

DE LA COMISIÓN DE JUSTICIA CON PROYECTO DE DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES AL CÓDIGO PENAL FEDERAL

Honorable Asamblea:

A la Comisión de Justicia de la LXI Legislatura, le fueron turnadas para su estudio, análisis y dictamen correspondiente, las iniciativas con proyecto de decreto por el que se reforman y adicionan diversas disposiciones al Código Penal Federal, y con proyecto de decreto que reforma el artículo 211 Bis 5 del Código Penal Federal, en Materia de delitos en contra de medios o sistemas informáticos o cometidos mediante el uso o empleo de éstos.

La Comisión de Justicia de la Cámara de Diputados del honorable Congreso de la Unión, de la LXI Legislatura, de conformidad con lo dispuesto en los artículos 70, 71, 72 y 73 de la Constitución Política de los Estados Unidos Mexicanos; 39 y 45, numeral 6, incisos e) y f), de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; y 80, 157, numeral 1, fracción I, 158, numeral 1, fracción IV y 167, numeral 4, del Reglamento de la Cámara de diputados, somete a la consideración de esta honorable asamblea, el presente dictamen de conformidad con los siguientes

Antecedentes

1. En sesión del pleno de fecha 29 de noviembre de 2011, los diputados Juan José Guerra Abud y Rodrigo Pérez-Alonso González, sometieron a consideración de esta soberanía, la iniciativa con proyecto de decreto que reforma y adiciona diversas disposiciones al Código Penal Federal.
2. En la misma fecha, la Mesa Directiva acordó turnar la iniciativa que nos ocupa a la Comisión de Justicia, para su estudio y dictamen correspondiente.
3. En sesión celebrada el 9 febrero de 2012 por la Cámara de diputados del honorable Congreso de la Unión, el diputado Canek Vázquez Góngora del Grupo Parlamentario del Partido Revolucionario Institucional, presentó la iniciativa con proyecto de decreto por el que se reforma el artículo 211 Bis 5 del Código Penal Federal.
4. En la misma fecha, la Mesa Directiva, mediante oficio D.G.P.L. 61-II-4-2398, turnó la Iniciativa en comento a la Comisión de Justicia, para efectos de su estudio, análisis y dictamen correspondiente.

Derivado de lo anterior, dicha comisión realizó diversos trabajos a efecto de revisar los contenidos de las citadas Iniciativas, con el objeto de expresar sus observaciones y comentarios a las mismas e integrar el presente dictamen.

Contenido de las iniciativas

A) Iniciativa de los diputados Juan José Guerra Abud y Rodrigo Pérez-Alonso González

La iniciativa propone sancionar diversas conductas que se cometen en perjuicio de los bienes y medios informáticos o que se perpetran con el empleo de los mismos.

Los legisladores proponentes señalan que los avances en el campo de las tecnologías de la información y las comunicaciones, sobre todo en lo que refiere al uso o empleo de herramientas informáticas, han propiciado el desarrollo y competitividad de los países, al tiempo que generan y facilitan infinidad de relaciones y oportunidades de interacción en los distintos ámbitos de la vida social, política, económica y productiva de las personas e instituciones, al tiempo que promueven la rapidez y eficiencia de servicios y la transmisión inmediata de información entre usuarios, gobiernos y diversos sectores de la sociedad.

La Comisión de Justicia coincide con los proponentes al señalar que no obstante las bondades que tales avances representan, la interacción y el intercambio de información de todo tipo que dichos instrumentos promueven debe realizarse de forma segura y confiable y sobre todo libre de los peligros que representa la posibilidad de usar a las

herramientas informáticas para transgredir, violentar o dañar a los propios bienes informáticos o al emplear éstos para cometer diversas conductas delictivas en perjuicio de las personas e instituciones que se valen de los mismos para el desarrollo de sus actividades económicas, empresariales, financieras, de gobierno o de servicios en general.

Del mismo modo, la comisión concuerda en la necesidad que expresan los diputados de tutelar diversos bienes jurídicos que actualmente no gozan de la protección del derecho, por lo que se encuentran expuestos a los ataques de individuos que aprovechando los vacíos legales y por ende, los espacios de impunidad que éstos generan, lesionan los mencionados bienes con métodos y mecanismos hasta hace poco desconocidos, por lo que es necesario actualizar el catalogo de delitos en los que se establezcan las penas que correspondan a tales conductas.

A fin de lograr tal objetivo, los autores plantean, como eje de la presente iniciativa, reformar y adicionar diversas disposiciones previstas en el Capítulo II denominado “Acceso ilícito a sistemas y equipos de informática”, el cual forma parte del Título Noveno del Código Penal Federal, con lo que proponen actualizar el catalogo de los llamados “delitos informáticos”, es decir aquellas conductas que atentan contra bienes, medios y sistemas informáticos tanto del Estado como de la esfera jurídica de los particulares.

En forma paralela, la iniciativa plantea incorporar a la legislación penal la descripción típica de diversas conductas relacionadas con la trata de personas, la divulgación ilícita de información, los delitos cometidos contra la paz y la seguridad de las personas entre los que se encuentran las amenazas y los delitos patrimoniales como el fraude y la extorsión, en los casos que dichos delitos se cometen mediante el uso o empleo de los medios o sistemas informáticos, es decir, que en estos casos estamos en presencia de delitos informáticos no porque se atente contra bienes de dicha naturaleza, sino porque éstos se utilizan como instrumentos o medios comisivos para la perpetración de las conductas ilícitas referidas.

Esta comisión coincide con los proponentes al señalar que la nueva realidad en materia del uso de las tecnologías en la vida cotidiana de las personas e instituciones, ha propiciado que emerjan nuevos fenómenos delictivos lo cual implica un desafío al Estado debido a la necesidad de responder a las preguntas acerca de la posibilidad de regulación y monitoreo de los sistemas. Lo anterior con el fin de promover la prevención y persecución de delitos que afecten a los bienes jurídicos de personas e instituciones.

