



J. Ricardo Fuentes G.

Diputado del Congreso de la Ciudad de México.
I Legislatura.

morena
La esperanza de México

Ciudad de México, a 29 de mayo de 2020
Oficio N° CCM/IL/JRFG/C19-35/20

**COORDINACIÓN DE SERVICIOS PARLAMENTARIOS
DEL CONGRESO DE LA CIUDAD DE MÉXICO
I LEGISLATURA
PRESENTE.**

De conformidad con lo establecido por los artículos 5 fracción I, 82, 95 Fracción II y 118 del Reglamento del Congreso de la Ciudad de México, le solicito de manera respetuosa, **sírvase enlistar en el Orden del Día de la próxima Sesión Ordinaria del año en curso**, la siguiente Iniciativa con Proyecto de Decreto bajo el siguiente Título:

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONAN LOS ARTÍCULOS 211 BIS 1 Y 211 BIS 2, AMBOS DEL CÓDIGO PENAL DEL DISTRITO FEDERAL, EN MATERIA DE DELITOS CIBERNÉTICOS.

Sin más por el momento, le envío un afectuoso saludo y adjunto al presente la iniciativa referida.

ATENTAMENTE



DIP. JESÚS RICARDO FUENTES GÓMEZ

Ciudad de México, a 29 de mayo de 2020.

**DIP. ISABELA ROSALES HERRERA
PRESIDENTA DE LA MESA DIRECTIVA
DEL CONGRESO DE LA CIUDAD DE MÉXICO
I LEGISLATURA
PRESENTE.**

El que suscribe, Diputado Jesús Ricardo Fuentes Gómez, integrante del Grupo Parlamentario del Partido MORENA, en la I Legislatura del Congreso de la Ciudad de México, con fundamento en los artículos 122 Apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 30, punto 1, inciso b), de la Constitución Política de la Ciudad de México; 12 fracción II de la Ley Orgánica del Congreso de la Ciudad de México y 95 fracción II y 96 del Reglamento del Congreso de la Ciudad de México, someto a consideración de esta Soberanía la **iniciativa con proyecto de decreto por el que se adicionan los artículos 211 bis 1 y 211 bis 2, ambos del Código Penal del Distrito Federal, en materia de delitos cibernéticos, de conformidad con la siguiente:**

EXPOSICIÓN DE MOTIVOS

I. Planteamiento del problema que la iniciativa pretende resolver y la solución que se propone.

La presente iniciativa propone incorporar en el texto del Código Penal del Distrito Federal, aquellos delitos que se cometan contra los sistemas informáticos de la Administración Pública de la Ciudad de México, con el objeto de causar un daño en la estabilidad del Estado, o bien que genere pérdidas en datos reservados o

confidenciales; relacionados con la seguridad, la administración de justicia, los aspectos económicos o financieros preponderantes, entre otros.

Además, se propone armonizar la presente iniciativa, con los diversos conceptos relacionados con los delitos cibernéticos, en términos de los previsto tanto en la jurisprudencia de la Suprema Corte de Justicia de la Nación como de la Corte Interamericana de Derechos Humanos, así como de los diversos tratados internacionales en materia de derechos humanos de los que el Estado mexicano es parte.

La aplicación tecnológica de los sistemas informáticos a la vida institucional es cada vez mayor cuantitativamente y cualitativamente. En este sentido, es necesario tomar las medidas necesarias de seguridad que permitan el buen uso de los mismos.

Lo anterior, toma relevancia al traer a colación diversos casos en los que han sido afectados dichos sistemas mediante la acción denominada "hackeo", el cual tiene un impacto negativo en el derecho de acceso a la información de quienes deseen ejercerlo. Tales fueron los casos de la página web del Gobierno del Estado de Tamaulipas hackeada el 12 de agosto de 2019, la de la Secretaría de Salud del Estado de Querétaro y la del Congreso de la Ciudad de México, ambas afectadas el pasado 18 de marzo.

El Congreso resultó gravemente afectado debido a la intervención o acto de mala fe, mejor conocido como "hackeo", toda vez que fueron eliminados gran parte de los archivos de su página Web y así mismo fue detectada la manipulación de algunos otros, por lo que la Mesa Directiva instruyó a la Dirección Jurídica de esta Soberanía a que levantara el acta correspondiente ante la Fiscalía para iniciar una investigación al respecto.

