públicas con el objetivo de bridar mayor seguridad a sus ciudadanos en el ciberespacio y la red. Como resultado de estas iniciativas, en el 2001 se redactó el Convenio de Budapest sobre Ciberdelincuencia elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China. Este es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales de los países miembros de la Unión Europea, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones europeas.

Destacan que su principal objetivo consiste en aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Este Convenio dio la pauta sobre la clasificación y tipificación de

delitos de base cometidos por medio de herramientas electrónicas y el Internet. Sin embargo, dados los rápidos avances tecnológicos, algunos países se han visto en la necesidad de modificar y actualizar sus leyes e incluso, en algunos casos, de crear agencias para la protección de sus ciudadanos y sus datos personales en el ciberespacio.

Reconocen que si bien México aún no forma parte del Convenio de Budapest, es indispensable crear un ambiente propicio para la cooperación internacional en materia de ciberseguridad, ya que para prevenir y mitigar los riesgos que implica una navegación no protegida en la red debemos entender que el ciberespacio es un mundo sin fronteras y la forma adecuada de prevenir ataques internos y/o externos es por medio de una legislación dinámica y contando con cooperación internacional fluida con buenos canales de comunicación. Por esto es indispensable dotar de lineamientos legales precisos a nuestras autoridades para perseguir a los criminales que utilizan las tecnologías de la información y comunicación como herramientas para la comisión de ilícitos.

Los Iniciantes afirman que, en el caso concreto de su propuesta legislativa, no se incluye ninguna restricción al ejercicio del derecho a la libertad de expresión o de acceso a internet, al contrario, el espíritu de la misma consiste en garantizar el pleno ejercicio de los derechos humanos en el uso de las tecnologías de la información y comunicación, a fin de armonizar plenamente los derechos fundamentales de todos y cada uno de los ciudadanos.

Finalmente, los Diputados proponentes concluyen diciendo que la falta de un marco jurídico adecuado para hacer frente a todas las amenazas que día a día se descubren con el uso de las tecnologías de la información y comunicación marcan la necesidad de adecuar la legislación vigente para lograr prevenir, sancionar y contrarrestar todas aquellas conductas que dañen los bienes de las personas y la

infraestructura nacional o el actuar y la estabilidad de las instituciones del Estado, por lo que un marco regulatorio debe considerarse como urgente y necesario para dar un paso considerable a fin de hacer frente a estas amenazas.

III. C O N S I D E R A C I O N E S

P R I M E R A.- Quienes integramos la Comisión de Justicia de este Órgano Legislativo, examinamos de manera minuciosa el contenido de la Iniciativa presentada, haciendo un estudio de la legislación vigente, tomando en todo momento como base, que la propuesta de reforma estuviera armonizada con la legislación nacional aplicable en la materia, así como en los estándares internacionales ratificados por el Estado mexicano en uso de su soberanía.

En atención de lo anterior, las presentes Consideraciones buscan analizar de forma puntual y precisa las propuestas de reforma planteadas por los legisladores iniciantes, utilizando como métodos el interpretativo, el analítico, el deductivo y el funcional, de manera que ello permita tomar una determinación acerca de la viabilidad o inviabilidad de cada una de las mencionadas propuestas.

Las diputadas y los diputados integrantes de esta Comisión de Justicia, compartimos plenamente la intención de los diputados proponentes, ya que con su Iniciativa se busca perfeccionar el marco jurídico penal en materia de ciberseguridad. Necesitamos desarrollar una política de Estado en esta materia, esto con el fin de garantizar la protección de los derechos fundamentales de los usuarios y los intereses económicos y políticos de nuestro país en el ciberespacio.

S E G U N D A.- Las diputadas y los diputados integrantes de la Comisión de Justicia reconocemos los esfuerzos que desde este Poder Legislativo se ha ido avanzando en el uso de las tecnologías de la información y comunicación. Como bien lo manifiestan los Diputados González Torres y Fernández González, la reforma constitucional en materia de telecomunicaciones, publicada en el Diario Oficial de la Federación el 11 de junio de 2013, reconoció y elevó a rango constitucional el derecho humano al internet, incluyéndolo en el artículo 6º de nuestra Norma Fundamental.

De igual modo, y habilitando la competencia de los legisladores federales en la materia, la reforma constitucional en materia de telecomunicaciones facultó al Congreso de la Unión "para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal."

Es importante destacar que, durante el Proceso Legislativo seguido en esta reforma, el Derecho Humano al internet fue reconocido una pluralidad de veces, así, se indicó que:

> "Es obligación del Estado garantizar el acceso a la información a través de diversos medios, como los tecnológicos. En la Asamblea de la Organización de las Naciones Unidas, llevada a cabo el 1 de junio del 2011, se expuso que el acceso a las tecnologías de la información y de la comunicación, es un derecho fundamental, por ser una herramienta que favorece el crecimiento y el progreso de la sociedad en conjunto. Si el Estado mexicano tiene activos suficientes para emprender un proyecto que pueda culminar a corto o mediano plazo con la prestación gratuita del servicio de internet a todos los mexicanos, lo propio sería establecer con claridad y de manera contundente que el Estado garantizará plenamente el derecho de acceso universal a los servicios de banda ancha...

> ... la competencia económica y las telecomunicaciones tiene relación directa con el derecho al desarrollo, derecho humano de tercera generación (de interés colectivo), el cual está íntimamente relacionado con el debido desarrollo de la economía de los Estados... Así pues, el derecho humano al desarrollo implica el respeto de todos los agentes públicos y privados en materia económica del bienestar social, de tal forma que todas sus actuaciones abonen al desarrollo social, y no menoscaben el derecho de los ciudadanos, de tal forma que su aprovechamiento implique el desarrollo económico de la sociedad, y con ello, el propio desarrollo civil y político."[1]

Como se destaca en los anteriores argumentos, ha sido primeramente desde la Comunidad Internacional de Estados donde el derecho humano al internet se ha gestado, como parte del derecho fundamental al desarrollo. Naciones Unidas, desde 1986, en la Declaración sobre el Derecho al Desarrollo indicaba:

> "**Artículo. 1.**
>
> **1.** El derecho al desarrollo es un derecho humano inalienable en virtud del cual todo ser humano y todos los pueblos están facultados para participar en un desarrollo económico, social, cultural y político en el que puedan realizarse plenamente todos los derechos humanos y libertades fundamentales, a contribuir a ese desarrollo y a disfrutar de él.
>
> **Artículo 2.**
>
> 1. La persona humana es el sujeto central del desarrollo y debe ser el participante activo y el beneficiario del derecho al desarrollo.
> 2. Todos los seres humanos tienen, individual y colectivamente, la responsabilidad del desarrollo, teniendo en cuenta la necesidad del pleno respeto de sus derechos humanos y libertades fundamentales, así como sus deberes para con la comunidad,

[1] Proceso Legislativo, Decreto por el que se reforman y adicionan diversas disposiciones de los artículo 6°., 7°., 27, 28, 73, 78, 94 y105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/proceso/cpeum/CPEUM_208_DOF_11jun13.zip

único ámbito en que se puede asegurar la libre y plena realización del ser humano, y, por consiguiente, deben promover y proteger un orden político, social y económico apropiado para el desarrollo.

3. Los Estados tienen el derecho y el deber de formular políticas de desarrollo nacional adecuadas con el fin de mejorar constantemente el bienestar de la población entera y de todos los individuos sobre la base de su participación activa, libre y significativa en el desarrollo y en la equitativa distribución de los beneficios resultantes de éste."

Asimismo, el Artículo 26 de la Convención Americana de Derechos Humanos dispone que:

"Artículo 26. Desarrollo Progresivo

Los Estados Partes se comprometen a adoptar providencias, tanto a nivel interno como mediante la cooperación internacional, especialmente económica y técnica, para lograr progresivamente la plena efectividad de los derechos que se derivan de las normas económicas, sociales y sobre educación, ciencia y cultura, contenidas en la Carta de la Organización de los Estados Americanos, reformada por el Protocolo de Buenos Aires, en la medida de los recursos disponibles, por vía legislativa u otros medios apropiados."

Más tarde, Naciones Unidas, por vía del Consejo de Derechos Humanos, ha señalado:

"Observando que el ejercicio de los derechos humanos, en particular del derecho a la libertad de expresión, en Internet es una cuestión que reviste cada vez más interés e importancia debido a que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones

...

Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración

> Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.
> Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;
> Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;
> ...
> Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos..."[2]

Bajo los argumentos anteriores puede constatarse plenamente como el acceso al internet ha sido reconocido como un derecho humano. Ciertamente aún no se encuentra consagrado plenamente dentro de un Tratado o Convención Internacional sujeta a ratificaciones por los Estados, más si en las diversas resoluciones, informes, observaciones generales y demás, de la Comunidad Internacional que hacen del mismo un derecho blando o *soft law*. No obstante ello, y como hemos comentado, nuestro país se coloca a la vanguardia al reconocer el acceso al internet como un derecho fundamental desde el texto constitucional, dentro del artículo 6º.

El mayor avance en las comunicaciones ha logrado, por un lado, que nuevos instrumentos puedan ser utilizados como vehículos o mecanismos para la maximización de derechos y en el caso de las tecnologías de la información y comunicación vemos una insuperable herramienta mediante la cual puede maximizarse el derecho fundamental a la libre expresión, al acceso a la información,

[2] Consejo de Derechos Humanos. 20º periodo de sesiones, 29 de junio de 2012. Documento: A/HRC/20/L.13, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

a la educación, la cultura, el trabajo, la salud, por citar solo algunos ejemplos. Por otra parte, esta gran maximización de poder conlleva consigo ciertas responsabilidades y ciertas modalidades que habrán de tomarse para garantizar que el pleno ejercicio de los derechos de las personas pueda armonizarse también con la plena tutela de los derechos fundamentales de todos los ciudadanos.

Como resultado, a 4 cuatro años de la reforma en materia de telecomunicaciones, México ha visto un incremento de 25 millones de usuarios de internet y 20 millones de usuarios de telefonía móvil. Esto no solo representa un tema de infraestructura crítica para el país, sino que también nos habla del enorme mundo de posibilidades y acceso a una economía y comercio digital nunca antes visto en México.

T E R C E R A.- Los esfuerzos por contar con un México Ciberseguro se encuentra reflejado en todas las acciones de gobierno que, desde su ámbito de competencia, el Estado Mexicano está realizando actualmente. Es así que, desde el Poder Ejecutivo se incluyó a este tema dentro de sus acciones prioritarias en el Plan Nacional de Desarrollo 2013-2018, el cual contiene el fortalecimiento de las capacidades institucionales en el ciberespacio y la ciberseguridad como uno de los puntos esenciales de la Seguridad Nacional, destacando que "es necesario apuntar que esta Administración trabajará activamente en el desarrollo y actualización del marco jurídico en materia de seguridad de la información y ciberdefensa, así como en materia de prevención, investigación y sanción de **delitos cibernéticos**, a fin de responder a estándares de excelencia y mejores prácticas internacionales…".