A fin de abundar en lo anterior, los diputados promoventes mencionan que poco a poco, los países recientemente han estado impulsando reformas en materia de delitos informáticos, con el fin de adecuar las legislaciones a la nueva realidad y la irrupción de las nuevas tecnologías a la vida de personas y las instituciones, públicas y privadas.

En el mismo sentido, los diputados que suscriben la iniciativa, afirman que a nivel internacional, diversos organismos e instituciones han promovido proyectos, mecanismos, convenios y otros instrumentos que buscan reflejar estas nuevas relaciones y conductas con el fin de tipificar las conductas delictivas relacionadas con los delitos informáticos y que implican un grave riesgo y vulnerabilidad para la vida y seguridad de las personas, su patrimonio afectando la confianza en las instituciones.

Entre ellas destacan tres figuras relevantes que marcan un antecedente en la categorización de los delitos informáticos, mismos que los Legisladores promoventes de la iniciativa señalan con precisión, a saber, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también llamado Convenio de Budapest; la Ley Modelo de la Commonwealth sobre Delitos Informáticos y relacionados con la Informática y el Proyecto de Convenio de Stanford, instrumentos que despliegan una lista de delitos, describiendo los tipos y bienes tutelados.

Como se advierte en ellos, se presentan recomendaciones de política pública y medidas legislativas a consideración y suscripción de los gobiernos.

Asimismo, y como señalan los Legisladores proponentes, organismos multilaterales y regionales entre los cuales destacan la Organización para la Cooperación y Desarrollo Económicos, la Organización de las Naciones Unidas, la Unión Internacional de Telecomunicaciones han emprendido iniciativas y proyectos con el fin de analizar el

fenómeno de los delitos informáticos, encontrar mecanismos de prevención y disminución de las vulnerabilidades al igual que promover la coordinación y cooperación internacional en la lucha contra los delitos informáticos.

En este sentido, los legisladores que suscriben la iniciativa documentan que en materia internacional, se han promovido diversos instrumentos mecanismos de colaboración y recomendación con el fin de armonizar y actualizar las disposiciones nacionales, en primer lugar, en materia penal, para incluir y tipificar los delitos informáticos.

A continuación se señalan los principales instrumentos y convenios.

Organismo	Instrumento
Organización para la Cooperación y Desarrollo Económicos (OCDE)	Líneas respecto a la Seguridad de los Sistemas de Información y Redes. (2002) y ha establecido diversas reuniones y recomendaciones.
Unión Internacional de Telecomunicaciones (UIT)	Agenda global de ciberseguridad en 2007.
APEC (Asian Pacific Economic Cooperation, por sus siglas en inglés)	En 2001 se condena el terrorismo, incluido a las telecomunicaciones Declaración de Shangai, que incluye una Declaratoria de la Seguridad de la infraestructura de la Información y Telecomunicaciones y un Programa de Acción (2002). Grupo de Trabajo TEL WG, sobre ciberseguridad.
Organización de Estados Americanos	Creación de un grupo de trabajo de expertos en cibercrimen, aprobándose en 2004 las recomendaciones y conclusiones.
Comunidad Europea	Creación de ley modelo relacionada con Computadoras y Delitos relacionados con ella (2002.)
Asociación de Naciones del Sureste de Asia	Se acuerda la estrategia relacionada con ciberseguridad y prevenir y combatir el cibercrimen (2003).
Organización de las Naciones Unidas Convención de Naciones Unidas contra la Delincuencia Organizada y otras instancias.	Emite diversas recomendaciones y reuniones.
Organismos regionales: G8, la Liga Árabe y la Unión Africana.	Se establecen medidas y estrategias

Por otra parte, estudios nacionales e internacionales documentan el incremento en la incidencia delictiva en materia de delitos informáticos.

El Informe de Delitos Cibernéticos de Norton 2011, comentado en la iniciativa, describe el impacto de los delitos informáticos en la vida de 24 naciones, incluido el caso de México. Como es de observarse, existe una tendencia creciente en la comisión de este tipo de delitos y por otra parte, el efecto en términos monetarios representa un monto considerable respecto de la actividad económica, el patrimonio y la seguridad de los mexicanos.

De acuerdo a la iniciativa, el Informe señala que el monto que los adultos en 24 países erogaron por las actividades del llamado cibercrimen superaron los 388 mil millones de dólares, lo que comprende dos elementos; en primer lugar, el gasto que tuvieron que efectuar por el tiempo y dinero perdidos por el cibercrimen, lo cual representa un monto de 114 mil millones de dólares debido al dinero robado por los delincuentes o bien, al monto gastado en resolver los ataques cibernéticos, y en segundo lugar, un monto de 274 mil millones de dólares derivado del tiempo perdido valuado por las víctimas.

De acuerdo a la propia encuesta, este monto es casi equivalente al del comercio ilegal de marihuana, cocaína y heroína que equivale a 288 mil millones de dólares o bien, todo el comercio ilegal de drogas, valuado en 411 mil millones de dólares. Los delitos de mayor incidencia se refieren a los virus informáticos (malware), el de la estafa y el *phishing* .

Igualmente, la encuesta menciona tres características del caso mexicano. En primer lugar, el sector más afectado es el de los usuarios de mayor uso del Internet; siendo el delito más común el de los virus informáticos, también llamados malware, en el cual México es el de mayor incidencia de la lista de países analizados, con un 71 por ciento de adultos en línea afectados.

En tercer lugar destaca el hecho de que el 83 por ciento de los adultos han sido víctimas del cibercrimen.

La iniciativa hace un análisis de los tipos de delitos informáticos en función de las posibilidades de acceso y uso de las tecnologías en la vida cotidiana y su grado de afectación y bien jurídico tutelado y detalla el tipo de delitos con el fin de proponer reformas al Código Penal incluyendo este tipo de conductas y su sanción respectiva.