Sin embargo, la Fiscalía de la Ciudad de México no puede actuar, porque en el Código Civil del Distrito Federal no está tipificado el delito materia de la presente

iniciativa, razón por la cual la investigación ha sido atraída por la Fiscalía General de la República.

La vulneración de la página Web del Congreso atenta no sólo al trabajo de los diputados y sus colaboradores, sino a la memoria legislativa, los archivos, versiones estenográficas trabajos de comisiones y sobre todo, al acceso de la ciudadanía al portal de transparencia y a todos los datos que hacen posible la vinculación del Poder Legislativo con sus representados, dejando en estado de indefensión sus derechos humanos elementales.

En este sentido, se sustenta en la jurisprudencia del Tribunal Pleno, cuyo texto y rubro indican:¹

“DERECHOS HUMANOS CONTENIDOS EN LA CONSTITUCIÓN Y EN LOS TRATADOS INTERNACIONALES. CONSTITUYEN EL PARÁMETRO DE CONTROL DE REGULARIDAD CONSTITUCIONAL, PERO CUANDO EN LA CONSTITUCIÓN HAYA UNA RESTRICCIÓN EXPRESA AL EJERCICIO DE AQUÉLLOS, SE DEBE ESTAR A LO QUE ESTABLECE EL TEXTO CONSTITUCIONAL. El primer párrafo del artículo 1o. constitucional reconoce un conjunto de derechos humanos cuyas fuentes son la Constitución y los tratados internacionales de los cuales el Estado Mexicano sea parte. De la interpretación literal, sistemática y originalista del contenido de las reformas constitucionales de seis y diez de junio de dos mil once, se desprende que las normas de derechos humanos, independientemente de su fuente, no se relacionan en términos jerárquicos, entendiéndose que, derivado de la parte final del primer párrafo del citado artículo 1o., cuando en la Constitución haya una restricción expresa al ejercicio de los derechos humanos, se

¹ Visible en la página 202 del Libro 5, Abril de 2014, Tomo I, del semanario judicial y su gaceta; esto es, durante la Décima Época.

deberá estar a lo que indica la norma constitucional, ya que el principio que le brinda supremacía comporta el encumbramiento de la Constitución como norma fundamental del orden jurídico mexicano, lo que a su vez implica que el resto de las normas jurídicas deben ser acordes con la misma, tanto en un sentido formal como material, circunstancia que no ha cambiado; lo que sí ha evolucionado a raíz de las reformas constitucionales en comento es la configuración del conjunto de normas jurídicas respecto de las cuales puede predicarse dicha supremacía en el orden jurídico mexicano. Esta transformación se explica por la ampliación del catálogo de derechos humanos previsto dentro de la Constitución Política de los Estados Unidos Mexicanos, el cual evidentemente puede calificarse como parte del conjunto normativo que goza de esta supremacía constitucional. En este sentido, los derechos humanos, en su conjunto, constituyen el parámetro de control de regularidad constitucional, conforme al cual debe analizarse la validez de las normas y actos que forman parte del orden jurídico mexicano."

Al respecto, cabe precisar que los delitos cibernéticos en contra del Estado o de los sistemas informáticos del Estado, pueden poner en riesgo la estabilidad de los poderes públicos. Es así que, es menester de la Administración Pública de la Ciudad de México, salvaguardar los datos que se encuentran bajo su responsabilidad que sean considerados como reservados o confidenciales, además de proteger los datos personales y en esencia, toda información que sea para uso de sus instituciones o dependencias, en términos de los previsto en la Ley General de Acceso a la Información y Protección de Datos Personales y de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Tomando en cuenta que "México no es un país que esté a la vanguardia en términos académicos, legales o profesionales, en dicho tema (ciber-seguridad)"²; es necesario contar con un tipo penal que establezca sanciones para las personas que cometan ataques contra los sistemas o equipos computacionales.