Este compromiso de gobierno ha tenido sus frutos con la reciente creación de la Estrategia Nacional de Ciberseguridad[3] la cual para cumplir con el objetivo general

[3] https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf consultada el 27 de Noviembre de 2017.

que consiste en es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano, se establecen 5 objetivos estratégicos:

1. Sociedad y derechos.

2. Economía e innovación.

3. Instituciones públicas.

4. Seguridad pública.

5. Seguridad nacional.

Para alcanzar los objetivos estratégicos se desarrollarán 8 ejes transversales, entre los que destaca es el punto "7. Marco jurídico y autorregulación". Es de destacar que, para la construcción de esta Estrategia se contó con la participación del Poder Legislativo, concretamente con la colaboración de la Diputada González Torres, Diputada proponente de la Iniciativa. Para desarrollar este eje se necesita de la estrecha colaboración de este Congreso de la Unión, mismo que, desde este órgano legislativo nos sumamos para contribuir a fortalecer la Ciberseguridad de México.

CUARTA.- Para los integrantes de esta Comisión de Justicia nos resulta importante legislar en materia de Ciberseguridad. Como lo mencionan los Iniciantes, las cifras sobre el universo de mexicanos que hacen uso de las tecnologías de la información y comunicación constituyen un nicho social importante para poner en el centro de atención este tema que es hoy en día, un elemento fundamental para la Seguridad y Protección de las Instituciones. Esto se ve reflejado en la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares, realizada

por el Instituto Nacional de Estadística y Geografía en 2016, la cual reveló que en nuestro país existen 81 millones de usuarios de un teléfono celular. Y de ellos, 60.6 millones utilizan un teléfono inteligente o smartphone, lo cual significa un incremento de 9.7 puntos porcentuales entre 2015 y 2016.

Por su parte, Naciones Unidas estimó, para febrero de 2015, una cantidad de 3000 millones de usuarios de internet, lo que corresponde a cerca del 40% de la población mundial. Además, el acceso al internet se da predominantemente entre la población joven del país, pues se registra que entre los 12 y 17 años, el 80% de la población se declaró usuaria de internet en 2014. En el caso de los niños menores de 12 y mayores de 6 años, el acceso es del 42.2% de la población, siendo también un dato significativo.[4]

Estos datos nos revelan un panorama de gran interés pues demuestran el acceso al internet por diversos sectores de la población, resultando evidente que la mayor parte de la población que accede al mismo, se ubica en rangos de edades inferiores a los 18 años y que, en el caso de los menores de 12 y mayores de 6, el porcentaje se eleva a casi el 50% de la población.

Sin lugar a dudas, no dejamos de reconocer que el internet ha sido uno de los más grandes inventos de la humanidad y que, su uso, ha venido a transformar radicalmente las formas de vida contemporáneas, haciendo más fácil muchas actividades que hasta hace poco requerían de gran empeño. No obstante, el uso del internet también conlleva sus responsabilidades (o al menor, debería de conllevarlas).

Ciertamente, por un lado, el internet se constituye como la herramienta más importante para la información y la comunicación, y es reconocido incluso como un

[4] ONU. "Seminario 3: el Fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional." Documento A/CONF.222/12.

derecho fundamental, pero por el otro lado, también ha traído aparejado diversos problemas al ser utilizado por sujetos con fines diversos a los de un sano intercambio de información entre los usuarios, todo esto en un anonimato incierto.

A la par de estos avances, es claro que el aumento de riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos.

Como exponen los iniciantes, las actividades ilícitas en el dominio digital se han vuelto cada vez más comunes y en el año 2013 le costaron a la economía mexicana 3 mil millones de dólares. El costo promedio por víctima aumentó de 197 a 238 dólares, entre 2012 y 2013. En el 2014, 10 millones de mexicanos fueron afectados por cibercrímenes y en 2016, de acuerdo al reporte de Ciberseguridad de la empresa de Norton, 689 millones de personas fueron víctimas de algún ciberdelito alrededor del mundo, de las cuales 22.4 millones fueron ciudadanos mexicanos. En el mismo reporte se calcula que el costo de los cibercrimenes en los 21 países analizados fue de cerca de 126 mil millones de dólares, de los cuales 5.5 mil millones se obtuvieron como resultado de crímenes cometidos en nuestro territorio. Por último, Norton identificó que las causas de los cibercrímenes más recurrentes en México fueron: robo de equipo celular (33%); falta de contraseñas seguras (26%); y correos hackeados (20%).

A estas alarmantes cifras podemos sumar los números que la Organización de Estados Americanos da a conocer en su reporte "Tendencias de seguridad en

América Latina y el Caribe[5]" donde establece que, en términos económicos, el cibercrimen le cuesta al país entre 3,000 y 5,000 1 millones de dólares al año.

Por su parte, el Modelo de Madurez de Capacidad de Seguridad Cibernética desarrollado en el estudio Informe Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?[6] realizado por el Banco Interamericano de Desarrollo donde señala que el cibercrimen le cuesta al mundo hasta US$575,000 2 millones al año, lo que representa 0.5 por ciento del producto interno bruto global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90,000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región.

Quienes integramos la Comisión de Justicia estamos ciertos que, si bien el uso de las tecnologías de la información y comunicación constituyen un medio para la libre expresión y manifestación de las ideas, también debemos señalar que estos medios son utilizados para cometer ataques en contra de personas e instituciones, vulnerando los derechos humanos de los usuarios y poniendo en peligro su privacidad y datos personales. Para ello, resulta necesario generar y poner en marcha una estrategia que evite afectaciones a las capacidades nacionales de comunicación y a la funcionalidad de los sistemas estratégicos de información.

Q U I N T A.- Para esta Comisión Dictaminadora, tenemos claro la premisa de generar las condiciones necesarias para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar

---

[5] https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf consultado en octubre 2017.

[6] https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/ consultado en octubre 2017.

su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros. Asimismo, tenemos presente la premisa que conduce la teoría de los derechos fundamentales, en el sentido de que todo ejercicio de un derecho fundamental conlleva responsabilidades y una de ellas es el que, con el ejercicio de un derecho no se afecte injustificadamente la esfera normativa de derechos fundamentales de otro sujeto.

Esto nos conduce ante los umbrales de las modalidades en las que determinados derechos pueden ser objeto de una atenuación en su ejercicio, con el único propósito de tutelar otro derecho fundamental o un valor que se estima de gran intensidad dentro de un Estado constitucional y democrático de derecho que, ante el caso concreto del estudio de viabilidad de la propuesta de los Diputados, sólo puede asegurarse su protección mediante la toma de medidas inmediatas que, incluso, pueden interferir con el pleno ejercicio de otros derechos. Para ello, se requiere la adopción de medidas dirigidas al logro de un equilibrio, de un balance (la tradición anglosajona lo llama balancing) a fin de que todos puedan disfrutar de sus derechos fundamentales.

En consecuencia, toda decisión pública por la que el ejercicio de un derecho puede estar sometida a alguna restricción o modalidad en su ejercicio, no puede ser arbitraria. Debe claramente estar justificada y motivada y ser proporcional entre la medida a adoptar y el riesgo presente, así como la justificación de la necesidad e idoneidad de la medida a emprender, así lo ha señalado la Corte Interamericana de Derechos Humanos en su sentencia del 23 de junio de 2005. Serie C. No. 127. Párrafo 206, en el caso Yatama Vs. Nicaragua donde argumento lo siguiente:

> *"La restricción debe encontrarse prevista en una ley, no ser discriminatoria, basarse en criterios razonables, atender a un propósito útil y oportuno que la torne necesaria para satisfacer*

un interés público imperativo, y ser proporcional a ese objetivo. Cuando hay varias opciones para alcanzar ese fin, debe escogerse la que restrinja menos el derecho protegido y guarde mayor proporcionalidad con el propósito que se persigue"

Por su parte, la Segunda Sala de la Suprema Corte de Justicia de la Nación se ha pronunciado por una restricción mínima pero necesaria, a fin de salvaguardar el ejercicio pleno de estos derechos para todos. En la tesis 2a. CII/2017 (10a.) materia constitucional publicada el viernes 16 de junio de 2017 a las 10:22 horas en el Semanario Judicial de la Federación, el Ministro Ponente Alberto Pérez Dayán fijo el siguiente criterio judicial:

"FLUJO DE INFORMACIÓN EN RED ELECTRÓNICA (INTERNET). PRINCIPIO DE RESTRICCIÓN MÍNIMA POSIBLE. *Atento a la importancia de las nuevas tecnologías de la información y la comunicación que permiten la existencia de una red mundial en la que pueden intercambiarse ideas y opiniones, conforme a lo sostenido por el Comité de Derechos Humanos de la Organización de las Naciones Unidas, el Estado debe tomar todas las medidas necesarias para fomentar la independencia de esos nuevos medios y asegurar a los particulares el acceso a éstos, pues precisamente el intercambio instantáneo de información e ideas a bajo costo, a través del Internet, facilita el acceso a información y conocimientos que antes no podían obtenerse lo cual, a su vez, contribuye al descubrimiento de la verdad y al progreso de la sociedad en su conjunto, a lo que se debe que el marco del derecho internacional de los derechos humanos siga*

siendo pertinente y aplicable a las nuevas tecnologías de la comunicación; de hecho, puede afirmarse que el Internet ha pasado a ser un medio fundamental para que las personas ejerzan su derecho a la libertad de opinión y de expresión, atento a sus características singulares, como su velocidad, alcance mundial y relativo anonimato. Por tanto, en atención a ese derecho humano, se reconoce que en el orden jurídico nacional y en el derecho internacional de los derechos humanos, existe el principio relativo a que el flujo de información por Internet debe restringirse lo mínimo posible, esto es, en circunstancias excepcionales y limitadas, previstas en la ley, para proteger otros derechos humanos." (subrayado propio)

Por lo tanto, realizando un análisis a la propuesta de la Diputada Sofía González Torres y el Diputado Waldo Fernández González mediante el sustento de criterios judiciales de la más alta calidad jurídica, esta Comisión Dictaminadora puede afirmar que la misma no se incluye ninguna restricción al ejercicio del derecho humano de acceso a internet o al uso de las tecnologías de la información y comunicación, sino más bien una modalidad en su ejercicio, esto con el fin de armonizar plenamente los derechos fundamentales de todos y cada uno de los individuos a los que también debe garantizar el pleno acceso al derecho al internet.

S E X T A.- Para realizar un análisis exhaustivo acerca de si esta Iniciativa es viable y acorde con los derechos humanos o que nos encontramos ante posibles colisiones de derechos, este órgano legislativo dictaminador considera necesario realizar un análisis de ponderación para tratar de determinar a cuál de los derechos en juego habrá que darle preferencia. No obstante, previo a ello, habrá que buscarse por

todos los medios de armonizar el ejercicio de los derechos en posible colisión a fin de no realizar restricción alguna en el ejercicio de ambos. Sólo cuando exploradas todas las alternativas no se encuentra medida alguna que pueda armonizar los derechos, podrá optarse por la ponderación, pero bajo determinados requisitos.