Derivado de lo anterior, y en correspondencia con esta tendencia internacional y al aumento de la incidencia delictiva, esta Comisión concuerda con la necesidad de fortalecer el marco jurídico mexicano en materia de delitos informáticos, resultando evidente la exigencia y urgencia de actualizar el Código Penal Federal y reconocer la existencia de nuevos tipos penales.

Por ello, coincidimos con la iniciativa objeto del presente dictamen en que las acciones deben ser reforzadas con una política de Estado que evite la afectación de los mexicanos y los bienes jurídicos mediante un cuerpo normativo adecuado a la innovación y uso de las tecnologías.

Los diputados integrantes de esta comisión dictaminadora coinciden en la necesidad de reformar el Código Penal con el fin de tipificar diversas conductas relacionadas con el uso de los medios y sistemas informáticos, en contra de ellos, o mediante el uso o empleo de los mismos.

B) Iniciativa del diputado Canek Vázquez Góngora

Esta iniciativa encuentra su justificación en algunos de los siguientes argumentos:

A través del tiempo hemos atestiguado como la tecnología ha logrado ser un medio cada vez más accesible para el usuario común.

Sin embargo, dichos avances tecnológicos, han traído también como resultado un mayor ingenio y creatividad para la comisión de nuevos delitos, cuyo medio es la red abierta conocida como Internet o el acceso a equipos tecnológicos y sus respectivas bases de datos.

Así, a través de ella, se tiene acceso a bases de datos con contenido personal, financiero, laboral y médico, entre otros, vulnerando en ocasiones al usuario en su privacidad, su economía y su integridad moral o física.

Actualmente, el clima de inseguridad que lastima profundamente la vida social de nuestro país, y por ende su gobernabilidad, se abona ante la colusión de diversos miembros de nuestra sociedad, entre los que destacan en buena medida aquellos cuyo marco de acción les permite el acceso a información personal como son las cuentas bancarias y datos personales de los usuarios.

Aunado a lo anterior, cabe destacar que en materia de delitos informáticos se derivan otras figuras, tales como el acoso, la extorsión y que en otras circunstancias pudieran conducir a delitos más graves como la privación ilegal de la libertad. En este caso, las autoridades han confirmado que los inculcados en el delito de secuestro en diversas ocasiones han obtenido información de la víctima auxiliándose del internet o teniendo acceso a información proporcionada por otra persona, logrando con ello seguir de cerca a su víctima en lo referente a su agenda laboral, académica, económica, financiera y social, utilizando las herramientas tecnológicas como una arma que amenaza la seguridad del usuario, y no una herramienta para simplificar sus tareas.

Las instituciones bancarias han sufrido a su vez grandes pérdidas en lo referente a transferencias no autorizadas, acceso indebido a los sistemas y modificación de estos, así como la obtención de números de cuentas bancarias, tarjetas de crédito o débito, números confidenciales de seguridad y de acceso, entre otros.

Análisis comparativo

a) Iniciativa de los diputados Juan José Guerra Abud y Rodrigo Pérez-Alonso González

La comisión reitera la preocupación de los diputados promoventes y reconoce que, en el caso de delitos que atentan contra la infancia como el de la pornografía infantil, corrupción de menores y turismo sexual, y la trata de personas menores de dieciocho años o de personas que no tienen capacidad de comprender el significado del hecho o que no tienen capacidad para resistirlo, hay una tendencia al uso de las tecnologías y el Internet.

Al respecto, se modifica el artículo 205 Bis de acuerdo a lo siguiente:

Texto vigente

Capítulo V

Trata 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

Artículo 205 Bis. Las sanciones señaladas en los artículos 200, 201, 202, 203 y 204 se aumentarán al doble de la que corresponda cuando el autor tuviere para con la víctima, alguna de las siguientes relaciones:

- a) Los que ejerzan la patria potestad, guarda o custodia;
- b) Ascendientes o descendientes sin límite de grado;
- c) Familiares en línea colateral hasta cuarto grado;
- d) Tutores o curadores;
- e) Aquél que ejerza sobre la víctima en virtud de una relación laboral, docente, doméstica, médica o cualquier otra que implique una subordinación de la víctima;
- f) Quien se valga de función pública para cometer el delito;
- g) Quien habite en el mismo domicilio de la víctima;
- h) Al ministro de un culto religioso;
- i) Cuando el autor emplee violencia física, psicológica o moral en contra de la víctima; y
- j) Quien esté ligado con la víctima por un lazo afectivo o de amistad, de gratitud, o algún otro que pueda influir en obtener la confianza de ésta.

En los casos de los incisos a), b), c) y d) además de las sanciones señaladas, los autores del delito perderán la patria potestad, tutela o curatela, según sea el caso, respecto de todos sus descendientes, el derecho a alimentos que pudiera corresponderle por su relación con la víctima y el derecho que pudiera tener respecto de los bienes de ésta.

En los casos de los incisos e), f) y h) además de las sanciones señaladas, se castigará con destitución e inhabilitación para desempeñar el cargo o comisión o cualquiera otro de carácter público o similar, hasta por un tiempo igual a la pena impuesta.

En todos los casos el juez acordará las medidas pertinentes para que se le prohíba permanentemente al ofensor tener cualquier tipo de contacto o relación con la víctima.