Óscar Manuel Lira Arteaga señala que: "en relación con el desarrollo y utilización de programas de cómputo y sistemas operativos, es de considerar que desde su concepción implican altos riesgos de estabilidad y seguridad de los datos que procesan, dando como resultados un alto nivel de vulnerabilidad (...) ya sea consecuencia de la pérdida de su información o por los altos costos de mantenimiento y soporte de las aplicaciones informáticas."³

Por tanto, es menester de las diversas instituciones y dependencias de la Administración Pública de la Ciudad de México, generar políticas públicas óptimas y adecuadas para la protección de la información que se encuentre en sus sistemas informáticos. Luego entonces, esta iniciativa tiene por objeto instituirse de una política legislativa criminal para sancionar a las personas que cometen delitos de naturaleza cibernética, contra los sistemas informáticos del Gobierno de la Ciudad de México.

II. Objetivo de la propuesta y motivaciones y argumentos que la sustentan.

En un inicio es importante sostener que la Administración Pública de la Ciudad de México, tiene la calidad de sujeto obligado para la preservación, cuidado y protección de los datos personales e información que se encuentren en sus bases de datos o sistemas informáticos.

² MENDIETA, Susana, "Ciber-delitos dañan a empresas y gobierno", Milenio, 2020, Enero 14, visible en: <https://www.google.com.mx/amp/s/amp.milenio.com/negocios/ciberdelitos-danan>

³ LIRA ARTEGA, Óscar Manuel, "Delitos cibernéticos", Revista punto seguridad, seguridad en TIC, número 6, mayo 2010, ISSN-en tramite, p. 14.

El artículo 2º de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, dispone:

"Artículo 2. Toda la información generada o en posesión de los sujetos obligados es pública, considerada un bien común de dominio público, accesible a cualquier persona en los términos y condiciones que establece esta Ley y demás normatividad aplicable."

Del contenido de dicho artículo se desprende que toda la información que se genere por la Administración Pública de la Ciudad de México será pública, con excepción de que se establezca que su naturaleza es de carácter reservado o confidencial, cuya protección le corresponde a los sujetos obligados en términos del artículo 24, fracción VII de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

El proceso para obtener dicha información se fija en los términos que prevé la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, con el objeto de respetar los principios de certeza, legalidad, objetividad, transparencia y seguridad jurídica.

Es así que cualquier acceso a información de las bases o sistemas informáticos de la Administración Pública de la Ciudad de México fuera de los estándares previstos en la legislación local en materia de acceso a la información, presume su obtención ilegal, y en su caso, la actualización de una conducta señalada como delito, si es que así lo dispone el legislador ordinario.

Con base en las premisas anteriores, puede válidamente asegurarse que la obtención o bloqueo de información fuera de los esquemas normativos, es decir, sin autorización de la autoridad, institución o dependencia competente, constituye un riesgo para la estabilidad del Estado y es susceptible de tipificarse como un delito.

III. Fundamento legal y sobre su constitucionalidad y convencionalidad.

Es necesario realizar un ejercicio de control de constitucionalidad y convencionalidad para verificar que la iniciativa que se propone no presente vicios de esa naturaleza. Sin perder de vista que la propuesta consiste en tipificar en el Código Penal del Distrito Federal, el delito contra sistemas o equipos informáticos del Estado.

Sirve de apoyo a lo anterior la tesis aislada del Tribunal Pleno, cuyo texto y rubro indican:⁴

"CONTROL PREVIO DE LA CONSTITUCIONALIDAD DE PROYECTOS DE LEY APROBADOS POR LA LEGISLATURA LOCAL. SU ESTABLECIMIENTO NO AFECTA EL PRINCIPIO DE DIVISIÓN DE PODERES. Es válido que los Estados de la Federación establezcan medios de control para garantizar la supremacía constitucional mediante el contraste jurisdiccional entre una norma ordinaria y la Constitución local, ya sea que se ejercite de manera correctiva, como sucede en la acción de inconstitucionalidad, o preventiva, como ocurre en el control previo de la constitucionalidad de proyectos de ley aprobados por la Legislatura Local, antes de su promulgación y publicación, sin que ello afecte el principio de división de poderes."

En principio, es importante sostener que la Primera Sala de la Suprema Corte de Justicia de la Nación advierte la complejidad de establecer un sistema de proporcionalidad de las penas que obedezca a una lógica estricta de proporcionalidad en términos de niveles ordinales y no cardinales o absolutos de sanción, en este último caso, propia de la corriente retribucionista, es decir, un sistema en el que se distribuye la pena de acuerdo con principios de justicia derivados de las intuiciones compartidas por la comunidad.