En toda decisión pública por la que el ejercicio de un derecho puede estar sometida a alguna restricción o modalidad en su ejercicio, no puede ser arbitraria. Debe claramente estar justificada y motivada y ser proporcional entre la medida a adoptar y el riesgo presente, así como la justificación de la necesidad e idoneidad de la medida a emprender. Es por ello que, como se ha expuesto en las consideraciones anteriores, ante las alarmantes cifras y el estado de vulnerabilidad que tenemos en nuestro país en materia de ciberseguridad y protección del espacio cibernético constituyen un hecho notorio para legislar de manera urgente sobre estos delitos, mismos que lesionan seriamente los derechos humanos en el uso de las tecnologías de la información y comunicación.

Entrando en materia, el principio de proporcionalidad, desarrollado ampliamente por Robert Alexy y, siendo uno de los métodos de interpretación más utilizados por las Altas Cortes en el mundo contemporáneo, comprende los subprincipios de idoneidad, necesidad y proporcionalidad (stricto sensu).

La idoneidad se refiere a que la medida a emprender sea la conducente para conseguir el valor o la finalidad protegida mediante la restricción del valor en conflicto.[7]

[7] Tribunal Electoral del Poder Judicial de la Federación. *Recurso de consideración. Expediente: SUP-REC-41/2013.* Resolución del 26 de junio de 2013.

La necesidad se refiere a que la medida a adoptar responda a una apremiante necesidad social, o bien, que no sea posible alcanzar el fin buscado con la restricción, por otros mecanismos.[8]

La proporcionalidad en sentido estricto se refiere a la constatación de que la norma que otorga el trato diferenciado guarde una relación razonable con el fin que se procura alcanzar, lo que supone una ponderación entre sus ventajas y desventajas, a efecto de comprobar que los perjuicios ocasionados no sean desproporcionados con respecto a los objetivos perseguidos, lo cual implica que si existe una alternativa menos gravosa para conseguir el fin buscado, debe emplearse dicha alternativa.[9]

En el caso concreto de esta iniciativa, esta Comisión Dictaminadora coincide con el análisis hecho por los Iniciantes, al introducir un catálogo de delitos cometidos en el ciberespacio y perfeccionar otros tipos penales, estas propuestas cumplen con el Test de Proporcionalidad, en tanto que la medida que proponen incluir en la norma sustantiva y adjetiva en materia penal resulta ser idónea y necesaria, pues con ella puede tenerse certeza respecto de aquellos casos en los que alguien pudiera vulnerar los derechos humanos de otra persona, pero se le respeta su derecho de acceso al uso de las tecnologías de la información y comunicación sin censura previa ni restricción alguna y sin una intervención directa por parte del Estado que pueda vulnerar su esfera de libertades.

Además, se cumple con el principio de necesidad en tanto que, existiendo otras opciones más gravosas para combatir posibles vulneraciones a derechos humanos, como la dignidad, la privacidad e intimidad, la seguridad de los datos, la prevención de la apología del odio racial, u otros, se opta por una medida que no es en modo alguna intimidatoria o restrictiva previa de derechos, sino por el contrario, basados

---

[8] Tribunal Electoral del Poder Judicial de la Federación. *Juicio para la protección de los derechos político-electorales del ciudadano: SX-JDC-954/2012.* Sentencia del 18 de abril de 2012.
[9] Tribunal Electoral del Poder Judicial de la Federación. *Recurso de consideración. Expediente: SUP-REC-41/2013.* Resolución del 26 de junio de 2013.

en el respeto a los derechos humanos y adaptando nuestra legislación a los estándares internacionales en la materia, cumpliendo cabalmente con el principio de proporcionalidad que debe imperar en todo proceder público.

Al haberse cubierto los principios de idoneidad y necesidad antes indicados, no resulta preciso acudir al principio de proporcionalidad en sentido estricto, toda vez que pueden armonizarse los derechos de acceso a internet, al uso y goce de las tecnologías de la información y comunicación, pero sobre todo, a la protección de los derechos de quienes son receptores de dicha información sin que se realice restricción alguna a un derecho fundamental, únicamente previéndose la pertinencia de establecer un catálogo de conductas ilícitas con el fin de proteger los derechos de quienes usan estas tecnologías.

S É P T I M A.- Como hemos podido exponer, las actividades que se realizan en el ciberespacio también tienen impacto en el mundo físico, resulta apremiante contar con un andamiaje jurídico vigoroso en materia de ciberseguridad con la finalidad de impulsar la innovación tecnológica y económica del país, contribuyendo a la vez al fortalecimiento de las instituciones públicas y al cumplimiento y respeto de los derechos humanos. Dada la complejidad y naturaleza transfronteriza de las dinámicas de la era digital, se advierte la necesidad de abordar la ciberseguridad de forma integral, colaborativa, holística y transversal. La meta es que cualquier esfuerzo que aborde dicho fenómeno evolucione en el tiempo, siempre apostando al esfuerzo conjunto de todos los sectores sociales.

La ciberdelincuencia, de acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito "...es utilizada para englobar muchos delitos distintos, entre ellos los que utilizan datos y sistemas informáticos, entre ellos la piratería informática, las estafas y fraudes electrónicos (como el "phishing"), los delitos relaciones con los

contenidos (como la divulgación de pornografía infantil) y los delitos contra los derechos de autor (como la divulgación de contenidos pirateados).[10]

Naciones Unidas utiliza el término "ciberdelincuencia" para referirse a "...un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos... los actos comprendidos habitualmente en la categoría de "ciberdelincuencia" son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del *modus operandi* del delito."[11]

Naciones Unidas cita como ejemplos de estos ilícitos cometidos mediante la ciberdelincuencia: los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos, como el acceso ilegal a datos o sistemas informáticos, el uso de datos para estafar, robar o causar daño a otras personas, los discursos de incitación al odio, la pornografía infantil, la venta de mercancías ilícitas vía internet, entre otras.[12]

De ahí que resulta indispensable empezar a legislar en esta materia, la falta de un piso mínimo de regulación en materia de ciberseguridad y responsabilidad en el uso de las TIC puede generar constantes riesgos y amenazas en el ciberespacio. La vulnerabilidad de los sistemas de información puede afectar gravemente a las personas, su información, su patrimonio, su reputación e incluso su dignidad. Si a esto sumamos la falta de un marco legal que proteja los intereses de las personas estaremos en un punto alto de vulnerabilidad.

---

[10] UNODC. Oficina de las Naciones Unidas contra la Droga y el Delito. Pág. 22.
[11] ONU. "Seminario 3: el Fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional." Documento A/CONF.222/12. Pág. 6-7.
[12] Ibídem. Pág. 7

La globalización y la hiperconectividad exigen soluciones centradas en la colaboración internacional de manera precisa, eficaz y eficiente. Ante la complejidad de la sociedad en la era digital y los retos que representa el uso y aprovechamiento de las TIC en la sociedad de la información, es importante plantear el tema de la ciberseguridad con la óptica del contexto internacional, por lo tanto esta Iniciativa viene a llenar esta laguna legal en materia penal, puesto que a la fecha no contamos con mecanismos ágiles y expeditos para interactuar en un mundo digital donde los límites de soberanía se desvanecen para dar paso a un mundo global integrado en un mundo sin barreras. Así se acordó en la Comisión de Prevención del Delito y Justicia Penal de esta Oficina de la ONU, la cual elaboró un estudio acerca de los delitos cibernéticos, que busca fortalecer el intercambio de experiencias y buenas prácticas y generar oportunidades de cooperación y asistencia técnica que permitan el apoyo táctico y operativo a los Estados frente a los usos con fines delictivos de las TIC, incluyendo Internet[13].

Esta Iniciativa atiende esta urgente necesidad de coadyuvar con la comunidad internacional en fortalecer un mundo ciberseguro. Como bien lo argumentaron los Diputados González Torres y Fernández González. El Convenio Sobre la Ciberdelincuencia, mejor conocido a nivel mundial como el "Convenio de Budapest" aprobado por el Consejo de Europa el 23 de noviembre del 2001, en la ciudad que lleva su sobrenombre, es el Tratado Marco que existe en la comunidad internacional para proteger a los Estados de los delitos que se cometen a través del ciberespacio. Ellos han sustentado su texto normativo propuesto en este esencial instrumento internacional que si bien el Estado Mexicano no es un país firmante, también lo es que este conjunto normativo es de gran utilidad para construir un marco jurídico penal uniforme con la comunidad internacional con el objeto de combatir la

[13] Oficina de las Naciones Unidas contra la Droga y el Delito, Declaración de Doha - Informe del 13° Congreso de las Naciones Unidas sobre la Prevención del Delito y Justicia Penal (julio de 2015), véase en: http://www.unodc.org/documents/congress//Declaration/V1504154_Spanish.pdf

ciberdelincuencia. Un requisito que el Consejo de Europa impone a todos los Estados que pretenden adherirse al tratado internacional, es precisamente realizar medidas legislativas y de otro tipo para armonizar su marco jurídico interno con las disposiciones del Convenio de Budapest, de ahí la importancia de transitar con esta propuesta que esta Comisión de Justicia tiene a bien aprobar.

O C T A V A.- Esta Comisión de Justicia ha analizado mediante diversos métodos la valoración de los argumentos de los autores que sustentan la Iniciativa materia del presente Dictamen, mismo que con los argumentos vertidos en las Consideraciones anteriores podemos concluir con la viabilidad de legislar en materia de ciberseguridad. Una vez hecho este análisis, procedemos a realizar el análisis y valoración de los textos normativos propuestos. En primer orden, las y los integrantes de este órgano legislativo analizaremos las propuestas de modificación al Código Penal Federal, analizando cada artículo propuesto por separado.

CÓDIGO PENAL FEDERAL

TEXTO VIGENTE	TEXTO PROPUESTO
Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de	**Artículo 202.-** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de

archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.	archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos, **incluidos sistemas informáticos**. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientas a dos mil **veces el valor diario de la Unidad de Medida y Actualización.**
(...)	(...)
La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.	La misma pena se impondrá a quien **produzca**, reproduzca, **ofrezca o ponga a disposición**, almacene, distribuya, venda, compre, arriende, exponga, publicite, **difunda o** transmita, importe, exporte o posea el material a que se refieren los párrafos anteriores.

Los Diputados Iniciantes incluyen a los sistemas informáticos dentro del tipo penal de pornografía infantil como una forma de exhibir el producto de esta conducta ilícita, la cual constituye un delito de alta incidencia delictiva y que en la actualidad se encuentra asociada con el uso de las tecnologías de la información y comunicación, por lo tanto, se propone modificar el texto normativo para perfeccionar su redacción. Como bien lo sustentan los Iniciantes, el numeral 1 del artículo 9 del Convenio de Budapest establece lo siguiente:

> *"Artículo 9 - Delitos relacionados con la pornografía infantil*
>
> *1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la Comision deliberada e ilegítima de los siguientes actos:*

a la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c la difusión o transmisión de pornografía infantil por medio de un sistema informático, d la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. a 4. ..."(subrayado nuestro)

Como podemos observar, el tipo penal que establece este Convenio incluye a los sistemas informáticos dentro de todas sus modalidades de la comisión de este delito, al tratarse de un ilícito que se comete por medio de sistemas informáticos. Asimismo, esta modificación resulta acorde con nuestra normatividad actual, misma que para efectos de técnica legislativa no se modifica el orden que ya tiene establecido, simplemente se agrega este elemento que faltan por incluir para ajustar este delito a los estándares internacionales en materia de ciberseguridad. Asimismo, se establece la Unidad de Medida y Actualización para adecuar el nuevo método para realizar el cálculo de las sanciones económicas conforme a la reforma constitucional en materia de desindexación del salario mínimo.