Propuesta de reforma

Capítulo V

Trata 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

Artículo 205 Bis. Las sanciones señaladas en los artículos 200, 201, 202, 203 y 204 se aumentarán al doble de la que corresponda cuando el autor tuviere para con la víctima, alguna de las siguientes relaciones:

- a) Los que ejerzan la patria potestad, guarda o custodia;
- b) Ascendientes o descendientes sin límite de grado;
- c) Familiares en línea colateral hasta cuarto grado;
- d) Tutores o curadores;
- e) Aquél que ejerza sobre la víctima en virtud de una relación laboral, docente, doméstica, médica o cualquier otra que implique una subordinación de la víctima;
- f) Quien se valga de función pública para cometer el delito;
- g) Quien habite en el mismo domicilio de la víctima;
- h) Al ministro de un culto religioso;
- i) Cuando el autor emplee violencia física, psicológica o moral en contra de la víctima; y
- j) Quien esté ligado con la víctima por un lazo afectivo o de amistad, de gratitud, o algún otro que pueda influir en obtener la confianza de ésta.
- k) Quien se valga del uso o empleo de medios informáticos para generar relación de confianza o amistad con la víctima.**

En los casos de los incisos a), b), c) y d) además de las sanciones señaladas, los autores del delito perderán la patria potestad, tutela o curatela, según sea el caso, respecto de todos sus descendientes, el derecho a alimentos que pudiera corresponderle por su relación con la víctima y el derecho que pudiera tener respecto de los bienes de ésta.

En los casos de los incisos e), f) y h) además de las sanciones señaladas, se castigará con destitución e inhabilitación para desempeñar el cargo o comisión o cualquiera otro de carácter público o similar, hasta por un tiempo igual a la pena impuesta.

En todos los casos el juez acordará las medidas pertinentes para que se le prohíba permanentemente al ofensor tener cualquier tipo de contacto o relación con la víctima.

Como es posible observar, se propone castigar con mayor severidad a quien emplee estos medios informáticos para fines y conductas delictivas. Igualmente, esta propuesta está en concordancia con las recientes reformas legales que castigan severamente la trata de personas.

La iniciativa propone modificaciones al Código Penal Federal en los siguientes aspectos.

En primer lugar, se penalizan conductas relacionadas con el acceso y la intervención ilícitas, el ataque contra la integridad del sistema y la manipulación de datos, el robo de identidad y la utilización indebida de dispositivos, así como la revelación de secretos relativa a información contenida en equipos informáticos obtenida a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos o través de la suplantación de identidad.

Estas conductas que atentan en contra de sistemas informáticos del Estado, los del sistema financiero y cualquier otra institución o persona en general.

En segundo lugar, en materia de sistemas financieros y respecto al lavado de dinero y el encubrimiento de las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento, se penaliza la realización o encubrimiento a través de medios electrónicos en la comisión de este delito.

Lo anterior de acuerdo al comparativo siguiente:

Texto vigente

Título Noveno

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

Capítulo I

Revelación de secretos

Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

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.

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 cuatro a diez años 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.

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.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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.

Propuesta de reforma

Título Noveno

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

Capítulo I

Revelación de secretos

Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Se impondrán las mismas penas que refiere el párrafo anterior a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad.

Capítulo II

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.

Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos de informática o mediante cualquier mecanismo que de manera próxima o remota les cause un daño.

En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.

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 seis meses a dos años de prisión y de cien a trescientos días multa.

La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad.

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 **o también sin autorización acceda a dichos sistemas o equipos informáticos o mediante cualquier mecanismo que de manera próxima o remota les cause un daño**, 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 **o también sin autorización acceda a dichos equipos o medios o mediante cualquier mecanismo les cause un daño**, 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 cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

En los casos en que el daño provocado por el acceso o la modificación no autorizados o por cualquier mecanismo empleado obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.

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.

Las penas establecidas en los párrafos anteriores se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero, las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo primero del artículo 400 Bis de este ordenamiento.

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.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Las penas establecidas en los párrafos primero y segundo de este artículo se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero; las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento.

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, **salvo en los casos que se disponga otra pena.**

En materia de amenazas, la comisión concuerda en adicionar un tercer párrafo al artículo 282, con el fin de sancionar a quien, haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos le amenace con divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis, lo cual se observa en el siguiente cuadro:

Texto Vigente

Título Decimoctavo

Delitos contra la paz y seguridad de las personas

Capítulo I

Amenazas

Artículo 282. Se aplicará sanción de tres días a un año de prisión o de 180 a 360 días multa:

I. Al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, y

II. Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer.

Si el ofendido fuere alguno de los parientes o personas a que se refieren los artículos 343 Bis y 343 Ter, en este último caso siempre y cuando habiten en el mismo domicilio, se aumentará la pena que corresponda hasta en una tercera parte en su mínimo y en su máximo.

Si el ofendido por la amenaza fuere víctima u ofendido o testigo en un procedimiento penal, la pena será de cuatro a ocho años de prisión y de cien a trescientos días multa.

Los delitos previstos en este artículo se perseguirán por querrela, con excepción del establecido en el párrafo anterior que se perseguirá de oficio.

Propuesta de reforma

Título Decimoctavo

Delitos contra la paz y seguridad de las personas

Capítulo I

Amenazas

Artículo 282. Se aplicará sanción de tres días a un año de prisión o de 180 a 360 días multa:

I. Al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo;

II. Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer;

III. Al que amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o le amenace con divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis 1.

Si el ofendido fuere alguno de los parientes o personas a que se refieren los artículos 343 Bis y 343 Ter, en este último caso siempre y cuando habiten en el mismo domicilio, se aumentará la pena que corresponda hasta en una tercera parte en su mínimo y en su máximo.

Si el ofendido por la amenaza fuere víctima u ofendido o testigo en un procedimiento penal, la pena será de cuatro a ocho años de prisión y de cien a trescientos días multa.

Los delitos previstos en este artículo se perseguirán por querrela, con excepción del establecido en el párrafo anterior que se perseguirá de oficio.

En materia de fraude, esta comisión dictaminadora concuerda con los diputados proponentes en el sentido de combatir y erradicar conductas que atentan y ponen en peligro la seguridad de las transacciones, operaciones y el intercambio o entrega de datos e información vía Internet.

