UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

"PROYECTO DE REFORMAS AL CÓDIGO PENAL FEDERAL MEXICANO, EN LOS DELITOS COMETIDOS POR REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA"

TESIS QUE PARA OPTAR POR EL TÍTULO DE LICENCIADO EN DERECHO, PRESENTA

ROLANDO GÜITRÓN ROIG

DIRECTOR DE LA TESIS: DR. JULIÁN GÜITRÓN FUENTEVILLA

CIUDAD UNIVERSITARIA, ABRIL DEL 2014

M É X I C O

D E D I C A T O R I A S

Para mis papás, que admiro y quiero y de los que siempre he recibido su infinito apoyo, paciencia, enseñanzas, consejos y tanto amor.

Para Ivette, por todo su amor, comprensión y por ser mi impulso.

Para Julián, Meghan, Julián Alejandro y Vincent, que siempre me apoyan e inspiran.

Para Leoba, por su amor y ejemplo, desde que nací.

Para mi familia, amigos y maestros, por todo lo que me han dado.

Para el Maestro Carlos Barragán y Salvatierra, mi eterno agradecimiento.

Para el Doctor David Vega Vera, por creer en mí.

Para Mariana Zaragoza Martínez, consejera y amiga.

Para mi Alma Mater.

P R Ó L O G O

Someter a la consideración de este honorable jurado, mi tesis profesional, denominada “Proyecto de Reformas al Código Penal Federal Mexicano en los Delitos Cometidos por Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática”, me estimula y alienta a seguir estudiando y superarme por la vía del conocimiento, para que una vez satisfechos los requisitos reglamentarios universitarios, pueda acudir a la cita histórica que para mi es trascendental, para llevar a efecto la defensa de mi tesis y las hipótesis y reformas propuestas en la misma, al realizar el examen profesional correspondiente y en su caso, lograr el título de licenciado en Derecho, expedido por la Facultad de Derecho de la Universidad Nacional Autónoma de México, que como es reconocida por todos los sectores relacionados con el Derecho, es la mejor de las instituciones públicas y privadas, que enseñan esta ciencia en Latinoamérica.

El privilegio que para mí representa, aspirar a graduarme de licenciado en Derecho en mi “Alma Mater”, que hoy, por primera vez en la historia, es dirigida por una mujer, jurista y académica, quien lo está haciendo de una manera tan sobresaliente, la doctora María Leoba Castañeda Rivas, primera en ocupar tan digno cargo en los últimos cuatrocientos sesenta años.

Mi vocación natural en el aprendizaje y práctica de los asuntos vinculados con la información digital y en general el mundo de la cibernética, se ha amalgamado con la otra, la que me ha dado grandes satisfacciones y frutos importantes en mi vida, al haber dedicado parte de ella al Derecho Penal; tanto en el aprendizaje en la propia Universidad, como en el ejercicio profesional en Juzgados Penales del fuero común y en Tribunales Colegiados de Circuito en materia penal y en prestigiados bufetes jurídicos de la iniciativa privada.

I N T R O D U C C I Ó N

Esta investigación se compone de cuatro capítulos y las conclusiones de los mismos, que son el sustento de mi posición ideológica original, para proponer que el Código Penal Federal mexicano, reforme los delitos comprendidos del artículo 211 Bis-1 al Bis-7 y los párrafos cuarto y último del artículo 400 Bis, todos de la legislación punitiva mencionada.

He aplicado varios métodos en la realización de esta tesis, destacando el histórico, el analítico, el comparativo y el jurídico, para darle un fundamento científico a mi proposición, que a pesar de que la información digital, la aparición de las computadoras y lo que hoy se conoce como mundo globalizado, es tan reciente, -en realidad no tiene más de setenta años de ser parte de la vida de quienes habitamos este planeta- ha rebasado a sus propios creadores y desgraciadamente el Derecho, los juristas, los especialistas en Derecho Penal y sobretodo los del Derecho Informático, se han quedado a la saga de las consecuencias de los descubrimientos y avances tecnológicos que surgen minuto a minuto, hora tras hora, día tras día y ante esa realidad, desde mi perspectiva y esto es esencial en mi tesis profesional, dentro de las reformas propuestas, el común denominador es que los sujetos activos de los delitos informáticos, dependiendo de los ilícitos cometidos, no deben en ningún supuesto, enfrentar los procesos penales correspondientes en libertad o con fianza, sino privados de ésta, porque en un momento dado, son una amenaza para la estabilidad, la paz y la estabilidad no sólo de México sino del mundo entero.

En el primer capítulo, hacemos un recorrido histórico del nacimiento y evolución de los delitos informáticos en Europa, Norteamérica y Suramérica, acudiendo a las fuentes bibliográficas más importantes de tratadistas, que analizan desde diferentes perspectivas, las consecuencias y los efectos que la comisión de estos delitos han provocado en países como Alemania, Austria, Francia, Gran Bretaña, Holanda, España e Italia. Igualmente, la situación actual de

estos delitos en México y en el vecino país del norte de los Estados Unidos de América. También como ejemplo de legislaciones diferentes, hemos analizado y comparado en Suramérica, tres países paradigmáticos en esta materia, Chile, Argentina y Venezuela.

Mi investigación se funda también en el análisis que hago de la Exposición de Motivos del Título Noveno del Libro Segundo del Código Penal Federal, específicamente lo referente a la revelación de secretos y el acceso ilícito a sistemas y equipos de informática. En esta parte de la tesis, está uno de los motivos de mi inspiración para proponer en el siguiente capítulo, la esencia de la tesis de mi tesis, que consiste en aplicar los métodos mencionados, haciendo los estudios correspondientes para plantear reformas que se adecúen con una prospectiva jurídica, al presente y al futuro, para que la nueva reglamentación de los delitos analizados, no nazcan a la saga o fuera de la realidad, porque mi intención y así ha quedado plasmada en este trabajo, es haber realizado el estudio de los artículos 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis 4, 211 Bis 5, 211 Bis 6, así como el 211 Bis-7 del Código Penal Federal.