TEXTO VIGENTE	TEXTO PROPUESTO
Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución	**Artículo 202 BIS.-** Quien almacene, **adquiera,** compre, arriende **o posea, a través de sistemas informáticos o en dispositivos de almacenamiento de**

se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.	**datos informáticos** el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientas **veces el valor diario de la Unidad de Medida y Actualización.** Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

En el mismo sentido, para efectos de este artículo, los diputados proponen incluir a los sistemas informáticos como el medio de distribución de este delito, así como para actualizar la desindexación del salario mínimo en las sanciones económicas.

TEXTO VIGENTE	TEXTO PROPUESTO
Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.	**Artículo 211 bis 1.-** Al que sin autorización **obstaculizare el funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de información y datos contenidos** en sistemas o equipos de informática protegidos **contra el acceso no autorizado,** se le impondrán de **dos a cuatro** años de prisión y de cien a trescientas **veces el valor diario de la Unidad de Medida y Actualización**.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le	Al que sin autorización copie información contenida en sistemas o equipos de informática protegidos **en contra del acceso no autorizado,** se

impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.	le impondrán de **seis** meses a **dos años** de prisión y de **doscientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**
Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.	**Artículo 211 bis 2.-** Al que sin autorización **acceda,** modifique, destruya o provoque pérdida **parcial o total** de información contenida en sistemas o equipos de informática del Estado, protegidos **en contra del acceso no autorizado,** se le impondrán de uno a cuatro años de prisión y de **quinientas a mil veces el valor diario de la Unidad de Medida y Actualización.**
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.	Al que sin autorización **acceda,** conozca o copie información **o datos contenidos** en sistemas o equipos de informática del Estado, protegidos **en contra del acceso no autorizado,** se le impondrán de seis meses a dos años de prisión y de **doscientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.	A quien sin autorización **acceda,** conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, **protegidos en contra del acceso no autorizado,** se le impondrá pena de cuatro a diez años de prisión **y de mil a dos mil veces el valor diario de la Unidad de Medida**

Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.	**y Actualización.** Si el responsable es o hubiera sido servidor público en una institución de seguridad pública **o del sistema nacional de administración de justicia penal**, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
(...)	(...)
Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.	**Artículo 211 bis 3.-** Al que estando autorizado indebidamente modifique, destruya o provoque pérdida **parcial o total** de información **contenida en sistemas o equipos de informática del Estado**, se le impondrán de dos a ocho años de prisión y de trescientas a novecientas **veces el valor diario de la Unidad de Medida y Actualización**.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.	Al que estando autorizado, indebidamente copie información **o datos contenidos en sistemas o equipos de informática del Estado,** se le impondrán de **dos a ocho** años de prisión y de **cien a ochocientas veces el valor diario de la Unidad de Medida y Actualización.**
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le	**Al que** estando autorizado, indebidamente obtenga, copie o utilice información **o datos contenidos en sistemas o equipos de informática en materia de seguridad pública**, se le impondrá pena de cuatro a diez años

impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.	de prisión y multa de **mil a dos mil veces el valor diario de la Unidad de Medida y Actualización.** Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.	**Artículo 211 bis 4.-** Al que sin autorización modifique, destruya o provoque pérdida de información **o datos contenidos** en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos **en contra del acceso no autorizado,** se le impondrán de seis meses a cuatro años de prisión y **multa de doscientas a mil doscientas veces el valor diario de la Unidad de Medida y Actualización.**
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.	Al que sin autorización copie información **o datos contenidos** en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos **en contra del acceso no autorizado,** se le impondrán de tres meses a dos años de prisión y **multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.	**Artículo 211 bis 5.-** Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero indebidamente modifique, destruya o provoque pérdida de información **o datos contenidos en sistemas o equipos de informática,** se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas **veces el valor diario de la Unidad de Medida y Actualización.**
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.	Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie **información o datos contenidos en sistemas o equipos de informática,** se le impondrán de tres meses a dos años de prisión y **multa** de cincuenta a trescientas **veces el valor diario de la Unidad de Medida y Actualización.**
(...)	(...)
Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.	**Artículo 211 bis 7.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información **o datos obtenidos** se **utilicen** en provecho propio o ajeno.

El análisis de este catálogo de delitos se realiza de manera conjunta, toda vez que estos quedan incluidos dentro del Capítulo II "Acceso ilícito a sistemas y equipos de informática" del Título Noveno "Revelación de secretos y acceso ilícito a sistemas y

equipos de informática", mismos que esta Iniciativa perfecciona los tipos penales a efecto de incluir los supuestos que al día de hoy, no contempla nuestra legislación.

El artículo 2 del Convenio de Budapest establece este tipo de delito, sin embargo, la legislación mexicana desarrolla con mayor amplitud (atendiendo al principio de la exacta aplicación de la ley penal) este tipo de delitos. Este Instrumento Internacional establece lo siguiente:

> *"Artículo 2 - Acceso ilícito*
>
> *Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá· exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático."*

En primer lugar, los Diputados proponen incluir el concepto del acceso no autorizado a los sistemas y equipos de informática, o la pérdida parcial o total de la información. Asimismo, se realiza un aumento proporcional pero mínimo a las penas de estos delitos para endurecer las sanciones de quienes cometen estas conductas ilícitas en detrimento del patrimonio de las personas o Instituciones que como ya hemos analizado, constituyen pérdidas millonarias tanto para las personas como a las empresas y a las Instituciones del Estado. De igual forma, se incrementan de las sanciones económicas para los mismos efectos, medida que es proporcional dada la frecuencia con la que los ciberdelincuentes están actuando de forma acelerada y sin un control para contrarrestar estas conductas ilícitas.

Otra modificación consiste en incluir a los servidores públicos del sistema nacional de administración de justicia penal, como responsables de este tipo de delitos, imponiéndoles la sanción de destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Esto es de gran importancia debido a que, en un Estado Democrático, el abuso de poder por parte de quienes al servicio de la ciudadanía utilizan la posición pública para delinquir deben ser sancionados con mayor rigor.

En sintonía con la modificación anterior y siguiendo la línea de actualizar nuestro Código sustantivo penal conforme a la nueva disposición de la desindexación del salario mínimo, se modifica el término días multa por la Unidad de Medida y Actualización para el cálculo de las sanciones económicas.

En consecuencia, este órgano legislativo atendiendo al principio constitucional del estricto derecho que la ley penal exige, es decir, la precisión en la norma punitiva, es que esta Dictaminadora considera viables. Por lo tanto, con estas modificaciones se cierran las lagunas jurídicas que persisten en este catálogo de delitos de acceso ilícito a sistemas y equipos de informática.

TEXTO VIGENTE	TEXTO PROPUESTO
Sin correlativo	**Artículo 211 bis 8.- A quien intercepte de forma dolosa y sin autorización por cualquier medio técnico, datos informáticos, información o comunicaciones dirigidas, originadas o efectuadas en o dentro de un sistema informático incluidas las emisiones electromagnéticas que transporten datos, información o comunicaciones, se le impondrá**

	pena de cinco a diez años de prisión y multa de mil a dos mil veces el valor diario de la Unidad de Medida y Actualización.

Por lo que respecta a la adición de este artículo 211 bis 8, debemos atender al estudio del artículo 3 del multicitado Convenio de Budapest, el cual establece la recomendación a los Estados Parte de este Convenio para adoptar· las medidas legislativas para tipificar en el derecho interno este delito:

> *"Artículo 3 - Interceptación ilícita*
>
> *Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá· exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático."*

Como podemos observar, los Diputados proponentes trasladan el tipo penal estipulado en esta norma internacional a nuestro Código Sustantivo Penal. Asimismo, incluyen además elementos adiciónales a la tipificación que realiza este instrumento internacional, esto en razón de englobar los aspectos minuciosos que se presentan en la comisión de este delito y atendiendo al buen uso del lenguaje.

Por lo tanto, esta Comisión ve procedente incluir esta conducta a nuestro catálogo de delitos de acceso ilícito a sistemas y equipos de informática.

Ahora bien, para analizar la viabilidad sobre la propuesta de los Iniciantes respecto de la adición del Capítulo III "Delitos Informáticos" con los artículos 211 TER, 211 QUATER, 211 QUINTUS; así como la adición de la fracción XXII al artículo 387 del Código Penal Federal respecto a la tipificación del fraude en su modalidad de fraude informático, se realizará un cuadro comparativo entre el articulado del Convenio de Budapest. y la propuesta contenida en la Iniciativa materia del presente Dictamen, en razón de que, en obviedad de razones, no se cuenta con un correlativo en el Código Penal Federal, esto a efecto de que las y los integrantes de la Comisión de Justicia tengamos una mejor perspectiva sobre la conveniencia de su aprobación.

CONVENIO DE BUDAPEST	TEXTO PROPUESTO
	CAPÍTULO III **Delitos Informáticos**
Artículo 6 - Abuso de los dispositivos 1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;	**Artículo 211 TER.- Abuso de Dispositivos.** **Comete el delito de abuso de dispositivos quien, sin autorización, cometiere cualquiera de las siguientes actividades:** **I. Producir, vender, obtener para su utilización, importar, difundir o de cualquier otra forma poner a disposición:** **a) Cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos**

ii) una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá· exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal. 2 No podrá· interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.	**previstos en el Título Noveno de este Código; y** **b) Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.** **II. Poseer alguno de los elementos previstos en los incisos a) o b) de la fracción primera del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.** **III. Crear, utilizar, alterar, capturar, grabar, copiar o transferir de un dispositivo de acceso o un medio a otro similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y acceso al servicio o sistema informático que permita la operación paralela, simultánea o independiente de un servicio o sistema informático, legítimamente obtenido por un tercero; o bien, con la intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.** **Se impondrá pena de prisión de tres a cinco años y multa de doscientas a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización.**

3 Cualquier Parte podrá· reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.	**No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo primero del presente artículo no tenga por objeto la comisión de alguno de los delitos previstos en el Título Noveno, de este Código.**
Artículo 7 - Falsificación informática Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.	**Artículo 211 QUÁTER.- Falsificación informática.** **Comete delito de falsificación informática quien sin autorización introdujere, alterare, borrare o suprimiere datos informáticos previamente almacenados en un sistema informático, que generen datos no auténticos con la intención que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Se le impondrá pena de prisión de dos a tres años y multa de cien a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización.** **Se impondrá pena de tres a cinco años de prisión y multa de doscientas a quinientas veces el valor diario de la Unidad de Medida**

	y Actualización en los casos siguientes: a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito; y, b) Cuando los actos descritos en el párrafo anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.
...	Artículo 211 QUINTUS.- Usurpación de Identidad Ajena. A quien usurpe, suplante, obtenga, utilice, apropie o adopte la identidad de otra persona, a través de un sistema informático con la intención de causar un daño o perjuicio a una persona, se le impondrá pena de uno a cinco años de prisión y de cuatrocientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.