⁴ Visible en la página 714 del Libro XIII, Octubre de 2012, Tomo 1, del semanario judicial y su gaceta; esto es, durante la Novena Época.

En ese contexto, para establecer que una pena como sanción no sea inconstitucional es necesario atender al hecho de que la pena sea acorde o no con el bien jurídico afectado. Es decir, con los derechos, principios o libertades tutelados y reconocidos por parte del Estado mexicano. Tomando en cuenta el contenido de los artículos 18 y 22, ambos de la Constitución Federal, con el objetivo de que no se establezca una pena desproporcional, así como, que la misma sea acorde con un sistema garantista, al que se aspira llegar en el sistema jurídico mexicano.

Sirve de apoyo a lo anterior la tesis aislada de la Primera Sala, cuyo texto y rubro indican:⁵

“PROPORCIONALIDAD DE LAS PENAS. SUS DIFERENCIAS CON EL TEST DE PROPORCIONALIDAD EN DERECHOS FUNDAMENTALES. El término "proporcionalidad" es ambiguo, ya que puede predicarse del test de proporcionalidad en materia de derechos fundamentales, o de las penas, en términos del artículo 22 constitucional. Así, en el primer caso, lo que se analiza es una relación entre principios, entendidos como mandatos de optimización que ordenan que algo debe realizarse en la mayor medida posible (de acuerdo con las posibilidades fácticas y normativas existentes). Los conflictos entre principios (o entre derechos así concebidos) deben resolverse aplicando un test de proporcionalidad, que viene a ser una especie de meta-principio o, si se quiere, el principio último del ordenamiento jurídico. Ese principio consta, a su vez, de tres sub-principios: el de idoneidad, el de necesidad y el de proporcionalidad en sentido estricto o ponderación. Los dos primeros se refieren a la optimización en relación con las posibilidades fácticas. Significa que una medida, esto es, una ley o una sentencia, etcétera, que limita un

⁵ Visible en la página 590 del Libro 10, Septiembre de 2014, Tomo I, del semanario judicial y su gaceta; esto es, durante la Décima Época.

derecho o un bien constitucional de considerable importancia para satisfacer otro, debe ser idónea para obtener esa finalidad y necesaria, o sea, no debe ocurrir que la misma finalidad pudiera alcanzarse con un costo menor. El tercer sub-principio, por el contrario, tiene que ver con la optimización en relación con las posibilidades normativas. En cambio, en el caso de la proporcionalidad de penas, regularmente se analiza una regla (el tipo penal de que se trate) frente a un principio constitucional (el principio de proporcionalidad establecido en el artículo 22 constitucional), con la finalidad de determinar si aquella -la regla- satisface o no la exigencia del principio constitucional; concretamente, si la pena es acorde o no en relación con el bien jurídico afectado. En estos casos, es posible adoptar cualquier metodología encaminada a la justificación exigida por el artículo 22, dejando fuera, naturalmente, un análisis de proporcionalidad en materia de derechos fundamentales, dado que en este tipo de casos no se está ante la colisión de dos principios.”

Así, los principios tutelados son los siguientes:

1. La paz;
2. La estabilidad estatal;
3. La seguridad estatal, y
4. La protección de datos personales, o información reservada o confidencial.

De ahí que se estime necesario, en un primer momento, esclarecer su fundamento acorde con el “parámetro de regularidad constitucional” y en un segundo término, realizar un test de proporcionalidad de la pena, para verificar que la medida que se pretende (penal), no vulnere los estándares constitucionales y convencionales.

En cuanto a los principios de paz y estabilidad estatal, cabe destacar que el artículo 21, apartado b), de la Constitución Política de los Estados Unidos Mexicanos, señala que le corresponde al Estado a cargo de la Federación, las

entidades federativas y los Municipios, salvaguardar entre otros, los principios de orden público y la paz social.

Además de que, es necesario contar con los mecanismos adecuados para salvaguardar la seguridad pública o ciudadana, con el objetivo de que no se genere un menoscabo en los derechos fundamentales de las personas que habitan en el Estado mexicano o bien, en las instituciones públicas que integran el mismo.