La metodología que seguí es en primer lugar, hacer una referencia clara al proyecto de estas reformas con su Exposición de Motivos, para que los distinguidos miembros de este H. Jurado, tengan todos los elementos necesarios para juzgar este trabajo.

He considerado que la teoría general del delito, con sus elementos tradicionales de conducta, –acción u omisión- tipicidad, antijuridicidad y culpabilidad, es indispensable, al llevarla a los diversos supuestos jurídicos de los delitos informáticos, aplicarla para definir, con género próximo y diferencia específica lo que sostengo respecto a cada uno de los artículos objeto de esta investigación.

La sistemática propuesta por mí, es analizar verbigracia, el artículo 211 Bis-1, emitir mi comentario al respecto, la crítica que le hago al mismo y la propuesta que sometemos a la consideración de este sínodo, respecto al nuevo texto del precepto citado. Así lo hacemos con los demás artículos, para darle un contenido más jurídico y científico a mi proyecto de reformas al Código Penal Federal.

Si bien es cierto que es elemental y que cualquier estudioso del Derecho Penal o estudiante, como es mi caso, debe considerar en el análisis de cualquier delito, propuesta de reforma o nueva creación, determinar con toda claridad, cual es o cuales son los bienes jurídicos protegidos en esos hechos ilícitos, comúnmente conocidos como delitos. En el capítulo cuarto y último de esta tesis, he hecho algunas reflexiones, porque mi propuesta de reformar varios artículos, que tienen supuestos distintos en cuanto a la sustracción, destrucción, modificación, utilización o copia de la información digital, para cometer otros delitos, tienen desde mi personal punto de vista, que el bien jurídico protegido en ellos, es la información. Rechazo que se tutele el patrimonio, porque sería desconocer la esencia del robo; por ello, he reiterado en este cuarto capítulo, que el bien jurídico protegido en el delito informático, es la información. Para mí este es un concepto esencial para que no haya desviaciones ni dudas, para incluir en ese supuesto jurídico, los bienes jurídicos protegidos de delitos colaterales, vinculados a la información digital, pero que no son esencia de ésta. Estoy de acuerdo en que la sustracción de la información puede afectar el patrimonio, pero el bien jurídico del delito informático debe ser la información.

CAPÍTULO PRIMERO
ANTECEDENTES HISTÓRICOS DE LOS DELITOS INFORMÁTICOS
I. EUROPA
A) ALEMANIA

En este país, como en otros europeos, los delitos informáticos han sido tan graves que fue en 1986, el 1 de agosto, cuando adoptaron la Segunda Ley contra la Criminalidad Económica, incluyendo en ella el espionaje de datos, la estafa informática, la falsificación de datos probatorios, así como otras modificaciones de falsedades documentales, verbigracia, el engaño en el tráfico jurídico, usando datos con falsedad ideológica y también documentos falsos.

Se consideró ilícito alterar o cancelar datos, inutilizar o alterarlos, incluso se llega al punto de que el delito en la tentativa es castigable. También se ha incluido el sabotaje informático a nivel mundial, destruir datos importantes, alterarlos o eliminarlos. Otro enfoque que no es el de nuestra tesis, se refiere al uso abusivo de cheques y tarjetas de crédito.[1]

Por lo que se vincula a la estafa informática, yendo propiamente al Derecho Penal, se formuló en Alemania un nuevo tipo penal, cuyo primer problema fue encontrar una analogía donde se pudiera dar la acción engañosa, la producción del error y que trajera como consecuencia un daño patrimonial. No se encontró la forma de controlar esas nuevas expresiones, por lo que no se obtuvo el resultado esperado.

Se han emitido diversas opiniones de expertos en la materia, llevado específicamente a Alemania, donde en realidad hay un número importante de nuevos tipos penales, para sancionar, aun cuando han tenido que renunciar a la tipificación de la mera penetración, que no se autoriza en sistemas ajenos de computación, incluyendo el castigo para quienes sin esa autorización, atente contra equipos de procesos de datos.

[1] DÍAZ GARCÍA, Alexander. Derecho Informático. Editorial Leyer. 1ª reimpresión. Bogotá, Colombia, 2012. p. 167 in fine y 168.

En este país, ha habido problemas para crear estos nuevos delitos, tratando de superar las verdaderas dificultades, para que la aplicación del nuevo Derecho, se ajustara al Penal tradicional, por lo que se refiere a las conductas u omisiones dañosas, donde se ha introducido un elemento que perjudica el proceso electrónico y destruye los datos o se echan a perder otros bienes jurídicos, que debían estar protegidos desde el punto de vista penal y que resultaban lesionados. [2]

En resumen, Alemania, al promulgar la ley contra la criminalidad económica, incluyó los delitos de espionaje de datos, la estafa informática, la alteración de datos y el sabotaje informático.

[2]VILLA ESCOBOSA, Jaime, et al. Derecho y MediosElectrónicos. Editorial Porrúa, México, 2012, p. 253.

B) AUSTRIA

En 1987, en su Código Penal reformado, cuando en el artículo 148, determinaron sancionar a quienes con dolo, a través de artificios, maquinaciones y engaños, causaran un perjuicio patrimonial a un tercero, no incluyeron en el resultado, la elaboración de datos automáticos por medio de un Programa o por la introducción, cancelación o alteración de aquéllos, como ocurre en México o por actuar sobre el curso de procesamiento de datos.

Igualmente, hay sanciones graves para los sujetos activos de este delito y que utilicen su profesión como especialistas en sistemas digitales. También en Austria, la ley mencionada, en cuanto a la reforma que se le hizo al Código Penal, agregaron los delitos de destrucción de datos; en este caso, el artículo 126, se refirió además, a los datos personales, a los que no lo fueran, y a los programas.

En cuanto a la estafa informática, que se modificó en el artículo 148 del ordenamiento punitivo en comento, se sancionó a quienes por medio de artificios, maquinaciones o dolo, causaran un perjuicio patrimonial a un tercero; en este caso, a través de esta influencia, elaboración de datos o los programas, incluyendo el hecho de que se cancelaran o alteraran esos datos, al actuar sobre el procesamiento de los mismos.[3]

[3]Loc. Cit.