	La misma pena se impondrá cuando la usurpación de identidad ajena se cometa infringiendo medidas de seguridad y con la intención de obtener de forma ilegítima un beneficio económico o lucro indebido para sí mismo o para otra persona o generar un daño en el patrimonio de una persona tanto física como jurídica.
Artículo 8 - Fraude informático Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a cualquier introducción, alteración, borrado o supresión de datos informáticos; b cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.	**Artículo 387.-** Las mismas penas señaladas en el artículo anterior, se impondrán: I. a XXI. (...) **XXII. A quien sin autorización causare un perjuicio patrimonial a otra persona, incluyendo a una persona moral, mediante la introducción, alteración, borrado o supresión de datos informáticos.** **Las mismas penas se impondrán a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.**

Al auscultar los elementos que contienen los tipos penales establecidos en el Convenio de Budapest, resulta evidente que los Diputados han basado su propuesta en el texto normativo de este tratado internacional, con el debido cuidado de adaptar estas disposiciones al correcto uso del lenguaje.

En primer orden, se tipifica el delito de abuso de dispositivos incluyendo los elementos esenciales que contiene este tratado marco, con la única adición de establecer la correspondiente pena consistente en la imposición de una pena de prisión de tres a cinco años y multa de doscientas a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización.

Por lo que respecta al delito de falsificación informática, los Diputados iniciantes aplican la misma razón de igualar los tipos penales del Convenio de Budapest con nuestro Código Penal Federal, plasmando los mismos elementos para tipificar este delito que como vemos constituye un riesgo constante para las personas que utilizan las tecnologías de la información y la comunicación. Incluso los Diputados van más allá del espíritu protector de este convenio al incluir los supuestos cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito; y cuando esta conducta ilícita se realice para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.

Por último, el fraude informático que establece el Convenio de Budapest se regula dentro del delito de fraude, esto en razón de que ya está contemplado este tipo penal, sin embargo, no se contempla la modalidad de la comisión de este delito en tratándose de dañar los sistemas o datos informáticos. Es por ello que, dentro del artículo 387 donde se establecen las modalidades del fraude, los Iniciantes incluyen una fracción XXII para regular este supuesto normativo. Esto sin duda abonará en el perfeccionamiento de la tipicidad del fraude informático, sin crear otro delito que

dé lugar a crear antinomias jurídicas y que obstaculicen la tarea investigadora de las autoridades.

N O V E N A.- Esta Comisión de Justicia, una vez hecho el análisis y valoración de las propuestas al Código Sustantivo Penal, procedemos a realizar el mismo ejercicio revisor a las modificaciones al Código Nacional de Procedimientos Penales. En nuestro país la legislación en materia penal, desde el año 2008, ha pasado por cambios importantes derivados de la implementación del Sistema de Justicia Penal Acusatorio, uno de los principales se vio materializado a través de la creación del Código Nacional de Procedimientos Penales (CNPP), publicado en el Diario Oficial de la Federación el 17 de junio de 2016, ya que se trata de uno de los cambios jurídicos más relevantes en las últimas décadas. De 33 códigos que había en el país, cada uno con distintas reglas para el desahogo de un juicio penal, ahora existe este un código único, que es válido y uniforme en todo el territorio nacional, lo cual se traduce en que todos los procesos penales se lleven a cabo bajo las mismas reglas, fortaleciendo el Estado de Derecho.

Este Código Adjetivo está adaptado a las nuevas necesidades que nuestro Sistema de Justicia Penal Acusatorio nos exige, sin embargo, tenemos que seguir perfeccionando este instrumento jurídico, máxime cuando el desarrollo tan veloz que presentan las tecnologías de la información y la comunicación hacen que las Instituciones del Estado como el Poder Legislativo realicen todas las acciones necesarias para ponerse a la vanguardia del mundo digital en el que vivimos.

En primer orden, las y los integrantes de este órgano legislativo analizaremos las propuestas de modificación al Código Penal Federal, auscultando la reforma al artículo 439 sobre de los alcances que tendrá la asistencia jurídica, respecto a la obtención de pruebas en materia de cooperación internacional en materia penal.

CODIGO NACIONAL DE PROCEDIMIENTOS PENALES

TEXTO VIGENTE	TEXTO PROPUESTO
Artículo 439. Alcances La asistencia jurídica comprenderá: I. (...) II. Obtención de pruebas; III. a XI. (...)	**Artículo 439. Alcances** La asistencia jurídica comprenderá: I. (...) **II.** Obtención de pruebas, **incluidas las evidencias digitales o pruebas almacenadas en un sistema informático.** III. a XI. (...)

El aspecto de las "Evidencias Digitales" constituye sin dudas, un interesante tema a desarrollar en materia penal, máxime cuando el mundo global en el que vivimos y con el desarrollo tan acelerado de las tecnologías de la información y comunicación y el empleo cada vez mayor del internet, las fronteras o limites existentes entre la delincuencia convencional y la ciberdelincuencia resultan cada vez menores, así lo indica la Organización de las Naciones Unidas al afirmar que: "Con el uso cada vez más generalizado de dispositivos electrónicos y de la conectividad global en la vida cotidiana, las pruebas electrónicas, como los mensajes de texto, los mensajes electrónicos, los datos de navegación por internet o los datos de redes sociales, son cada vez más habituales en muchas investigaciones penales convencionales."[14] Por esta razón, este órgano legislativo considera que esta reforma abonará en una mejora en la asistencia jurídica internacional en materia penal por parte del Estado Mexicano respecto a las evidencias digitales o pruebas almacenadas en un sistema

[14] ONU. "Seminario 3: el Fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional." Documento A/CONF.222/12. Pág. 7

informático, cumpliendo así con el concierto internacional que reclama la cooperación de todos los Estados para fortalecer el Sistema de Ciberseguridad a nivel mundial.

CONVENIO DE BUDAPEST	TEXTO PROPUESTO
Sin correlativo	**Artículo 390 BIS 1. Disposiciones Generales** **Los actos de investigación para la obtención de evidencias digitales, deberán considerar los supuestos previstos en la Constitución Política de los Estados Unidos Mexicanos, los instrumentos y tratados internacionales que versen sobre los derechos humanos de los que el Estado Mexicano sea parte, así como las garantías, principios y reglas que fundamentan el presente Código.**
Artículo 16 - Conservación rápida de datos informáticos almacenados 1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos	**Artículo 390 BIS 2. Conservación de Datos Informáticos Almacenados** **El Ministerio Público podrá ordenar a cualquier persona física o jurídica, la conservación de la integridad de los datos informáticos concretos, almacenados en un sistema informático que esté bajo su disposición cuando tenga motivos suficientes para considerar que puedan ser alterados o suprimidos y afectar así el resultado de una investigación. La medida no podrá exceder de noventa días y será**

resultan especialmente susceptibles de pérdida o de modificación. 2 Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales Órdenes sean renovables. 3 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno. 4 ...	**prorrogable por igual período, si se mantienen los motivos que fundamentaron la orden.** **La persona requerida, una vez que reciba la comunicación respectiva, deberá ejecutar los actos necesarios que garanticen la preservación, inmediata de los datos en cuestión y estará obligado a mantener secreto en los términos de lo previsto por la legislación penal aplicable.** **Cuando se trate del aseguramiento o conservación de datos relativos al tráfico de comunicaciones, si el proveedor de servicios requerido advierte que en la comunicación objeto de la investigación han participado otros proveedores de servicios, informará inmediatamente a la autoridad competente que haga el requerimiento o solicitud, para que adopte las medidas necesarias.** **Para llevar a cabo la conservación de la integridad de los datos informáticos almacenados en un sistema informático, se requerirá la autorización judicial del Juez de control y para ello, se estará a lo dispuesto en el tercer párrafo de artículo 291 y artículos 292 a 302 de este Código.**

Artículo 18 - Orden de presentación 1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar: a a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y b a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios. 2 Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14. 3 A los efectos del presente artículo, por datos relativos a los abonados se entender· toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:	**Artículo 390 BIS 3. Datos Almacenados de Usuarios o Abonados** **El Ministerio Público podrá ordenar a cualquier persona física o jurídica, que presente, remita o entregue datos almacenados en un sistema informático que este bajo su poder o control y que se vinculen con la investigación de un delito concreto. Asimismo, podrá ordenar a toda persona física o jurídica que preste un servicio de comunicaciones o a los proveedores de servicios de cualquier tipo, la entrega de datos de los usuarios o abonados o los datos de identificación y facturación con los que cuente. La orden podrá contener la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de sanción penal en los términos de lo previsto por la legislación aplicable. Estas medidas serán ejecutadas por el Ministerio Público correspondiente, salvo las excepciones previstas en la legislación vigente, en las cuales se exija la autorización judicial del Juez de control.**

a el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.	
Artículo 19 - Registro y confiscación de datos informáticos almacenados 1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar: a a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y b a un medio de almacenamiento de datos informáticos en el que puedan	**Artículo 390 BIS 4. Registro y Preservación de Datos Almacenados** **El órgano jurisdiccional podrá ordenar a solicitud del Ministerio Público, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:** **I. Acceder a los componentes físicos y lógicos del sistema y,** **II. Obtener copia de los datos en un soporte autónomo o**

almacenarse datos informáticos, en su territorio. 2 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema. 3 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 o 2. Estas medidas incluirán las siguientes facultades: a confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;	**III. Preservar por medios tecnológicos o bloquear el acceso a los datos de interés para la investigación.** **En los supuestos en los que, durante la ejecución de una medida de incautación de datos de un sistema Informático, previstos en el párrafo anterior, surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla o ampliar el registro al otro sistema. La ampliación del registro a los fines de la incautación deberá ser autorizada por el órgano jurisdiccional salvo que estuviera prevista.**

b realizar y conservar una copia de dichos datos informáticos; c preservar la integridad de los datos informáticos almacenados de que se trate; d hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso. 4 y 5 ...	
Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público Una Parte podrá·, sin la autorización de otra Parte: a tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o b tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.	**Artículo 390 BIS 5. Datos Informáticos Almacenados en otro Estado** **Con fundamento en lo dispuesto en los tratados y convenciones internacionales ratificados por el Estado Mexicano, las autoridades especializadas en la investigación de delitos del fuero federal o fuero común, incluida la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas adscrita a la Agencia de Investigación Criminal, podrán acceder o recibir datos informáticos almacenados en un sistema informático, ubicado en otro Estado, cuando éstos se encuentren accesibles en fuentes de acceso público, independientemente de la ubicación geográfica de los mismos; o a través de un sistema informático ubicado en México, si la autoridad**