Asimismo, el Estado mexicano, tiene la obligación por mandato de los artículos 6º y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, de proteger la información que tiene bajo su resguardo, así como de salvaguardar los datos personales que los que se cuenta como sujeto obligado.

Cabe destacar que el artículo 2º de la Convención de Budapest sobre delitos cibernéticos, establece que los Estados parte, tienen la facultad de establecer como delito, el acceso indebido o ilícito a los sistemas informáticos. Con el objetivo de proteger sus sistemas o datos informáticos, tal como lo prevé el artículo 1º del citado instrumento internacional.

Es por ello que, esta iniciativa busca establecer la tipificación de los delitos que tiendan a intervenir de manera ilegítima los sistemas o datos informáticos, así como los actos que tiendan a dañar, borrar, deteriorar, alterar o suprimir datos informáticos, tanto de particulares como del Estado.

En ese contexto, es claro que la tipificación de los delitos contra sistemas o datos informáticos del Estado, es necesaria y de observancia vinculante, en aras de armonizar la legislación penal de la Ciudad de México con lo señalado en la Convención de Budapest sobre delitos cibernéticos.

Test de proporcionalidad de la pena

Para establecer la proporcionalidad de las penas, regularmente se analiza una regla (el tipo penal de que se trate) frente a un principio constitucional (el principio de proporcionalidad establecido en el artículo 22 constitucional), con la finalidad de determinar si aquélla -la regla- satisface o no la exigencia del principio constitucional; concretamente, si la pena es acorde o no en relación con el bien jurídico afectado.

La Primera Sala de la Suprema Corte de Justicia de la Nación ha establecido que de conformidad con el artículo 22 de la Constitución Política de los Estados Unidos Mexicanos, la gravedad de la pena debe ser proporcional a la del hecho antijurídico y del grado de afectación al bien jurídico protegido, de manera que las penas más graves deben dirigirse a los tipos penales que protegen los bienes jurídicos más importantes.⁶

La Corte Constitucional Colombiana, ha definido que tanto la tipificación penal de una conducta como la fijación de la pena, son asuntos que se enmarcan dentro de la competencia del legislador.⁷ En tal sentido, este Congreso de la Ciudad de México, tiene la facultad de establecer la pena que mejor proteja los principios constitucionales antes citados, con el objetivo de que exista una racionalidad y proporcionalidad de la misma.

a) Regla prevista en el Código Penal local.

Es de señalarse que en la Legislación Penal de la Ciudad de México, no existe un tipo penal específico para poder establecer los delitos que se cometan contra los sistemas o datos informáticos del Estado. Por lo que existe la necesidad de que este Congreso, genere un tipo detallado y pormenorizado que cumpla con el principio de taxatividad.

⁶ Visible en la página 1407 del Libro 15, Febrero de 2015, Tomo II, del semanario judicial y su gaceta; esto es, durante la Décima Época.

⁷ BERNAL PULIDO, Carlos, *El derecho de los derechos*, Colombia, Universidad del Externado, 2005, p. 117.

b) Principios tutelados.

Como se dijo, los principios constitucionales tutelados en el caso, son la paz y estabilidad estatal, el orden público, la seguridad pública o ciudadana, y el acceso a la información y la protección de datos personales por parte de sujetos obligados.

c) Grado de afectación.

En cuanto al grado de afectación, debe decirse que los delitos contra los sistemas o datos informáticos de propiedad del Estado, genera una afectación grave a los principios de paz y estabilidad estatal, orden público, la seguridad pública o ciudadana y el acceso a la información y la protección de datos personales por parte de sujetos obligados.

Bajo esas premisas, se estima que existe una relación entre la regla que se pretende establecer y los principios tutelados, lo cual genera que la pena impuesta sea proporcionalidad y por tanto, respete los estándares constitucionales, bajo una perspectiva de constitucionalismo garantista.