C) FRANCIA

Es evidente que en Europa, en los años señalados-1986-1987- esto tuvo una gran influencia, incluida Francia y así su Ley No. 88-19, el 5 de enero, abordó el tema del fraude informático. En éste, se adicionaron de manera general, los delitos de sabotaje informático, la destrucción de datos, y la falsificación de documentos informatizados.

En el primer caso, en el artículo 462-2, se sancionó a quienes accedieran al sistema, y a los que se mantuvieran en él, aumentando la pena, si ese acceso, era resultado de haber suprimido o modificado, los datos contenidos en el sistema o fuera resultado de una alteración del funcionamiento del mismo. Esta información es importante, porque en México, en el Proyecto que proponemos en nuestra tesis, se incluyen otros supuestos que no se contemplan, ya que en nuestro Código Penal, regula los delitos cometidos por relaciones secretas y el acceso ilícito a sistemas y equipos de informática.

Más adelante, en el precepto 162, en la modificación -3, el Derecho Penal francés, adicionó el delito de destrucción de datos. En este caso, se pena a quien lo haga con la intencionalidad y menospreciando los derechos de otras personas, realizando estas conductas, introduciendo datos en un sistema de tratamiento automático que los contenga, los suprima o modifique, lo que traerá como consecuencia, que se alteren los modos de tratamiento o de que esos datos puedan ser transmitidos.

También se determina en el artículo 462-5 del Código de la Ley de 1988, que venimos comentando, la falsificación de documentos informatizados; en este caso, se sanciona a la persona que de cualquier manera, no importa cómo lo realice, falsifique esos documentos y tenga la intención de causar un perjuicio a otra persona. Así, con el uso de estos documentos informatizados falsos, se llega a la reforma del numeral 462-6 en el que se establece una grave sanción, para

quien conscientemente esté haciendo uso de esos documentos falsos, trayendo a colación lo que mencionamos del artículo 462-5.[4]

En resumen en el Derecho francés, las reformas de enero de 1988, impusieron las penas de prisión, que iban de dos meses a dos años, y multas que en aquellos tiempos, se calculaban en francos, que se tendrán que modificar hoy en día, para hacerlo en euros.

Esto es importante, porque se puede utilizar en el Derecho Penal mexicano, al considerar, que deben haber penas graves, cuando además de suprimir o modificar esos datos en el sistema, las personas se mantengan en él, es decir, acceden y se mantengan en él, esto obliga a que haya una pena mayor, como lo estamos proponiendo en el capítulo tercero de este trabajo, donde hacemos un análisis de los diferentes supuestos de 1999, sus reformas y lo que proponemos en cuanto a los diversos artículos del 211 Bis-1 al Bis 7 del Código Penal Federal, así como la propuesta de reformas en las que en todas incide, nuestra tesis de incrementar las penas de prisión.

[4]VILLA ESCOBOSA, Jaime, et. al,Ob. Cit., p. 255.

D) GRAN BRETAÑA

Como consecuencia de este movimiento europeo 1987-1988, en 1991, atendiendo a un caso de “hacking”, (Por ser un término inventado en inglés, de acepción controversial y sin traducción literal al español, consideramos, que para tener un criterio unificado, admitamos los conceptos más comunes encontrados en la materia respectiva. Bajo estas circunstancias, las traducciones propuestas son: la violación o invasión informática; piratear un sistema.) se empezó a aplicar en este país, la ley de abusos informáticos, llamada “Computer MisuseAct” (Acta de hacer mal uso de la computadora) y ésta sancionaba inclusive la pura intención, o sea, tuviera o no éxito el delincuente para tratar de alterar datos informáticos, recibe una pena que puede ser hasta de cinco años de prisión o en su caso, multas.

Siguiendo la misma línea de las reformas, en esta ley se plantean casos de modificación de datos, donde las personas se meten sin autorización y como novedad, se incluyen los virus, es decir, quienes los introduzcan también serán sancionados en los términos que hemos apuntado. Por otro lado, estas penas, para quienes liberan los virus, van con sanciones de un mes a cinco años, dependiendo del daño que hubieran causado.[5]

[5] Loc. Cit.

E) HOLANDA

Los holandeses en la década de los noventa, específicamente el 1 de marzo de 1993, pusieron en vigor la ley denominada, “Delitos Informáticos”, donde se sanciona la utilización de servicios de telecomunicaciones, para evitar el pago total o parcial de ese servicio, igualmente lo que se llama el hacking y el phreacking.

Asimismo, hay sanciones para quien convence a otro, de entregar información, que en circunstancias normales no lo haría, es decir, lo que los holandeses llaman la ingeniería social, incluye la distribución de virus.

En este caso, se castiga de manera diferente, si éstos entraron a las computadoras por error o si fue deliberadamente para causar esos daños. Incluso, ordena la ley, que si fue por error, la pena será máximo de un mes de prisión pero si fue deliberado, puede haber penas hasta de cuatro años de prisión.[6]

[6]VILLA ESCOBOSA, Jaime. Ob. Cit. pp. 255 in fine y 256.

F) ESPAÑA

Es el país europeo, que le ha dado un tratamiento especial a los delitos informáticos. Han hecho una serie de reformas en el nuevo Código Penal de 1995, y en él han incluido delitos que no son materia de esta tesis y una vez que los hemos analizado, hemos llegado a la conclusión, de que algunos sí se vinculan con el tema que estamos desarrollando en esta tesis y así por ejemplo, consideran que es un delito, el acto que se realiza para apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal, siempre y cuando los ficheros estén registrados o haya soportes informáticos, electrónicos o telemáticos, que de alguna manera se vinculan con los delitos informáticos.[7]

También hay algunas referencias al fraude informático o daños informáticos, este Código los define, diciendo que se da, cuando hay una manipulación de esta información o se utilizan artificios semejantes que concurren con el ánimo de lucro y que además, traigan como consecuencia, transferir contra el consentimiento de la persona, que tiene el derecho de hacerlo, cualquier activo patrimonial que lo perjudique; la otra hipótesis, que a nuestro juicio se encuentra ahí, se da en el delito de daños, ya que en este caso, surgen varias hipótesis que contempla los supuestos de destruir, alterar, inutilizar o cualquier otra modalidad que como consecuencia, dañen esos datos, alteren los programas o borren los documentos electrónicos, contenidos en redes, en soportes y sistemas informáticos.