	investigadora competente obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos en ese país por medio de un sistema informático.
Artículo 20 - Obtención en tiempo real de datos sobre el tráfico 1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a: a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y b obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: i a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. 2 Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no	**Artículo 390 BIS 6. Obtención de Datos en Tiempo Real** **Para la obtención, en tiempo real, de datos de tráfico de comunicaciones electrónicas o la interceptación de datos informáticos de contenido, regirá lo dispuesto en los artículos 178 Bis del Código Penal Federal, 303 del Código Nacional de Procedimientos Penales y los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.**

pueda adoptar las medidas indicadas en el apartado 1.a), podrá· adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo. 3 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto. 4 Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	
Artículo 23 - Principios generales relativos a la cooperación internacional Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación	**Artículo 390 BIS 7. Cooperación y Asistencia Jurídica en Materia Procesal Penal** **En caso de cooperación y asistencia jurídica internacional, las solicitudes de aseguramiento de datos, solicitudes de presentación de datos, de obtención o confiscación, de acceso libre a fuentes de acceso público y asistencia mutua para obtención de**

uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos. Artículo 25 - Principios generales relativos a la asistencia mutua 1 Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito. 2 a 5 ...	**datos sobre el tráfico e interceptación de comunicaciones, se estará a lo dispuesto en el Titulo XI de este Código, así como los tratados y convenciones internacionales ratificados por el Estado Mexicano. Asimismo, se tomará en cuenta el derecho a la intimidad y a la confidencialidad de ciertos datos protegidos bajo la legislación nacional vigente y tratados y convenciones internacionales en materia de derechos humanos ratificados por el Estado Mexicano.**
Sin correlativo	**Artículo 390 BIS 8. Protección de Datos Personales en Investigaciones** **Las autoridades nacionales encargadas de investigar y perseguir delitos informáticos y el órgano jurisdiccional competente, deben respetar los principios y garantías individuales establecidas en la Constitución Política de los Estados Unidos Mexicanos, en convenios y tratados sobre derechos humanos ratificados por el Estado Mexicano, de tal forma que los derechos de las personas sean**

	protegidos a través del uso de tecnologías de información y comunicación, en particular el respeto a su intimidad y la protección de datos personales, tanto datos de tráfico como datos de contenido, salvo con fines legítimos para la prevención de delitos o la protección de los derechos y libertades de terceros. **Con respecto a la obtención y tratamiento de datos personales por parte de las instancias de seguridad, procuración y administración de justicia, se estará a lo dispuesto en los Artículos 80, 81 y 82 de la Ley General de Protección de Datos en Posesión de los Sujetos Obligados.** **El tratamiento de datos personales para efectos de la investigación o como medio de prueba, deberá cumplir exclusivamente la finalidad para el que fueron originalmente obtenidos y tratados, por un tiempo de dos años y una vez cumplida la finalidad y propósito de investigación debe procederse a su cancelación y supresión.** **La protección de la información y los datos personales es responsabilidad compartida de las autoridades en las distintas entidades que intervienen en la vigilancia, investigación y**

	persecución penal de los delitos establecidos en el Código Penal Federal y otras leyes.

En esta importante aportación a nuestro Código Adjetivo Penal se adicionan los artículos 390 BIS 1 al 390 BIS 8 para que, atendiendo a la técnica legislativa, no se interfiera con las demás disposiciones normativas de este ordenamiento jurídico. En este conjunto de artículos se establecen aspectos de especial relevancia para la obtención de Evidencias Digitales como medios de prueba.

En primer lugar, coincidimos con los diputados iniciantes al establecer en el artículo 390 BIS 1 con las disposiciones generales que habrán de observarse en esta sección delos actos de investigación necesarios para la obtención de evidencias digitales, anteponiendo la observancia de los derechos humanos contenidos tanto en la Constitución como en los tratados internacionales en la materia, espíritu rector de nuestra carta magna establecido en su artículo 1º.

En el artículo 390 BIS 2 se regula la conservación de datos informáticos almacenados, armonizando el contenido del artículo 16 del Convenio de Budapest, al fijar que el Ministerio Público pueda ordenar la conservación de datos almacenados en un sistema informático cuando esta tenga motivos para considerar que puedan ser alterados o suprimidos afectando con ello el resultado de una investigación, fijando con ello el plazo sugerido en este Convenio que es de 90 días prorrogables por un periodo igual. Asimismo, se incluye el deber de secrecía por parte de quien se encuentra bajo la custodia de los datos y sus procedimientos. Los Iniciantes al final establecen el requisito sine qua non para realizar este procedimiento, el cual como lo marca nuestra carta magna, debe ser previamente bajo una autorización judicial.

En el artículo 390 BIS 3, se regulan los datos almacenados de usuarios o abonados, mismos que, los Diputados iniciantes replican conforme al artículo 18 del Convenio.

Como lo señala este artículo el Estado debe adoptar las medidas legislativas como lo es este Dictamen, para que las autoridades competentes en este caso el Ministerio Público, ordene a una persona a que presente los datos almacenados en un sistema informático que este bajo su poder o control o bien a un proveedor de servicios en este mismo sentido, así como la secrecía del procedimiento, como bien lo proponen los Diputados, se debe exigir el control constitucional de la autorización judicial para los casos concretos que así lo requieran.

Respecto al artículo 390 BIS 4 se replica lo establecido en el artículo 14 del Convenio de Budapest adaptándolo a nuestro orden interno tal como lo marca este instrumento internacional., en este caso facultar al Ministerio Público a realizar el registro de un sistema informático para obtener copia de los datos en un soporte autónomo o preservar por medios tecnológicos o bloquear el acceso a los datos de interés para la investigación, así como su ampliación cuando surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático, esto colocándole un candado jurídico de ser autorizada por el órgano jurisdiccional salvo que estuviera prevista.

En el artículo 390 BIS 5 se regulan los datos informáticos almacenados en otro estado, tal como lo establece el artículo 32 del multicitado convenio. Los Iniciantes facultan a la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas adscrita a la Agencia de Investigación Criminal como autoridades encargadas de acceder o recibir datos informáticos almacenados en un sistema informático cuando éstos se encuentren accesibles en fuentes de acceso público, tal como lo establece este artículo 32, adaptándolo conforme al buen uso del lenguaje y a la correcta técnica legislativa.

En el artículo 390 BIS 6 se regula la obtención de datos en tiempo real, plasmando el espíritu del artículo 20 del Convenio, adoptando las medidas legislativas necesarias para cumplir con este artículo tan importante para intercambiar

ágilmente el intercambio de información para la obtención de las evidencias digitales. Esta Comisión Dictaminadora coincide con los Diputados al delegar a la normatividad especial el contenido de esta disposición a los artículos 178 BIS del Código Penal Federal, 303 del Código Nacional de Procedimientos Penales y los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, que dispone lo siguiente:

Código Penal Federal

> *"Artículo 178 Bis.- A la persona física o en su caso al representante de la persona moral que sea requerida por el Ministerio Público o por la autoridad competente para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión, 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 hacerlo de forma dolosa, se le impondrá una pena de prisión de 3 a 8 años y de cinco mil a diez mil días multa.*
>
> *Las mismas penas se aplicarán a la persona física, o en su caso al representante de la persona moral que de forma dolosa obstaculice, retrase sin justa causa o se rehusé a colaborar en la intervención de comunicaciones privadas, o a proporcionar información a la que estén obligados, en los términos de la legislación aplicable.*

Se aplicarán las mismas penas a la persona física, o en su caso al representante de la persona moral que sea requerida por las autoridades competentes, para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión y que se rehusare hacerlo de forma dolosa."

Código Nacional de Procedimientos Penales

"Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados

Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente."

Ley Federal de Telecomunicaciones y Radiodifusión

"Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables.

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;

IV. Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título.

Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo 189 de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener

facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;

V. Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo;

VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular. Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios;

VII. Realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier modalidad reportadas por los clientes, utilizando cualquier medio, como robadas o extraviadas; así como realizar la suspensión inmediata del servicio de telefonía cuando así lo instruya la autoridad competente para hacer cesar la comisión de delitos, de conformidad con lo establecido en las disposiciones legales aplicables;

VIII. Colaborar con las autoridades competentes para que en el ámbito técnico operativo se cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación.

El bloqueo de señales a que se refiere el párrafo anterior se hará sobre todas las bandas de frecuencia que se utilicen para la recepción en los equipos terminales de comunicación y en ningún caso excederá de veinte metros fuera de las instalaciones de los centros o establecimientos a fin de garantizar la continuidad y seguridad de los servicios a los usuarios externos. En la colaboración que realicen los concesionarios se deberán considerar los elementos técnicos de reemplazo, mantenimiento y servicio.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen;

IX. Implementar un número único armonizado a nivel nacional y, en su caso, mundial para servicios de emergencia, en los términos y condiciones que determine el Instituto en coordinación con el Sistema Nacional de Seguridad Pública, bajo plataformas interoperables, debiendo contemplar

mecanismos que permitan identificar y ubicar geográficamente la llamada y, en su caso, mensajes de texto de emergencia;

X. Informar oportuna y gratuitamente a los usuarios el o los números telefónicos asociados a los servicios de seguridad y emergencia que determine el Instituto en coordinación con el Sistema Nacional de Seguridad Pública, así como proporcionar la comunicación a dichos servicios de forma gratuita;

XI. En los términos que defina el Instituto en coordinación con las instituciones y autoridades competentes, dar prioridad a las comunicaciones con relación a situaciones de emergencia, y

XII. Realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal.

Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada."

Como podemos observar estos ordenamientos jurídicos ya establecen estas disposiciones para obtener los datos en tiempo real, por lo que únicamente se armoniza nuestro marco jurídico para no crear antinomias jurídicas al remitir a estos artículos para estos efectos.

Para el artículo 390 BIS 7 respecto de la Cooperación y Asistencia Jurídica en Materia Procesal Penal, se establece una armonización con las discusiones del artículo 23 del Convenio de Budapest, misma que contempla la asistencia mutua entre los Estados conforme a los tratados internacionales aplicables en cooperación internacional en materia penal en tratándose de solicitudes de aseguramiento de datos, solicitudes de presentación de datos, de obtención o confiscación, de acceso libre a fuentes de acceso público y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones, remitiéndolo así al título XI del mismo código que contempla la "ASISTENCIA JURÍDICA INTERNACIONAL EN MATERIA PENAL", donde se incluyen a las evidencias digitales como un alcance de la asistencia jurídica para la obtención de pruebas.

Por último, en el artículo 390 BIS 8 se atiende el principio de la protección de datos personales en las investigaciones, aspecto de vital importancia para la privacidad, intimidad y seguridad de la información de las personas e instituciones involucradas en la investigación u persecución de los delitos informáticos y la secrecía de las autoridades involucradas. De esta forma se remite a lo dispuesto por la recién creada Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, misma que salvaguarda los derechos humanos de la ciudadanía con sus disposiciones protectoras, por lo que con este artículo que si bien no está contemplado en el Convenio de Budapest, esta Comisión Dictaminadora considera de vital necesidad incluir para que en estos procedimientos se atienda la observancia de estas deposiciones en pro de la seguridad de la información de todos los involucrados.