IV. Ordenamiento a modificar

Para mayor claridad en el análisis de la propuesta materia de la presente iniciativa, expongo en el siguiente cuadro comparativo la **adición de los artículos 211 bis 1 y 211 bis 2, ambos del Código Penal del Distrito Federal, en materia de delitos cibernéticos:**



TEXTO VIGENTE	TEXTO PROPUESTO
<p style="text-align: center;">Capítulo III USURPACIÓN DE IDENTIDAD</p> <p>Artículo 211 Bis.-</p> <p>(Sin correlativo)</p>	<p style="text-align: center;">Capítulo III USURPACIÓN DE IDENTIDAD E INTERVENCIÓN EN SISTEMAS Y DATOS INFORMÁTICOS</p> <p>Artículo 211 Bis.-</p> <p>Artículo 211 bis 1.- Al que sin autorización, borre, suprima, modifique, altere, destruya, elimine o provoque pérdida de información contenida en sistemas o datos informáticos protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas unidades de medida y actualización diarias.</p> <p>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 multa de cincuenta a ciento cincuenta unidades de medida y actualización diarias.</p> <p>Artículo 211 bis 2.- Al que sin autorización, borre, suprima, modifique, altere, destruya, elimine, falsifique, o provoque pérdida de información contenida en sistemas o datos informáticos del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y multa de doscientos a seiscientas unidades de medida y actualización diarias.</p> <p>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 multa de</p>



J. Ricardo Fuentes G.

Diputado del Congreso de la Ciudad de México.
I Legislatura.

morena
La esperanza de México

LEGISLATURA

	<p>cien a trescientas unidades de medida y actualización diarias.</p> <p>A quien sin autorización conozca, obtenga, venda, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad ciudadana, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil unidades de medida y actualización diarias.</p> <p>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. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.</p>
--	--

V. Denominación del proyecto de ley o decreto y texto de la propuesta

Por lo anteriormente expuesto y fundado, someto a consideración de este H. Congreso de la Ciudad de México la siguiente iniciativa con proyecto de decreto por el que se **adicionan los artículos 211 bis 1 y 211 bis 2, ambos del Código Penal del Distrito Federal, en materia de delitos cibernéticos:**

Por las consideraciones expuestas, se somete al pleno de este honorable Congreso de la Ciudad de México, la presente **iniciativa con proyecto de decreto por el que se adicionan los artículos 211 bis 1 y 211 bis 2, ambos del**

Código Penal del Distrito Federal, en materia de delitos relacionados con la intervención en sistemas y datos informáticos, para quedar como sigue:

“SISTEMAS Y DATOS INFORMÁTICOS

Artículo 211 bis 1.- Al que, sin autorización, borre, suprima, modifique, altere, destruya, elimine o provoque pérdida de información contenida en sistemas o datos informáticos protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas unidades de medida y actualización diarias.

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 multa de cincuenta a ciento cincuenta unidades de medida y actualización diarias.

Artículo 211 bis 2.- Al que sin autorización, borre, suprima, modifique, altere, destruya, elimine, falsifique, o provoque pérdida de información contenida en sistemas o datos informáticos del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y multa de doscientos a seiscientas unidades de medida y actualización diarias.

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 multa de cien a trescientas unidades de medida y actualización diarias.

A quien sin autorización conozca, obtenga, venda, copie o utilice información contenida en cualquier sistema, equipo o medio de

almacenamiento informáticos de seguridad ciudadana, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil unidades de medida y actualización diarias.

Si el responsable es o haya sido servidor público, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes."

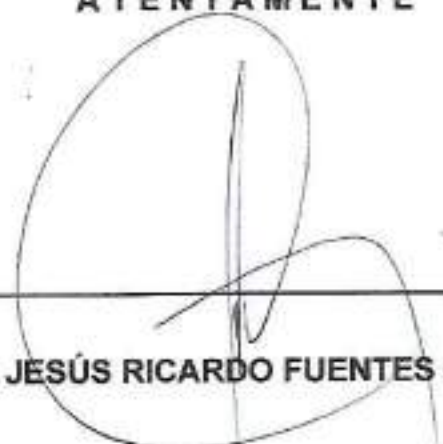
ARTÍCULOS TRANSITORIOS

PRIMERO. - El presente Decreto entrará en vigor el día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. - Publíquese en la Gaceta Oficial de la Ciudad de México para su conocimiento y en el Diario Oficial de la Federación para su mayor difusión.

Dado en el Recinto Legislativo de Donceles a los 29 días del mes de mayo de 2020.

ATENTAMENTE



DIP. JESÚS RICARDO FUENTES GÓMEZ