Consideramos que las penas son leves, esencia de nuestra tesis, donde hemos propuesto que estos castigos se incrementen, para que en un momento dado, puedan ser un elemento preventivo de la comisión de esos delitos. También en España, formaron parte del Convenio de Ciberdelincuencia del Consejo de Europa y se ratifica lo que hemos comentado, de donde consideramos, que hay penas de prisión, multas y se repite el supuesto de que quien usando cualquier medio destruya, altere, inutilice o de cualquier otro modo, dañe esos datos,

[7] Ob. Cit. pp. 253 in fine y 254.

programas o documentos electrónicos, ajenos, contenidos en redes, soportes o sistemas informáticos.

Terminamos con esta breve reseña de España, destacando que el 46.71% de la materia que venimos analizando, se vincula a delitos informáticos que incluyen la falsificación o fraude, al introducir, borrar o suprimir datos informáticos o interferir en sistemas de esta naturaleza.

G) ITALIA

Atendiendo a que el 18 de marzo del año 2008, Italia, en relación a los delitos informáticos, ratificó la Convención de Budapest, modificó su Código Penal para tipificar varios delitos, cuyo bien jurídico protegido es la informática. Entre otros, reguló el acceso abusivo a los sistemas informáticos; agravando este hecho ilícito, con la calificativa de abuso de la calidad de operadores de sistemas.

Determinó castigar, a quien introduzca virus informáticos a una red programática, cuya función sea bloquear un sistema, destruir sus datos o alterar el disco duro, sancionando con penas privativas de la libertad, hasta de dos años y multas elevadas.

En el fraude informático, se incluye el dolo, determinando que quien use artificios o engaños o induzca a otro al error, comete ese delito o si altera el funcionamiento de sistemas informáticos; en este caso, se castiga con tres años de prisión, más una multa considerable. Otros delitos informáticos, son la intercepción abusiva; la falsificación informática; el espionaje de esta naturaleza; la violencia sobre bienes digitales; abusar al detentar o difundir códigos o contraseñas de acceso y la violación de correspondencia electrónica. [8]

[8]VILLA ESCOBOSA, Jaime, et al, Ob. Cit. pp. 256 y 257.

II. NORTEAMÉRICA

A) ESTADOS UNIDOS DE AMÉRICA

La influencia de las leyes europeas, los convenios que allá se celebraron entre 1986 y 1987, van a tener efectos en Estados Unidos, donde en 1994, adoptan la llamada Acta Federal de Abuso Computacional, la cual vino a modificar el Acto de Fraude y Abusos Computacionales de 1986, que como decíamos, siguió los lineamientos europeos.[9]

Considerando la proliferación de todo lo relativo a esta materia, los legisladores norteamericanos, tuvieron como propósito, que no hubiera argumentos discutibles, en cuanto a que si la destrucción de los datos informáticos, se había hecho por un virus o un gusano, ellos le dicen un caballo de Troya.

En la nueva Acta, prohibieron que la transmisión de un programa, información, códigos o comandos, que causen daños a la computadora, al sistema informático, a las redes de información, datos o programas, fueran sancionados. Debe subrayarse que la ley en cuestión, es un adelanto, porque en realidad prevé estos actos de transmisión de virus.

Esta ley diferencia, acudiendo a principios de Derecho Penal, las conductas dolosas de las imprudenciales. Llevan estos supuestos, al tratamiento de los sujetos que para dañar o causar el mayor número de perjuicios posible, lanzan ataques con virus, que en realidad tienen la intención de destruir totalmente.

En este caso, esta ley, diferencia las dos clases de sujetos que pueden realizar esta conducta, a la vez, se refiere a los virus y dice que en realidad, quienes con intención causan un daño, deben recibir una pena privativa de la libertad, hasta por diez años en una prisión federal y una multa significativa. En

[9] Ob. Cit. p. 254.

cambio, quienes lo hayan hecho de manera imprudencial, es decir, lanzando ese virus, deben ser castigados con multa pequeña y un año de prisión.

En la Exposición de Motivos de esa Ley, se destaca, que en realidad no puede alegarse ignorancia o negligencia, porque la ley sólo ubica las dos hipótesis acotadas.

Incluso, se afirma en su Exposición, que esta Ley en realidad, pretende fincar responsabilidad más grave a los creadores de los virus informáticos, y en este caso, no dicen ellos cuál es el género próximo ni la diferencia específica de los mismos, sino que los dan de manera general, pensando precisamente en que en un futuro, los ataques tecnológicos de los sistemas informáticos, sean tan graves, que puedan burlar la ley, si no se tipifica ese virus así de manera general, queda incluido y lo que se diferencia, son los niveles del delito con esta nueva ley, que sanciona o define lo que es un acto delictivo.[10]

Es evidente que el legislador, igual que nuestra preocupación, es que se incrementen las sanciones a los sujetos activos de estos delitos, para proteger a las personas, a los negocios, incluso a los gobiernos y las agencias gubernamentales, para evitar que haya interferencias, daños y accesos no autorizados a las bases de datos y a los sistemas computarizados creados legalmente.

Igualmente, debe destacarse que en el Derecho Penal norteamericano, en el caso específico que venimos comentando, es importante expresar, que hay una gran proliferación de aparatos tecnológicos y digitales en relación con las computadoras, lo que evidentemente trae como consecuencia, que los delitos informáticos aumenten y vayan surgiendo nuevas formas no tipificadas que permitan a una persona acceder a esas computadoras, a los sistemas, a los datos, a la protección y destruirlos, llegando al punto, que no es la esencia de nuestra

[10] Loc. Cit.

tesis, de atacar la intimidad de las personas, lo que sí incide en nuestro estudio, es el bienestar de las instituciones financieras, de los negocios, de las agencias gubernamentales y otras vinculadas con el gobierno.