D E C I M A. Esta Comisión Dictaminadora considera viable aprobar esta Iniciativa, la cual constituye una medida legislativa eficaz en el combate a los ciberdelitos, mismos que, atendiendo al principio de estricto derecho de la ley penal que nos mandata nuestra Constitución Política, necesitamos regular con toda puntualidad y rigor para que estas normatividades sustantivas y adjetivas penales estén resguardadas bajo el principio de legalidad y atendiendo a las mejores prácticas legislativas internacionales.

Resulta importante destacar que en este Dictamen no se incluye ninguna restricción al ejercicio del derecho a la libertad de expresión o de acceso a internet, al contrario, el espíritu de esta reforma integral consiste en garantizar el pleno ejercicio de los derechos humanos en el uso de las tecnologías de la información y comunicación, a fin de armonizar plenamente los derechos fundamentales de todos y cada uno de los ciudadanos. Desde este Poder Legislativo tenemos que ejercer todos los medios necesarios para alcanzar una legislación eficaz y vigorosa que si bien, por la naturaleza del tema, impide que toda legislación esté acorde y en tiempo real con las transformaciones tan aceleradas que conlleva proteger el uso de estas tecnologías, se tienen que buscar las acciones que estén al alcance del Estado para fortalecer el andamiaje institucional en materia de Ciberseguridad.

Desde esta Comisión de Justicia nos sumamos a colaborar con el combate a todas las amenazas que día a día se descubren con el uso de las tecnologías de la información y comunicación, amenazas que marcan la necesidad de adecuar la legislación vigente para lograr prevenir, sancionar y contrarrestar todas aquellas conductas que dañen los bienes de las personas y la infraestructura nacional o el actuar y la estabilidad de las instituciones del Estado, por lo que un marco regulatorio vigoroso en materia de ciberdelincuencia debe considerarse como urgente y necesario para dar un paso considerable a fin de hacer frente a estos riesgos.

El mundo global en el que nos desarrollamos exige al Estado Mexicano realizar todas las acciones de gobierno necesarias para evolucionar en las áreas estratégicas de seguridad, incluyendo el uso de las tecnologías de la información y comunicación. Necesitamos garantizar y dar certeza jurídica a aquellas personas que han sufrido afectación en el uso de estas tecnologías, por lo que este Dictamen generará las condiciones idóneas para colocar a la vanguardia a nuestro país para enfrentar los retos que la Cuarta Revolución Industrial plantea a México.

Por todo lo anteriormente expuesto, esta dictaminadora considera viable la iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, por lo que los integrantes de la Comisión de Justicia ponemos a consideración de la Honorable Asamblea el siguiente:

PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL Y DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES

ARTÍCULO PRIMERO.- Se reforman los artículos 202, párrafos primero y tercero, 202 BIS, la denominación del Título Noveno "Revelación de secretos, acceso ilícito a sistemas y equipos de informática y Delitos Informáticos" del Libro Segundo, los artículos 211 bis 1 al 211 bis 5 y 211 bis 7; y se adicionan el artículo 211 bis 8, el Capítulo III "Delitos Informáticos" del Título Noveno, conteniendo los artículos 211 TER al 211 QUINTUS y la fracción XXII del artículo 387 del Código Penal Federal; para quedar como sigue:

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos**, incluidos sistemas informáticos**. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientas a dos mil **veces el valor diario de la Unidad de Medida y Actualización.**

(...)

La misma pena se impondrá a quien **produzca**, reproduzca, **ofrezca o ponga a disposición**, almacene, distribuya, venda, compre, arriende, exponga, publicite, **difunda o** transmita, importe, exporte o posea el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, **adquiera,** compre, arriende **o posea, a través de sistemas informáticos o en dispositivos de almacenamiento de datos informáticos** el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientas **veces el valor diario de la Unidad de Medida y Actualización.** Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

TÍTULO NOVENO

Revelación de secretos, acceso ilícito a sistemas y equipos de informática y Delitos Informáticos

Artículo 211 bis 1.- Al que sin autorización **obstaculizare el funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de información y datos contenidos** en sistemas o equipos de informática protegidos **contra el acceso no autorizado,** se le impondrán de **dos a cuatro** años de prisión y de cien a trescientas **veces el valor diario de la Unidad de Medida y Actualización**.

Al que sin autorización copie información contenida en sistemas o equipos de informática protegidos **en contra del acceso no autorizado,** se le impondrán de **seis** meses a **dos años** de prisión y de **doscientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**

Artículo 211 bis 2.- Al que sin autorización **acceda,** modifique, destruya o provoque pérdida **parcial o total** de información contenida en sistemas o equipos de informática del Estado, protegidos **en contra del acceso no autorizado,** se le impondrán de uno a cuatro años de prisión y de **quinientas a mil veces el valor diario de la Unidad de Medida y Actualización.**

Al que sin autorización **acceda,** conozca o copie información **o datos contenidos** en sistemas o equipos de informática del Estado, protegidos **en contra del acceso no autorizado,** se le impondrán de seis meses a dos años de prisión y de **doscientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**

A quien sin autorización **acceda,** conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, **protegidos en contra del acceso no autorizado,** se le impondrá pena de cuatro a diez años de prisión **y de mil a dos mil veces el valor**

diario de la Unidad de Medida y Actualización. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública **o del sistema nacional de administración de justicia penal**, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

(...)

Artículo 211 bis 3.- Al que estando autorizado indebidamente modifique, destruya o provoque pérdida **parcial o total** de información **contenida en sistemas o equipos de informática del Estado**, se le impondrán de dos a ocho años de prisión y de trescientas a novecientas **veces el valor diario de la Unidad de Medida y Actualización**.

Al que estando autorizado, indebidamente copie información **o datos contenidos en sistemas o equipos de informática del Estado,** se le impondrán de **dos a ocho** años de prisión y de **cien a ochocientas veces el valor diario de la Unidad de Medida y Actualización.**

Al que estando autorizado, indebidamente obtenga, copie o utilice información **o datos contenidos en sistemas o equipos de informática en materia de seguridad pública**, se le impondrá pena de cuatro a diez años de prisión y multa de **mil a dos mil veces el valor diario de la Unidad de Medida y Actualización.** Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información **o datos contenidos** en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos **en contra del acceso no autorizado,** se le impondrán de seis meses a cuatro años de prisión y **multa de doscientas a mil doscientas veces el valor diario de la Unidad de Medida y Actualización.**

Al que sin autorización copie información **o datos contenidos** en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos **en contra del acceso no autorizado,** se le impondrán de tres meses a dos años de prisión y **multa de cien a seiscientas veces el valor diario de la Unidad de Medida y Actualización.**

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero indebidamente modifique, destruya o provoque pérdida de información **o datos contenidos en sistemas o equipos de informática,** se le impondrán de seis meses a cuatro años de prisión y multa de cien a seiscientas **veces el valor diario de la Unidad de Medida y Actualización.**

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie **información o datos contenidos en sistemas o equipos de informática,** se le impondrán de tres meses a dos años de prisión y **multa** de cincuenta a trescientas **veces el valor diario de la Unidad de Medida y Actualización.**

(...)

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información **o datos obtenidos** se **utilicen** en provecho propio o ajeno.

Artículo 211 bis 8.- A quien intercepte de forma dolosa y sin autorización por cualquier medio técnico, datos informáticos, información o comunicaciones dirigidas, originadas o efectuadas en o dentro de un sistema informático incluidas las emisiones electromagnéticas que transporten datos, información o comunicaciones, se le impondrá pena de cinco a diez años de prisión y multa de mil a dos mil veces el valor diario de la Unidad de Medida y Actualización.

CAPÍTULO III
Delitos Informáticos

Artículo 211 TER.- Abuso de Dispositivos.

Comete el delito de abuso de dispositivos quien, sin autorización, cometiere cualquiera de las siguientes actividades:

I. Producir, vender, obtener para su utilización, importar, difundir o de cualquier otra forma poner a disposición:

a) Cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en el Título Noveno de este Código; y

b) Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático con

intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.

II. Poseer alguno de los elementos previstos en los incisos a) o b) de la fracción primera del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.

III. Crear, utilizar, alterar, capturar, grabar, copiar o transferir de un dispositivo de acceso o un medio a otro similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y acceso al servicio o sistema informático que permita la operación paralela, simultánea o independiente de un servicio o sistema informático, legítimamente obtenido por un tercero; o bien, con la intención de que sean utilizados para cometer cualquiera de los delitos previstos en el Título Noveno de este Código.

Se impondrá pena de prisión de tres a cinco años y multa de doscientas a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización.

No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo primero del presente artículo no tenga por objeto la comisión de alguno de los delitos previstos en el Título Noveno, de este Código.

Artículo 211 QUÁTER.- Falsificación informática.

Comete delito de falsificación informática quien sin autorización introdujere, alterare, borrare o suprimiere datos informáticos previamente almacenados en un sistema informático, que generen datos no auténticos con la intención que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Se le impondrá pena de prisión de dos a tres años y multa de cien a cuatrocientas veces el valor diario de la Unidad de Medida y Actualización.

Se impondrá pena de tres a cinco años de prisión y multa de doscientas a quinientas veces el valor diario de la Unidad de Medida y Actualización en los casos siguientes:

a) Cuando los actos descritos en el párrafo anterior se realicen con la intención de cometer otro delito; y,

b) Cuando los actos descritos en el párrafo anterior se realicen para inducir a usuarios a la provisión de datos confidenciales, personales y/o financieros, tanto de personas físicas como de personas morales.

Artículo 211 QUINTUS.- Usurpación de Identidad Ajena.

A quien usurpe, suplante, obtenga, utilice, apropie o adopte la identidad de otra persona, a través de un sistema informático con la intención de causar un daño o perjuicio a una persona, se le impondrá pena de uno a cinco años de prisión y de cuatrocientas a seiscientas veces el valor diario de la Unidad de Medida y Actualización.

La misma pena se impondrá cuando la usurpación de identidad ajena se cometa infringiendo medidas de seguridad y con la intención de obtener de forma ilegítima un beneficio económico o lucro indebido para sí mismo o para otra persona o generar un daño en el patrimonio de una persona tanto física como jurídica.

Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

I. a XXI. (...)

XXII. A quien sin autorización causare un perjuicio patrimonial a otra persona, incluyendo a una persona moral, mediante la introducción, alteración, borrado o supresión de datos informáticos.

Las mismas penas se impondrán a quien interfiera en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para sí mismo o para un tercero.

ARTÍCULO SEGUNDO.- Se reforma la fracción II del artículo 439; y se adiciona la "Sección VII Actos de Investigación necesarios para la obtención de Evidencias Digitales", del Capítulo IV Disposiciones Generales Sobre la Prueba, del Título VIII Etapa del Juicio, del Libro Segundo Del Procedimiento, conteniendo los artículos 390 BIS 1 a 390 BIS 8; del Código Nacional de Procedimientos Penales, para quedar como sigue:

SECCIÓN VII
ACTOS DE INVESTIGACIÓN NECESARIOS PARA LA OBTENCIÓN DE EVIDENCIAS DIGITALES

Artículo 390 BIS 1. Disposiciones Generales

Los actos de investigación para la obtención de evidencias digitales, deberán considerar los supuestos previstos en la Constitución Política de los Estados Unidos Mexicanos, los instrumentos y tratados internacionales que versen sobre los derechos humanos de los que el Estado Mexicano sea parte, así como las garantías, principios y reglas que fundamentan el presente Código.

