

ANÁLISIS TÉCNICO PRELIMINAR

No. Expediente: 4289-1PO3-17

I.- DATOS DE IDENTIFICACIÓN DE LA INICIATIVA

1. Nombre de la Iniciativa.	Que reforma y adiciona diversas disposiciones de los Códigos Penal Federal, y Nacional de Procedimientos Penales
2. Tema de la Iniciativa.	Justicia
3. Nombre de quien presenta la Iniciativa.	Dip. Sofía González Torres e integrantes del Grupo Parlamentario del PVEM y el Dip. Waldo Fernández González (PRD)
4. Grupo Parlamentario del Partido Político al que pertenece.	PVEM y PRD
5. Fecha de presentación ante el Pleno de la Cámara.	14 de noviembre de 2017
6. Fecha de publicación en la Gaceta Parlamentaria.	14 de noviembre de 2017
7. Turno a Comisión.	Justicia, con opinión de la Comisión Especial de las Tecnologías de Información y Comunicación

II.- SINOPSIS

Tipificar como delito al que intercepte sin autorización, sin permiso o consentimiento legalmente reconocido por cualquier medio técnico, datos informáticos, información o comunicaciones dirigidas, originadas o efectuadas en o dentro de un sistema informático o sistema que utilice sistemas de tecnologías de información y comunicación incluidas las emisiones electromagnéticas que transporten datos, información o comunicaciones. Agrupar los delitos informáticos de abuso de dispositivos, falsificación informática y usurpación de identidad ajena. Tipificar el fraude informático. Incorporar como medio de obtención de pruebas las evidencias digitales o pruebas almacenadas en un sistema informático o que utilice tecnologías de la información y comunicación.

III.- ANÁLISIS DE CONSTITUCIONALIDAD.

El derecho de iniciativa se fundamenta en la fracción II del artículo 71 y la facultad del Congreso de la Unión para legislar en la materia se sustenta en las fracciones XXI y XXIII del artículo 73, de la Constitución Política de los Estados Unidos Mexicanos.

IV.- ANÁLISIS DE TÉCNICA LEGISLATIVA

En la parte relativa al texto legal que se propone, se sugiere lo siguiente:

- Incluir el fundamento legal en que se sustenta la facultad del Congreso para legislar en la materia de que se trata.

La iniciativa cumple en general con los requisitos formales que se exigen en la práctica parlamentaria y que son los siguientes:

Ser formulada por escrito, tener un título, contener el nombre y firma de la persona que presenta la iniciativa, una parte expositiva de motivos, el texto legal que se propone, el artículo transitorio que señala la entrada en vigor, la fecha de elaboración y ser publicada en la Gaceta Parlamentaria.

dos mil *días multa*.

...

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.

Artículo 202 BIS.- Quien almacene, compre, arriende, 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 *quinientos días multa*. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

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*.

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



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

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

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*.

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*.

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*. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación 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**

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*.

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*.

A *quien* estando autorizado *para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública*, indebidamente obtenga, copie o utilice información *que contengan*, se le impondrá pena de 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.

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.



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

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*.

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*.

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*.

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*.

...

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**.

(...)



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

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.

- Sin correlativo vigente

- Sin correlativo vigente

- Sin correlativo vigente

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



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

- Sin correlativo vigente

- Sin correlativo vigente

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

- Sin correlativo vigente

- Sin correlativo vigente

- Sin correlativo vigente

Código.

Artículo 211 Quáter. Falsificación informática.

Comete delito de falsificación informática quien sin autorización introdujere, alterare, borrar 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,



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

- Sin correlativo vigente

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

I.- a XXI.- ...

- Sin correlativo vigente

- Sin correlativo vigente

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.

CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES

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

- Sin correlativo vigente

- Sin correlativo vigente

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

- Sin correlativo vigente

- Sin correlativo vigente

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



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

- Sin correlativo vigente

- Sin correlativo vigente

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.



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

- Sin correlativo vigente

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 Título 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 vigente

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.

- Sin correlativo vigente

Artículo 439. Alcances

La asistencia jurídica comprenderá:

I. ...

II. Obtención de pruebas;

III. a XI. ...

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. (...)



CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE APOYO PARLAMENTARIO
DIRECCIÓN DE APOYO A COMISIONES
SUBDIRECCIÓN DE APOYO TÉCNICO-JURÍDICO A COMISIONES

Transitorio

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