Como un ejemplo más específico, que encontramos en nuestra investigación, es que en 1992, dos años antes que esta Acta, en California se adoptó una ley vinculada a la privacidad, en cuanto a las personas, para castigar los delitos informáticos, con sanciones menores respecto a los relacionados con cuestiones de agencias gubernamentales.

Si bien es cierto, que se indujeron en esta reforma, sanciones de diez a cincuenta mil dólares para los responsables de estos daños, sobretodo personas jurídicas físicas, es decir, personas en lo individual.[11]

En resumen, es trascendente destacar, que esa ley californiana, regula lo que se llama los virus, the computer contaminant, (el contaminante de la computadora), definiéndolos aun cuando no se limiten a una clase determinada, pero sí que se les denomine virus o gusano, ya que su propósito es contaminar, destruir bases de datos o programas, modificar, destruir, copiar, transmitir o alterarlos, por lo que es loable que esto se haga en este sentido y por ello, nuestro interés en esta tesis y en las propuestas que hemos realizado.

[11] TÉLLEZ VALDÉS, Julio, Derecho Informático, Editado por el Instituto de Investigaciones Jurídicas de la UNAM, México, 1987, pp. 175 y ss.

B) MÉXICO

En este apartado, para hablar de los antecedentes históricos, sólo haremos referencia a que por primera vez, en el Diario Oficial de la Federación, bajo el Título Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, por lo que en este caso, sólo lo dejamos enunciado, en virtud de que la esencia de nuestra tesis, es el análisis de estos supuestos, la revisión que hacemos de la Exposición de Motivos del mismo y la aplicación de los métodos comparativo, analítico e histórico del artículo 211 Bis-1 hasta el 211 Bis-7 del Código Penal Federal, junto con los comentarios, críticas y propuestas a los mismos.

Resulta interesante para nuestra investigación, lo que dice Jaime Villa Escobosa, en cuanto al tema en estudio, quien afirma: "A la par de estas conductas tipificadas en el Código Penal Federal, el sistema jurídico mexicano contempla otras conductas típicas, antijurídicas, culpables y punibles, que se contienen en diversas leyes especiales. De acuerdo al artículo 6, del citado Código, 'Cuando se cometa un delito no previsto en este Código, pero sí en una ley especial o en un Tratado Internacional de observancia obligatoria en México, se aplicarán éstos, tomando en cuenta las disposiciones del Libro Primero del presente Código, y, en su caso, los conducentes del Libro Segundo. Cuando una misma materia, aparezca regulada por diversas disposiciones, la especial prevalecerá sobre la general'.

En México –continúa diciendo Villa Escobosa- numerosas leyes especiales, tipifican delitos. Verbigracia, de las Leyes de Vías Generales de Comunicación, la Ley General de Salud, la de la Propiedad Industrial y los diversos ordenamientos en materia financiera, entre muchas otras". [12]

De la opinión del jurista mencionado, se infiere que los delitos informáticos, regulados en México, en el Código Penal Federal, se reflejan permanentemente

[12] VILLA ESCOBOSA, Jaime. Ob. Cit. pp. 259 in fine y 260.

en la comisión de delitos que afectan a las personas jurídicas físicas y jurídicas colectivas, en su calidad de usuarios de los servicios financieros, las instituciones de éstos y las de seguridad.

III. SURAMÉRICA

A) CHILE

Este país, es un ejemplo interesante de los delitos informáticos, su Ley 19.223, que es pionera en la materia. En 1993, cuando entró en vigor y como se apunta en su Exposición de Motivos, lo que se ha pretendido, es proteger la calidad y la pureza o idoneidad de la información contenida en un sistema digital del tratamiento de éste y de sus productos o de lo que de éstos se obtengan, estén protegidos.

Esta ley tiene cuatro artículos fundamentales, que hablan de penas graves, si hay mala fe para destruir o inutilizar sistemas de tratamiento de información o de sus partes, si se afectan esos datos, así como si hay el ánimo de apoderarse de esa información, para usarla en forma personal o a quien les destruyan los datos de esos sistemas y también reciban una pena grave.

Finalmente, ordena penas de cárcel, para quienes incurran en esas conductas, pero en realidad, lo que para nosotros es más importante, es que esta ley se refiere a lo que es esencia de nuestra tesis, en relación al sabotaje y espionaje informático, si bien, no está explícito, entendemos que se llevan a cabo estos delitos, cuando se atenta contra el hardware y que se destruya o inutilice, porque originaría un delito informático a pesar de que los daños sean convencionales.

Quizá encontraríamos que este sabotaje informático, hecho de manera maliciosa, tienda a dañar o destruir los datos contenidos en un sistema, que es la razón de los artículos del Código Penal Federal mexicano, a los que nos hemos referido. Si bien, no se incluye el hacking o el fraude informático, sí es importante subrayar, que hay penas severas y se dan los tipos donde haya dolo, que se ingrese indebidamente a un sistema para conocer la información sin autorización. Igualmente, quien dé a conocer con dolo, el contenido de esa información, que se haya guardado en el sistema informático. Por ello, es importante esta referencia,

aunque breve de la ley chilena, que entró en vigor en 1999 y en México se reguló sobre el tema seis años después. [13]

[13] VILLA ESCOBOSA, Jaime, Ob. Cit. p. 253.

B) ARGENTINA

Este país, sigue la misma tendencia que los chilenos y un año después de ellos, intenta una legislación, aun cuando no es específica, sobre delitos informáticos. Lo que los argentinos pretenden, es proteger las obras y bases de datos de software, que se van a agregar a su ley de propiedad intelectual, según el Decreto del 8 de febrero de 1994.

Por no ser esencia de nuestra investigación, sólo dejamos la mención somera, agregando que en el artículo 72, se determinó que el propósito es proteger los programas de computación, los sistemas o la información en ellos contenidos, para sancionar a quienes, con conductas delictivas, así como el ingreso no autorizado, la violación de secretos, el espionaje, el uso indebido, el sabotaje, la permanencia en los sistemas que traen como consecuencia una sanción.