Para tal fin, se adiciona el artículo 389 Ter a fin de sancionar como un delito equiparable al fraude, la conducta cometida por quien valiéndose del error en que se encuentra la víctima provoque que revele o ponga a su disposición información o datos de carácter personal, patrimonial o financiero a los que no tenga derecho a acceder, utilizando para tales fines sitios o direcciones de correo u otros medios electrónicos creados por él mismo o por un tercero y que por sus características, emblemas, marcas o cualquier distintivo gráfico o de leyendas de

texto simulen o reproduzcan de manera apócrifa e ilegítima a las que pertenecen a los prestadores de servicios financieros o de cualquier otro tipo de carácter público o privado que brinde atención o establezca contacto con sus clientes, usuarios o público en general por dichos medios.

Asimismo, en el segundo párrafo del propio artículo 389 Ter que se adiciona, se propone que en los casos en que se use la información obtenida por los mecanismos que describe el párrafo primero de dicho artículo para hacerse de alguna cosa, beneficio o lucro indebido, además de las penas que le correspondan por la obtención de datos o información por medio del engaño que sufre la víctima, se imponga al sujeto activo la pena que dependiendo del valor o monto obtenido de esa forma ilícita corresponda, de conformidad con los fracciones I, II y III del artículo 386 del Código Penal Federal.

Igualmente, se adiciona un segundo párrafo al artículo 390 con el fin de incluir el uso de los medios y sistemas informáticos en el delito de extorsión.

Propuesta de añadido

Capítulo III

Fraude

Artículo 389 Ter. Se equipara al delito de fraude y se sancionará con pena de seis meses a tres años de prisión y de cien a cuatrocientos días multa, sin perjuicio de las penas que correspondan por la comisión de otros delitos, al que valiéndose del error en que se encuentra la víctima provoque que revele o ponga a su disposición información o datos de carácter personal, patrimonial o financiero a los que no tenga derecho a acceder, utilizando para tales fines sitios o direcciones de correo u otros medios electrónicos creados por él mismo o por un tercero y que por sus características, emblemas, marcas o cualquier distintivo gráfico o de leyendas de texto simulen o reproduzcan de manera apócrifa e ilegítima a las que pertenecen a los prestadores de servicios financieros o de cualquier otro tipo de carácter público o privado que brinde atención o establezca contacto con sus clientes, usuarios o público en general por dichos medios.

Además de las penas que correspondan conforme al presente artículo, se impondrán las penas que establece el artículo 386 de este Código, al que mediante el uso o empleo de la información o datos obtenidos por los medios descritos en el párrafo anterior, obtenga algún beneficio, cosa o lucro indebido, según sea el valor o monto de lo obtenido.

Texto Vigente

Capítulo III Bis

Extorsión

Artículo 390. Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.

Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas. En este caso, se impondrá además al servidor o ex servidor público y al miembro o ex miembro de alguna corporación policial, la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos.

Propuesta

Capítulo III Bis

Extorsión

Artículo 390. Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.

Las penas que refiere el párrafo anterior se aumentaran hasta en una mitad al que para lograr los fines que refiere el párrafo anterior haga empleo o uso de comunicados o mensajes que envíe a la víctima a través de medios o sistemas informáticos o se valga de la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis 1.

Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas. En este caso, se impondrá además al servidor o ex-servidor público y al miembro o ex-miembro de alguna corporación policial, la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos.

B) Iniciativa del diputado Canek Vázquez Góngora

Se propone la reforma el artículo 211 Bis 5 del Código Penal Federal, a efecto de incorporar al tipo penal la conducta de divulgar.

Texto vigente

Código penal federal

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.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Propuesta

Código Penal Federal

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 copie o divulgue información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

Las penas previstas en este artículo se incrementan **al doble** cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Establecidos los antecedentes y los contenidos de las iniciativas, los miembros de la Comisión de Justicia exponemos las siguientes:

Consideraciones

Antes de entrar al análisis de las iniciativas en comento, es necesario establecer que en virtud de que las mismas se refieren al mismo tema, se dictaminan conjuntamente, ya que coinciden en el tema de delitos informáticos.

Primera. La Constitución Política de los Estados Unidos Mexicanos en su artículo 73 fracción XXI, señala que corresponde al Congreso de la Unión establecer los delitos y las faltas contra la Federación y fijar los castigos que por ellos deban imponerse.

En este contexto, la comisión dictaminadora estima que las iniciativas en comento es susceptible de ser analizadas, al ser el Congreso de la Unión un órgano competente para legislar en materias relacionadas con la aplicación de leyes federales y establecer delitos que lesionen a sujetos que realicen actividades reguladas por las mismas, como en el caso de los delitos informáticos en los que los bienes que son objeto de su tutela se encuentran regulados por leyes en materia de telecomunicaciones, vías generales de comunicación, o los que de manera específica se relacionan con la trata de personas, los ataques a las instituciones financieras, los que se cometen con recursos de procedencia ilícita o lavado de dinero o en general todas aquellos delitos que se cometen fuera del territorio nacional por un mexicano contra mexicanos o contra extranjeros, o por un extranjero contra mexicanos, quienes, de conformidad con el artículo 4o. del Código Penal Federal, deberán ser penados en la República, con arreglo a las leyes federales.

Segunda. De la misma manera, la Comisión considera pertinentes las propuesta de reforma de los diputados promoventes y determina que son totalmente atendibles los cambios planteados dada la creciente incidencia de delitos informáticos en la vida de los mexicanos.

Asimismo, esta propuesta responde a la necesidad y apremiante urgencia de actualizar el Código Penal Federal a fin de adecuar las disposiciones del orden jurídico a las exigencias que impone el avance tecnológico y la condición social actual de nuestro país, en materia de dichos ilícitos.

Los avances tecnológicos y la irrupción de las tecnologías de la información y comunicaciones en la vida cotidiana de los mexicanos obligan a actualizar el catálogo de delitos en función de las modalidades y tipos aquí descritos.

La Comisión de Justicia estima, en el mismo sentido que los Legisladores, la legislación penal nacional vigente, se ha vuelto insuficiente y carente de normas claras y precisas para combatir esta clase de conductas delictivas en medios informáticos.