Artículo 390 BIS 2. Conservación de Datos Informáticos Almacenados

El Ministerio Público podrá ordenar a cualquier persona física o jurídica, la conservación de la integridad de los datos informáticos concretos, almacenados en un sistema informático que esté bajo su disposición cuando tenga motivos suficientes para considerar que puedan ser alterados o suprimidos y afectar así el resultado de una investigación. La medida no podrá exceder de noventa días y será prorrogable por igual período, si se mantienen los motivos que fundamentaron la orden.

La persona requerida, una vez que reciba la comunicación respectiva, deberá ejecutar los actos necesarios que garanticen la preservación, inmediata de los datos en cuestión y estará obligado a mantener secreto en los términos de lo previsto por la legislación penal aplicable.

Cuando se trate del aseguramiento o conservación de datos relativos al tráfico de comunicaciones, si el proveedor de servicios requerido advierte que en la comunicación objeto de la investigación han participado otros proveedores de servicios, informará inmediatamente a la autoridad competente que haga el requerimiento o solicitud, para que adopte las medidas necesarias.

Para llevar a cabo la conservación de la integridad de los datos informáticos almacenados en un sistema informático, se requerirá la autorización judicial del Juez de control y para ello, se estará a lo dispuesto en el tercer párrafo de artículo 291 y artículos 292 a 302 de este Código.

Artículo 390 BIS 3. Datos Almacenados de Usuarios o Abonados

El Ministerio Público podrá ordenar a cualquier persona física o jurídica, que presente, remita o entregue datos almacenados en un sistema informático que este bajo su poder o control y que se vinculen con la investigación de un delito concreto. Asimismo, podrá ordenar a toda persona física o jurídica que preste un servicio de comunicaciones o a los proveedores de servicios de cualquier tipo, la entrega de datos de los usuarios o abonados o los datos de identificación y facturación con los que cuente. La orden podrá contener la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de sanción penal en los términos de lo previsto por la legislación aplicable. Estas medidas serán ejecutadas por el Ministerio Público correspondiente, salvo las excepciones previstas en la legislación vigente, en las cuales se exija la autorización judicial del Juez de control.

Artículo 390 BIS 4. Registro y Preservación de Datos Almacenados

El órgano jurisdiccional podrá ordenar a solicitud del Ministerio Público, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:

I. Acceder a los componentes físicos y lógicos del sistema y,

II. Obtener copia de los datos en un soporte autónomo o

III. Preservar por medios tecnológicos o bloquear el acceso a los datos de interés para la investigación.

En los supuestos en los que, durante la ejecución de una medida de incautación de datos de un sistema Informático, previstos en el párrafo anterior, surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla o ampliar el registro al otro sistema. La ampliación del registro a los fines de la incautación deberá ser autorizada por el órgano jurisdiccional salvo que estuviera prevista.

Artículo 390 BIS 5. Datos Informáticos Almacenados en otro Estado

Con fundamento en lo dispuesto en los tratados y convenciones internacionales ratificados por el Estado Mexicano, las autoridades especializadas en la investigación de delitos del fuero federal o fuero común, incluida la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas adscrita a la Agencia de Investigación Criminal, podrán acceder o recibir datos informáticos almacenados en un sistema informático, ubicado en otro Estado, cuando éstos se encuentren accesibles en fuentes de acceso público, independientemente de la ubicación geográfica de los mismos; o a través de un sistema informático ubicado en México, si la autoridad investigadora competente obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos en ese país por medio de un sistema informático.

Artículo 390 BIS 6. Obtención de Datos en Tiempo Real

Para la obtención, en tiempo real, de datos de tráfico de comunicaciones electrónicas o la interceptación de datos informáticos de contenido, regirá lo dispuesto en los artículos 178 Bis del Código Penal Federal, 303 del Código Nacional de Procedimientos Penales y los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.

Artículo 390 BIS 7. Cooperación y Asistencia Jurídica en Materia Procesal Penal

En caso de cooperación y asistencia jurídica internacional, las solicitudes de aseguramiento de datos, solicitudes de presentación de datos, de obtención o confiscación, de acceso libre a fuentes de acceso público y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones, se estará a lo dispuesto en el Titulo XI de este Código, así como los tratados y convenciones internacionales ratificados por el Estado Mexicano. Asimismo, se tomará en cuenta el derecho a la intimidad y a la confidencialidad de ciertos datos protegidos bajo la legislación nacional vigente y tratados y convenciones internacionales en materia de derechos humanos ratificados por el Estado Mexicano.

Artículo 390 BIS 8. Protección de Datos Personales en Investigaciones

Las autoridades nacionales encargadas de investigar y perseguir delitos informáticos y el órgano jurisdiccional competente, deben respetar los principios y garantías individuales establecidas en la Constitución Política de los Estados Unidos Mexicanos, en convenios y tratados sobre derechos humanos ratificados por el Estado Mexicano, de tal forma que los derechos de las personas sean protegidos a través del uso de tecnologías de

información y comunicación, en particular el respeto a su intimidad y la protección de datos personales, tanto datos de tráfico como datos de contenido, salvo con fines legítimos para la prevención de delitos o la protección de los derechos y libertades de terceros.

Con respecto a la obtención y tratamiento de datos personales por parte de las instancias de seguridad, procuración y administración de justicia, se estará a lo dispuesto en los Artículos 80, 81 y 82 de la Ley General de Protección de Datos en Posesión de los Sujetos Obligados.

El tratamiento de datos personales para efectos de la investigación o como medio de prueba, deberá cumplir exclusivamente la finalidad para el que fueron originalmente obtenidos y tratados, por un tiempo de dos años y una vez cumplida la finalidad y propósito de investigación debe procederse a su cancelación y supresión.

La protección de la información y los datos personales es responsabilidad compartida de las autoridades en las distintas entidades que intervienen en la vigilancia, investigación y persecución penal de los delitos establecidos en el Código Penal Federal y otras leyes.

Artículo 439. Alcances

La asistencia jurídica comprenderá:

I. (...)

II. Obtención de pruebas, **incluidas las evidencias digitales o pruebas almacenadas en un sistema informático.**

III. a XI. (...)

TRANSITORIO

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

Dado en el Palacio Legislativo de San Lázaro, a 26 de abril de 2018

CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

Comisión de Justicia

Dictamen con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito.

POR LA COMISIÓN DE JUSTICIA

No.	FOTO	NOMBRE	FRACCIÓN	VOTO		
				A FAVOR	EN CONTRA	ABSTENCIÓN
1		**Ibarra Hinojosa Álvaro** Presidente	**PRI**			
2		**Domínguez Domínguez Cesar Alejandro** Secretario	**PRI**			
3		**Hernández Madrid María Gloria** Secretaria	**PRI**			
4		**Huicochea Alanís Arturo** Secretario	**PRI**			
5		**Ramírez Nieto Ricardo** Secretario	**PRI**			
6		**Cortés Berumen José Hernán** Secretario	**PAN**			

CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

Comisión de Justicia

Dictamen con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito.

No.	FOTO	NOMBRE	FRACCIÓN	VOTO		
				A FAVOR	EN CONTRA	ABSTENCIÓN
7		**Neblina Vega Javier Antonio** Secretario	**PAN**			
8		**Sánchez Carrillo Patricia** Secretaria	**PAN**			
9		**Ángel Olvera José Hugo** Secretario	**PRD**			
10		**Limón García Lia** Secretaria	**PVEM**			
11		**Sánchez Orozco Víctor Manuel** Secretario	**M.C.**			
12		**Álvarez López Jesús Emiliano** Integrante	**MORENA**			
13		**Basurto Román Alfredo** Integrante	**MORENA**			

CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

Comisión de Justicia

Dictamen con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito.

No.	FOTO	NOMBRE	FRACCIÓN	VOTO		
				A FAVOR	EN CONTRA	ABSTENCIÓN
14		**Bañales Arambula Ramón** Integrante	**PRI**			
15		**Canales Najjar Tristán Manuel** Integrante	**PRI**			
16		**Corzo Olán Omar** Integrante	**PRI**			
17		**González Navarro José Adrián** Integrante	**PAN**			
18		**González Torres Sofía** Integrante	**PVEM**			
19		**Gutiérrez Campos Alejandra** Integrante	**PAN**			
20		**Luna Canales Armando** Integrante	**PRI**			

CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

Comisión de Justicia

Dictamen con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito.

No.	FOTO	NOMBRE	FRACCIÓN	VOTO		
				A FAVOR	EN CONTRA	ABSTENCIÓN
21		**Martínez Urincho Alberto** Integrante	**MORENA**			
22		**Murrieta Gutiérrez Abel** Integrante	**PRI**			
23		**Ordoñez Hernández Daniel** Integrante	**PRD**			
24		**Ramírez Núñez Ulises** Integrante	**PAN**			
25		**Serna de León César Alberto** Integrante	**PRI**			
26		**Villagómez Guerrero Ramón** Integrante	**PRI**			

Cámara de Diputados del Honorable Congreso de la Unión, LXIII Legislatura

Junta de Coordinación Política

Diputados: Marko Antonio Cortés Mendoza, presidente, PAN; Carlos Iriarte Mercado, PRI; Francisco Martínez Neri, PRD; Jesús Sesma Suárez, PVEM; Virgilio Dante Caballero Pedraza, MORENA; Macedonio Salomón Tamez Guajardo MOVIMIENTO CIUDADANO; Luis Alfredo Valles Mendoza, NUEVA ALIANZA; José Alfredo Ferreiro Velazco, PES.

Mesa Directiva

Diputados: Édgar Romo García, presidente; vicepresidentes, Martha Sofía Tamayo Morales, PRI; Edmundo Javier Bolaños Aguilar, PAN; Arturo Santana Alfaro, PRD; María Ávila Serna, PVEM; secretarios, Sofía del Sagrario de León Maza, PRI; Mariana Arámbula Meléndez, PAN; Isaura Ivanova Pool Pech, PRD; Andrés Fernández del Valle Laisequilla, PVEM; Ernestina Godoy Ramos, MORENA; Verónica Bermúdez Torres, MOVIMIENTO CIUDADANO; María Eugenia Ocampo Bedolla, NUEVA ALIANZA; Ana Guadalupe Perea Santos, PES.

Secretaría General

Secretaría de Servicios Parlamentarios

Gaceta Parlamentaria de la Cámara de Diputados

Director: Juan Luis Concheiro Bórquez, **Edición:** Casimiro Femat Saldívar, Ricardo Águila Sánchez, Antonio Mariscal Pioquinto.

Apoyo Documental: Dirección General de Proceso Legislativo. **Domicilio:** Avenida Congreso de la Unión, número 66, edificio E, cuarto nivel, Palacio Legislativo de San Lázaro, colonia El Parque, CP 15969. Teléfono: 5036 0000, extensión 54046. **Dirección electrónica: http://gaceta.diputados.gob.mx/**