En este caso, los argentinos aplican sanciones leves; como indemnizar por los daños sufridos en dinero, no hay sanción de prisión y hace referencia al Código Civil argentino, que vincula actos ilícitos, ejecutados con la intención de dañar y que en este caso, esta legislación erróneamente llama delito, con una falta de técnica y obliga a reparar los daños causados por los mismos. En este caso, solo hacemos esta mención, para destacar que esta ley regula la indemnización, debiendo pagar la cosa destruida.

José Saéz Capel, jurista argentino, rechaza “la existencia de una categoría que con autonomía propia, puede ser considerada como conducta punible del delito informático”. [14]

La Revista Electrónica de Derecho Informático No. 45, publicó el artículo “Delitos informáticos o delitos cometidos por medios informáticos. El bien jurídico tutelado”, de la autoría de Saéz Capel, quien sostiene que es absurdo, fundados

[14] DÍAZ GARCÍA, Alexander, Ob. Cit., p. 163.

en la modernidad, proponer delitos, cuya única vinculación con las computadoras, es su conexión; sostiene que es absurdo tipificar los delitos informáticos, por el solo hecho de usar la información digital y relacionarla con la informática, se declara enemigo de crear nuevas leyes especiales de delitos informáticos, exponiendo, que "en Argentina estos argumentos no son nuevos, ya fueron planteados en el Comité Restringido sobre Delincuencia Económica del Consejo de Europa y ha sido resuelto con un criterio realista, prudente y eficaz. Arguye que no debe utilizarse al Derecho Penal, sino cuando por razón del bien jurídico tutelado, la intensidad de la vulneración y la propia realidad social, tal como allí se dijo, resulta indispensable". [15]

En resumen, para este autor, aun cuando el delito se relacione con la informática, no cambia en su esencia el contenido del hecho ilícito penal; reconoce que si bien es verdad, que los sujetos activos de los delitos informáticos, tienen características especiales, no son suficientes "para crear nuevos tipos penales". [16]

[15] Loc. Cit.
[16] Loc. Cit.

C) VENEZUELA

En el año 2001, Venezuela promulgó y puso en vigor la Ley Especial Contra los Delitos Informáticos. En la misma, se protegen determinados bienes jurídicos; como las tecnologías de información; el derecho de propiedad; la privacidad de las personas; de las comunicaciones y la protección de niños, niñas y adolescentes, así como los delitos que atentan contra el orden económico. [17]

En el primer caso, se regula el acceso indebido a un sistema; el sabotaje o daño a sistemas; la posesión de equipos o prestación de servicios para actos de sabotaje y el espionaje informático; estableciendo penas privativas de la libertad de uno a seis años de prisión y multas elevadas. Incluyen la falsificación de documentos, utilizando las tecnologías de información.

En los delitos contra la propiedad, se tipifican como tales, el hurto y el fraude, usando indebidamente tecnologías de información; obtener bienes por medio de tarjetas de crédito o semejantes; creando, duplicando o incorporando datos a registros o listas de consumo; apropiarse de tarjetas inteligentes y la posesión de equipos para falsificar.

En tercer lugar, están los delitos cometidos contra la privacidad de las personas y de las comunicaciones; abarcando las que tienen por objeto, violar cuestiones de carácter personal; o las comunicaciones o revelar indebidamente datos privados o personales, agregando penas, que van de dos meses a seis años de prisión.

El caso de los delitos informáticos, contra niños y adolescentes, encuentran cabida, cuando se da la difusión o exhibición de material pornográfico, sin advertir, que su uso se restrinja a menores de edad. Lo mismo ocurre, cuando se da la exhibición pornográfica de niños o adolescentes, y en ambos supuestos, las penas de prisión van de dos a ocho años y multas elevadas.

[17] Ob. Cit. p. 257.

Finalmente, en los delitos cometidos contra el orden económico, están los que se tipifican, cuando alguien, usando la reproducción, divulgación, modificación o copia de un software, hace suya indebidamente la propiedad intelectual. También se incluye en esta clase de delitos, a quienes haciendo ofertas engañosas de bienes o servicios, utilicen la información digital; en ambos supuestos, además de las multas, las penas privativas de la libertad son de uno a cinco años. [18]

[18] DÍAZ GARCÍA, Alexander. Ob. Cit. pp. 172 y ss.

CAPÍTULO SEGUNDO
NUEVO PROYECTO DE REFORMAS Y ADICIONES A LOS DELITOS INFORMÁTICOS; APLICACIÓN DE LA DOGMÁTICA JURÍDICO-PENAL A LOS MISMOS Y EL ANÁLISIS DE DIVERSAS DEFINICIONES

I. NUEVA PROPUESTA DEL PODER LEGISLATIVO FEDERAL MEXICANO PARA REFORMAR Y ADICIONAR EL MARCO JURÍDICO NACIONAL VIGENTE EN MATERIA DE DELITOS INFORMÁTICOS