En este sentido, es posible apreciar que las estadísticas nos reflejan la importancia que el fenómeno de los delitos informáticos está teniendo en nuestro país.

Al respecto, el Informe de la Secretaría de Seguridad Pública emitido con motivo del Quinto Informe de Gobierno refiere que la policía cibernética manifiesta que de septiembre de 2010 a julio de 2011 se atendieron 5 mil 582 denuncias ciudadanas en materia de delitos cibernéticos.

De acuerdo al reporte, las conductas que presentaron un mayor índice de denuncias fueron el fraude al comercio electrónico y el *phishing*, entendido como el sitio falso creado con apariencia de uno real, con el fin de recopilar información personal o de tarjeta de crédito de un usuario, para fines delictivos, de acuerdo a la propia SSP.

En materia de delitos contra menores de edad, la División Científica de la Policía Federal formalizó 15 denuncias relativas a dichos delitos, logrando una sentencia en materia de pornografía infantil. ¹

Asimismo, del análisis a la iniciativa es posible advertir del impacto de los delitos informáticos en la vida de las personas e instituciones, según quedo señalado con antelación, lo cual justifica plenamente las reformas propuestas.

Dadas estas cifras, se observa que una de las reformas muy pertinentes se refieren precisamente a las relacionadas con el fraude y fraude equiparado, así como con las conductas relacionadas.

Tercera. Los suscritos coinciden en que es necesario adecuar el marco vigente en materia penal, con el propósito de adecuarlo a los instrumentos y convenios internacionales aquí descritos que presentan recomendaciones y propuestas de leyes, con el fin de armonizar estos delitos que pueden ser realizados en cualquier parte del mundo, dada la naturaleza propia del Internet pero que sin embargo, afectan a los habitantes de nuestro país.

Cuarta. La Comisión de Justicia, considera de suma importancia llevar a cabo la reforma propuesta. En este sentido, se observa al revisar el catálogo de los delitos tipificados como tales en la propuesta de los diputados Guerra y Pérez-Alonso, dicha propuesta incluye la mayoría de las conductas delictivas señaladas en los convenios internacionales, como en el caso del Convenio llamado de Budapest que refiere delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; los delitos informáticos; los delitos relacionados con el contenido; los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines y otros como el llamado *phishing* .

Respecto al primer rubro, los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, el dictamen que aquí se propone incluye el acceso y la intervención, ilícitos, la manipulación de datos y el ataque contra la integridad del sistema.

En materia de delitos informáticos, se incluye el fraude y fraude informático, la falsificación, el robo de identidad y la utilización indebida de dispositivos.

Al revisar los delitos relacionados con el contenido, el dictamen propuesto por la comisión, en concordancia con el espíritu de la iniciativa, incluye la tipificación de delitos relacionados con la pornografía infantil, la trata de personas, el turismo sexual y corrupción de menores, las amenazas y la extorsión a través de medios electrónicos.

Respecto a los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, se incluyen disposiciones en la materia.

Destaca igualmente que los promoventes contemplan delitos complementarios como el del llamado *phishing* y el encubrimiento y realización de operaciones con recursos de procedencia ilícita.

Quinta. Reconociendo la relevancia que ha adquirido el uso de las tecnologías y el Internet en el caso de la pornografía infantil, corrupción de menores y turismo sexual, y la trata de personas menores de dieciocho años o de personas que no tienen capacidad de comprender el significado del hecho o que no tienen capacidad para resistirlo, la Comisión dictaminadora concuerda con los proponentes en la adición del inciso k) al artículo 205.

Con el fin de clarificar y precisar la forma en que el uso de los medios informáticos pueden ser usados para cometer los delitos previstos en los artículos 200, 201, 202, 203 y 204, relativas a los delitos de pornografía infantil, corrupción de menores y a la trata de los mismos, esta Comisión considera modificar la propuesta planteada determinando claramente que será sancionado con el doble de las sanciones a la persona que se valga del uso o empleo de medios informáticos para cometer cualquiera de estos delitos.

Lo anterior con el fin de evitar que adultos continúen contactando a menores y a quienes no tienen capacidad de comprender el significado del hecho o que no tienen capacidad para resistirlo, en la red y por medio de engaños,

lastimen su dignidad e integridad y usen estos medios para cometer alguno de los delitos señalados con anterioridad.

Dicha propuesta promueve que el Internet deje de ser usado como un medio para agredir y lastimar a menores e incapaces y sea un medio seguro para ellos, castigando con el doble de penas a quien emplee estos medios informáticos para fines y conductas delictivas.

En forma adicional, la tutela que deriva del inciso K) propicia que en aplicación de las disposiciones contenidas en el artículo 205, el juez que conozca de la causa que derive de la aplicación de dicho precepto, deberá en todos los casos acordar las medidas pertinentes para que se le prohíba permanentemente al ofensor tener cualquier tipo de contacto o relación con la víctima incluyendo desde luego el contacto vía internet.

Sexta. Esta instancia dictaminadora concurre con los proponentes en que se debe tipificar como delito la revelación de la información contenida en equipos informáticos obtenida a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos o través de la suplantación de identidad, en los términos de la adición que proponen del párrafo segundo al artículo 211 Bis.

En el mismo sentido se considera la viabilidad de que se penalicen conductas relacionadas con el acceso y la intervención ilícitas, el ataque contra la integridad del sistema y la manipulación de datos, el robo de identidad y la utilización indebida de dispositivos, cuando tales conductas atenten en contra de sistemas del Estado, del sector financiero o de cualquier otro sistema en general por lo que resultan atendibles las propuestas de reformas y adiciones que se plantean en el Capítulo II del Título Noveno del Código Penal, en materia de acceso ilícito a sistemas y equipos de informática.