A) PROPUESTA DE LOS SENADORES Y DIPUTADOS FEDERALES

B) ADICIONES Y REFORMAS AL CÓDIGO PENAL FEDERAL

1.- Artículo 139

2.- Artículo 178 Bis

3.- Artículo 211 Bis-2 y 211 Bis-3

4.- Artículo 211 Bis-7

5.- Artículo 211 Bis-8

6.- Artículo 211 Bis-9

7.- Artículo 211 Bis-10

8.- Artículo 211 Bis-11

9.- Artículo 211 Bis-12

10.- Artículo 211 Bis-13

11.- Artículo 211 Bis-14

II. APLICACIÓN DE LA DOGMÁTICA JURÍDICO-PENAL A LOS DELITOS INFORMÁTICOS

A) DEFINICIÓN PERSONAL DEL DELITO INFORMÁTICO

B) ANÁLISIS DE LOS ELEMENTOS DEL CONCEPTO DE DELITO INFORMÁTICO, PROPUESTA PERSONAL

1.- CONDUCTA POR ACCIÓN U OMISIÓN

2.- TIPO Y TIPICIDAD

3.- ANTIJURIDICIDAD

4.- LA IMPUTABILIDAD COMO PRESUPUESTO NECESARIO DE LA CULPABILIDAD

5.- ELEMENTOS COMPLEMENTARIOS DEL DELITO INFORMÁTICO

C) REALIDAD EN MÉXICO

D) VISIÓN INTERNACIONAL

E) CONVENCIÓN DE BUDAPEST SOBRE DELITOS INFORMÁTICOS

F) EL IMPACTO DE LOS DELITOS INFORMÁTICOS A NIVEL INTERNACIONAL

G) SITUACIÓN EN MÉXICO DE LOS DELITOS INFORMÁTICOS DEL 2009 AL 2012

III. ANÁLISIS DE DIVERSAS DEFINICIONES Y CONCEPTOS DE LOS DELITOS INFORMÁTICOS

I. NUEVA PROPUESTA DEL PODER LEGISLATIVO FEDERAL MEXICANO, PARA REFORMAR Y ADICIONAR EL MARCO JURÍDICO NACIONAL VIGENTE RESPECTO A LOS DELITOS INFORMÁTICOS

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

Con esta información, salta a la vista, que México no tiene una ley específica, en delitos informáticos. No obstante, aunque existen disposiciones en la materia, que se encuentran dispersas, dentro del marco jurídico nacional, han sido insuficientes, para combatir conductas delictivas en medios cibernéticos.

Si bien la tecnología ha generado grandes beneficios económicos, al mismo tiempo, ha facilitado el aumento del crimen cibernético. De ahí la necesidad de incluir y actualizar, el catálogo de los delitos previstos en nuestro marco jurídico penal, a fin de adecuarlo para tipificar otras conductas delictivas llevadas a cabo a través de Internet.

Debemos insistir, en que el Poder Legislativo Federal, ha manifestado su interés en la atención de esta delincuencia, por medio de la presentación de diversas iniciativas y, en concreto, con la emisión de un punto de acuerdo, de la Comisión Permanente del Senado de la República, en el que se exhorta al

Ejecutivo Federal para que México se adhiera formalmente a la Convención de Budapest.

Se destaca, que éste es un mecanismo bien articulado, vasto en sus concepciones, explícito en sus medios y fines, y respetuoso de la soberanía y de los sistemas judiciales de los países adherentes, a los que concede un notable campo de acción, a nivel internacional, en la investigación, persecución y sanción de los delitos cibernéticos.

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

Las líneas principales de esta iniciativa de reformas, en Derecho Penal, son reflejan el interés del Estado Mexicano, de regular ilícitos que, además, de no ser privativos nuestros, constituyen un grave problema, frente a la evolución en la tecnología.

Por otro lado, los delitos cibernéticos, además de ser expresión negativa de la globalización, su nulo o inadecuado tratamiento jurídico, puede interrumpir el esquema de seguridad de la información de la Nación y, rebasar las estructuras de contención, control y vigilancia, implementadas por el Gobierno para estos efectos.

Los legisladores federales, proponen adicionar y reformar diversos preceptos del Código Penal Federal, de la Ley General para prevenir, sancionar y erradicar, los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, del Código Federal de Procedimientos Penales, de la Ley de la Policía Federal y de la Ley Federal de Telecomunicaciones.

Su finalidad es alinear las disposiciones del orden jurídico nacional, con las exigencias impuestas por el avance tecnológico y la situación social actual de México, en materia de delitos cibernéticos.

A) PROPUESTA DE LOS SENADORES Y DIPUTADOS FEDERALES

De la propuesta original del Poder Legislativo Federal, de adicionar y reformar, no sólo el Código Penal Federal, sino la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, el Código Federal de Procedimientos Penales, la Ley de la Policía Federal y la Ley Federal de Telecomunicaciones, haremos mención, sólo a la vinculada con nuestra investigación, que se relaciona con los artículos 139, 178 Bis, 211 Bis-2, 211 Bis-3, 211 Bis-7, del Código Penal Federal, creando y proponiendo esos legisladores, nuevos delitos, que se identifican con los numerales, 211 Bis-8, 211 Bis-9, 211 Bis-10, 211 Bis-11, 211 Bis-12, 211 Bis-13 y 211 Bis-14, cuyos textos, por su trascendencia, transcribimos a continuación.

B) ADICIONES Y REFORMAS AL CÓDIGO PENAL FEDERAL

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

2. Artículo 178 Bis, se propone incluir como sujeto de la conducta delictiva a las comercializadoras de servicios de telecomunicaciones o del concesionario de comunicación vía satélite, al ser ellos quien en un momento dado proporcionan directamente el servicio. Asimismo, se incluyen los delitos contemplados en el Capítulo II del Título Noveno referentes al acceso ilícito a sistemas y equipos de informática, en los cuales hay modificaciones, añadiéndose nuevos tipos penales.
Finalmente, se determina la misma sanción para quienes incumplan de forma inmediata las obligaciones de conservación de tráfico de datos, que se refieren a la duración, fecha, hora, origen y destino de los datos; y de contenido, es decir, la información que se envía. Lo anterior no excluye las sanciones que correspondan por la violación a la secrecía.

3. Artículo 211 Bis-2 y 211 Bis-3, se considera necesario sancionar a quien sin autorización, o contando con ésta, pero de manera indebida, conozca, obtenga, copie o utilice información contenida en sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad nacional, por lo que se adiciona esta hipótesis a la que se encuentra vigente en los artículos en cita con

respecto a la información de seguridad pública, toda vez que se trata de bienes jurídicamente tutelados análogos. En consecuencia, se propone adicionar la sanción de inhabilitación o destitución, según corresponda, para quienes cometan esos delitos y sean o hayan sido servidores públicos de alguna instancia de seguridad nacional.

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

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

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

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

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

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

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

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

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

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

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

10. Artículo 211 Bis-13, el orden jurídico nacional prevé el tipo penal de fraude informático únicamente en operaciones con instituciones de crédito, según

lo establece el artículo 400 Bis por lo que se considera necesario la creación de un tipo penal que sancione de manera genérica el fraude informático cuyo objetivo es tipificar como delito cualquier manipulación indebida en el curso de tratamiento de datos con la intención de efectuar una transferencia ilegal de la propiedad.
Las manipulaciones en el fraude informático se tipifican como delito cuando se produce una pérdida económica directa o posesión de la propiedad de otra persona y el autor actuó con la intención de obtener una ganancia.