Séptima. Esta comisión considera oportuno incorporar la propuesta del diputado Canek Vázquez Góngora, a efecto de incorporar como conducta tipificada en el artículo 205 Bis 5 la “divulgación”, precisando que quien esté autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie o divulgue la información que contengan los archivos será merecedor de una sanción penal.

Los integrantes de esta comisión consideramos muy oportuna dicha propuesta, toda vez que como se ha establecido en la introducción de la misma, se ha incrementado el intercambio de información bancaria entre los empleados de las instituciones del sistema bancario.

Lo anterior, previo análisis realizado del artículo 211 Bis 5, donde se observa que si hace falta la palabra “divulgue”, toda vez que no solo se concreta la acción con el copiar la información a que se tiene acceso en las instituciones bancarias, sino también con el intercambio de ésta. Como lo establece el diccionario de la Real Academia Española:

“**Divulgar.** (Del latín divulgare).

1. tr. Publicar, extender, poner al alcance del público algo. U. t. c. prnl.”

De lo anterior consideramos necesario que se agregue dicha conducta al tipo, para darle mayores herramientas al Ministerio Público de poder consignar.

Asimismo, propone incrementar la pena al doble, en los casos en que la persona o personas que incurran en el supuesto anterior sean empleados de una institución de sistema financiero. Toda vez que la pena establecida en el texto actual es de “tres meses a dos años”, siendo esta baja para las dimensiones a las que ha llegado a crecer este tráfico de información entre los empleados y delincuentes, así como el daño patrimonial, moral y físico que causan a las víctimas, consideramos correcto el incrementarla de la pena al doble.

Octava. Los integrantes de esta comisión destacan las propuestas de los promoventes que para sancionar las conductas que atentan en contra de los sistemas informáticos del sector financieros, plantean adiciones a los

artículos 211 Bis 4 y 211 Bis 5, relativas al uso de los medios y sistemas informáticos con el fin de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento. Ello en correspondencia a las reformas recientemente planteadas en materia de Lavado de dinero y las recomendaciones internacionales del uso de medios electrónicos en la comisión de este delito, por lo que igualmente se consideran atendibles dichas adiciones.

Novena. En el rubro de los delitos que atentan contra de las personas en su patrimonio, esta comisión coincide con los legisladores en que es necesario combatir y erradicar conductas que atentan y ponen el peligro la seguridad de las transacciones, operaciones y el intercambio o entrega de datos e información vía internet, por lo que la propuesta de adicionar el artículo 389 Ter a fin de sancionar como un delito equiparable al fraude, la conducta cometida por quien valiéndose del error en que se encuentra la víctima provoque que revele o ponga a su disposición información o datos de carácter personal, patrimonial o financiero a los que no tenga derecho a acceder, utilizando para tales fines sitios o direcciones de correo u otros medios electrónicos creados por él mismo o por un tercero y que por sus características, emblemas, marcas o cualquier distintivo gráfico o de leyendas de texto simulen o reproduzcan de manera apócrifa e ilegítima a las que pertenecen a los prestadores de servicios financieros o de cualquier otro tipo de carácter público o privado que brinde atención o establezca contacto con sus clientes, usuarios o público en general por dichos medios.

En este mismo tenor se considera viable aprobar el contenido del segundo párrafo del propio artículo 389 Ter que se adiciona, en el que se propone que en los casos en que se use la información obtenida por los mecanismos que describe el párrafo primero de dicho artículo para hacerse de alguna cosa, beneficio o lucro indebido, además de las penas que le correspondan por la obtención de datos o información por medio del engaño que sufre la víctima, se imponga al sujeto activo la pena que dependiendo del valor o monto obtenido de esa forma ilícita corresponda, de conformidad con los fracciones I, II y III del artículo 386 del Código Penal Federal, con lo cual se considera que se complementa el esquema de tutela al patrimonio de las personas que luego de sufrir el engaño entregan información personal de tipo bancario, financiero o de cualquier otro tipo que reporte la posibilidad de que a través de la misma el sujeto activo pueda acceder a la obtención de un beneficio patrimonial que no le pertenece de donde deriva la ilicitud de dicha obtención.

Asimismo, en el rubro de delitos patrimoniales, la extorsión, conducta ilícita que comete el que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se ha diversificado en su forma comisiva, a través del empleo de medios informáticos como son correos electrónicos o mensajes instantáneos a través de internet, por lo que son cada vez más altos los índices de criminalidad en los que aparece el empleo de dichos medios, por lo que al no existir un tipo que considere estas circunstancias las víctimas queden sin remedio sin posibilidad de recibir la asistencia de las instancias de procuración e impartición de justicia, ante el vacío legal que queda en esos casos.

Por ello, la comisión que dictamina considera procedente la adición del artículo 389 Ter al Código Penal Federal.

Décima. No menos atendible resulta para esta Comisión de Justicia resulta la propuesta de adición de un tercer párrafo al artículo 282, para que se sancionen las a quien haga haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o le amenace con divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis, ante el hecho de que cada vez es más frecuente el empleo de de los medios informáticos para la realización de estas conductas que deben ser catalogadas como delictivas, que atentan con la paz y la seguridad de las personas.

Undécima. Por lo que hace a la penalidad, el Código Penal Federal describe a la prisión como “la privación de la libertad corporal”; además, indica que su duración será de tres días a sesenta años, y sólo podrá imponerse una pena adicional al límite máximo cuando se cometa un nuevo delito en reclusión.

En el mismo sentido el propio ordenamiento legal dispone que al responsable de un homicidio calificado se le sanciona con una pena que puede ir de treinta a sesenta años de prisión; en consecuencia, la vida es el bien jurídico

de mayor valía que tutela el derecho penal en nuestro país, y ese puede ser un parámetro para graduar la gravedad de los ilícitos en nuestro sistema jurídico que se propone para las conductas que se pretenden tipificar, por lo que esta Comisión considera que las penas propuestas en la iniciativa que se dictamina, cumplen con los principios de racionalidad y retributividad de la pena, ya que oscilan entre los tres meses y los doce años de prisión, salvo en los casos en que por una circunstancia particular resulte la agravación de la pena, casos en lo que aun así se observa que persiste la proporcionalidad respecto a la sanción que se impone para conductas de la misma naturaleza o gravedad.

Por las consideraciones expuestas y para los efectos de la fracción a) del artículo 72 de la Constitución Política de los Estados Unidos Mexicanos, la Comisión de Justicia somete a la consideración del pleno de esta honorable asamblea, el siguiente

Decreto por el que se reforman y adicionan diversas disposiciones al Código Penal Federal

Único. Se **reforman** los artículos 211 Bis 2, párrafo segundo, y el 211 Bis 5 en sus párrafos segundo y tercero; se **adicionan** un inciso k) al artículo 205 Bis; un párrafo segundo al artículo 211 Bis; se adicionan un segundo, un tercero y un último párrafo al artículo 211 Bis 1, recorriendo el actual párrafo segundo para quedar como cuarto; un párrafo cuarto al artículo 211 Bis 2; un párrafo tercero al artículo 211 Bis 4; un párrafo tercero al artículo 211 Bis 5; un párrafo cuarto al artículo 282, recorriendo el actual párrafo cuarto para quedar como quinto; el artículo 389 Ter, y un segundo párrafo al artículo 390, recorriendo el actual párrafo segundo para quedar como tercero, todos del Código Penal Federal, para quedar como sigue:

Artículo 205 Bis. ...

a) a j) ...

k) Quien se valga del uso o empleo de medios informáticos para cometer el delito.

...

...

...

Artículo 211 Bis. ...

Se impondrán las mismas penas que refiere el párrafo anterior a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad.

Artículo 211 Bis 1. ...

Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización y con el ánimo de causar un daño, acceda y modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad.

En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.

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 **seis meses a dos años** de prisión y **de cien a trescientos días multa**.

La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad.

Artículo 211 Bis 2. ...

Al que sin autorización **y con el ánimo de causar un daño**, 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.

...

En los casos en que el daño provocado por el acceso o la modificación no autorizados, obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.

Artículo 211 Bis 4. ...

...

Las penas establecidas en los párrafos anteriores se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero, las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo primero del artículo 400 Bis de este ordenamiento.

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 copie o **divulgue** información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

Las penas previstas en este artículo se incrementan **al doble** cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Las penas establecidas en los párrafos primero y segundo de este artículo se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero; las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento.

Artículo 282. ...

I. y II. ...

...

...

Si la amenaza se realiza **haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o si la amenaza se refiere a divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis 1, la pena se agravará hasta en una mitad.**

...

Artículo 389 Ter. Se equipara al delito de fraude y se sancionará con pena de seis meses a tres años de prisión y de cien a cuatrocientos días multa, sin perjuicio de las penas que correspondan por la comisión de otros delitos, al que valiéndose del error en que se encuentra la víctima provoque que revele o ponga a su disposición información o datos de carácter personal, patrimonial o financiero a los que no tenga derecho a acceder, utilizando para tales fines sitios o direcciones de correo u otros medios electrónicos creados por él mismo o por un tercero y que por sus características, emblemas, marcas o cualquier distintivo gráfico o de leyendas de texto simulen o reproduzcan de manera apócrifa e ilegítima a las que pertenecen a los prestadores de servicios financieros o de cualquier otro tipo de carácter público o privado que brinde atención o establezca contacto con sus clientes, usuarios o público en general por dichos medios.

Además de las penas que correspondan conforme al presente artículo, se impondrán las penas que establece el artículo 386 de este Código, al que mediante el uso o empleo de la información o datos obtenidos por los medios descritos en el párrafo anterior, obtenga algún beneficio, cosa o lucro indebido, según sea el valor o monto de lo obtenido.

Artículo 390. ...

Las penas que refiere el párrafo anterior se aumentaran hasta en una mitad al que para lograr los fines que refiere el párrafo anterior haga empleo o uso de comunicados o mensajes que envíe a la víctima a través de medios o sistemas informáticos o se valga de la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos en los términos que refiere el artículo 211 Bis 1.

...

Transitorios

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

Segundo. Se derogan todas las disposiciones que se opongan al presente decreto.

Nota

Secretaría de Seguridad Pública, Quinto Informe de Gobierno, página 29.

Palacio Legislativo de San Lázaro, a 15 de febrero de 2012.

La Comisión de Justicia

Diputados: Víctor Humberto Benítez Treviño (rúbrica), presidente; Sergio Lobato García, Miguel Ernesto Pompa Corella, Óscar Martín Arce Paniagua (rúbrica), Camilo Ramírez Puente, Ezequiel Rétiz Gutiérrez (rúbrica), Olga Luz Espinosa Morales (rúbrica), Eduardo Ledesma Romo, secretarios; María de Jesús Aguirre Maldonado (rúbrica), Luis Carlos Campos Villegas (rúbrica), Nancy González Ulloa (rúbrica), Leonardo Arturo Guillén Medina, Mercedes del Carmen Guillén Vicente (rúbrica), Cuauhtémoc Gutiérrez de la Torre, Gregorio Hurtado Leija, Israel Madrigal Ceja, Sonia Mendoza Díaz, Dolores de los Ángeles Nazares Jerónimo (rúbrica), María Antonieta Pérez Reyes (rúbrica), Rodrigo Pérez-Alonso González (rúbrica), Norma Leticia Salazar Vázquez

(rúbrica), Cuauhtémoc Salgado Romero, Miguel Ángel Terrón Mendoza, Enoé Margarita Uranga Muñoz, Josué Cirino Valdés Huevo (rúbrica), Alma Carolina Viggiano Austria, Pedro Vázquez González (rúbrica), J. Eduardo Yáñez Montaña (rúbrica), Arturo Zamora Jiménez.