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

De igual forma, define que se entiende por datos informáticos, toda representación de hechos, actos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema de informática ejecute una función.
Finalmente, establece la forma en que se tratará a las personas morales en la comisión de los delitos comprendidos en este Capítulo.

II. APLICACIÓN DE LA DOGMÁTICA JURÍDICO-PENAL A LOS DELITOS INFORMÁTICOS

En este Capítulo, es importante revisar las reglas generales sobre delitos y responsabilidad y entender, que "el dogma de legalidad –nadie puede ser castigado sino por los hechos que la ley previamente ha definido como delitos, ni con otras penas que las en ellas establecidas (nullum crimen nulla poena sine lege)- se encuentra consagrado en el artículo 7º, que no es sino corolario de las garantías consignadas en el art. 14 Const." [19]

La dogmática jurídico-penal, es una herramienta útil para definir nuevos delitos o conductas, que debe sancionar la ley y en ella nos estamos apoyando, para proponer nuestro concepto de delito informático. En el estudio de los delitos informáticos, es esencial ubicarse en la definición jurídica del delito y aceptar, como elementos indispensables, "la conducta, la tipicidad, la antijuridicidad y la culpabilidad." [20]

En este sentido, el maestro Fernando Castellanos Tena, sostiene que la imputabilidad, no es un elemento esencial del delito. Se refiere a que ésta, es un presupuesto necesario de la culpabilidad y en cuanto a los elementos tradicionales del delito, afirma "que el acto o la omisión se tienen como delictuosos, por su oposición con las exigencias estatales para la creación y conservación del orden social y por ejecutarse culpablemente; es decir, con conocimiento y voluntad; más no puede tildarse de delictuosa una conducta por el hecho de que sea punible". [21]

[19] GONZÁLEZ DE LA VEGA, Francisco, El Código Penal Comentado, 9ª edición. Editorial Porrúa, México, 1989. p. 54
[20] GÜITRÓN FUENTEVILLA, Julián, El Delito de Atentados al Pudor (Estudio Dogmático), Universidad Nacional Autónoma de México, Facultad de Derecho, Talleres Gráficos Galesa, México, 1961. p. 28
[21] CASTELLANOS TENA, Fernando, Lineamientos Elementales de Derecho Penal. Editorial Jurídica Mexicana, México, 1959. p. 126

A) DEFINICIÓN PERSONAL DEL DELITO INFORMÁTICO

Las expresiones transcritas, han sido una guía importante para nosotros, para proponer la definición o concepto de los delitos informáticos, haciendo prevalecer en ellos, la acción u omisión, la tipicidad, la antijuridicidad y la culpabilidad. Lo conceptualizamos como, toda acción u omisión típica, antijurídica y la culpabilidad, realizada por una persona jurídica física, desde cualquier lugar, para sustraer, destruir, modificar, utilizar o copiar, información digital protegida, utilizando cualquier equipo informático, computadora, internet o alguno semejante, para cometer un delito contra la propiedad intelectual, sistemas de seguridad, sistemas financieros públicos o privados o actividades semejantes.

B) ANÁLISIS DELOS ELEMENTOS DEL CONCEPTO DE DELITO INFORMÁTICO PROPUESTA PERSONAL

1.- CONDUCTA POR ACCIÓN U OMISIÓN

Con especial énfasis, debemos destacar que la conducta, es el primer elemento de este delito, quien involucra la acción u omisión que realice el sujeto activo del ilícito, que debe tener la capacidad técnica o el conocimiento, para poder, en su caso, sustraer, dañar o utilizar la información dentro de una computadora, que esté protegida por un sistema de seguridad.

La acción, no requiere más explicaciones, empero, la omisión sí, porque el responsable, el vigilante, quien tenga a su cargo las funciones de salvaguardar esa información, podría disimular, abstenerse de señalar la posible comisión del delito o simplemente voltear para otro lado, cuando se estuvieran cometiendo las acciones o los hechos ilícitos.

2.- TIPO Y TIPICIDAD

El segundo elemento, que de manera general, referimos en nuestra propuesta, es que esa conducta sea típica, en este caso, subrayar en que la tipicidad, es la adecuación de la conducta del sujeto activo del delito al tipo, entendido éste, como sinónimo de norma legal, que determina cuáles deben ser las características, de quien realiza la conducta, para que en palabras muy simples, se adecue la conducta al tipo y podamos hablar de la tipicidad, como segundo elemento del delito informático.

Incluso, en el desarrollo de esta investigación, cuando decimos dogmática jurídico-penal, destacamos el aforismo latino, nullum crimen sine lege; es decir, no hay delito sin ley. En el delito informático, sobran los ejemplos del tipo en abstracto, legislado en los artículos 211 Bis-1 al Bis-7, en los que se ha sostenido claramente que quien ejecute la sustracción, destrucción, modificación, utilización o copia de la información digital protegida, estará materializando con su conducta, la tipicidad del delito informático.

3.- ANTIJURIDICIDAD

La antijuridicidad surge cuando se actúa en contra de una norma jurídica. Cuando hay una oposición subjetiva al mandato legal. Si la conducta del sujeto activo del delito informático, va en contra de la ley, surge la antijuridicidad; sería absurdo decir, que lo antijurídico es contrario al Derecho, porque en realidad, la norma está determinando, ordenando, que si la acción u omisión del sujeto activo del delito va en contra de ese presupuesto normativo, habrá antijuridicidad.

Sería tautológico afirmar, que quien sustrae en forma indebida, la información de una computadora, protegida por la ley, comete del delito informático. La opinión, de quien fuera un gran jurista, especialista en Derecho Penal, Celestino Porte Petit, respecto al concepto de antijuridicidad, es tan importante para este estudio, que nos permitimos transcribirla a continuación: "Una conducta o hecho son antijurídicos cuando siendo típicos no están protegidos por una causa de justificación, al realizarse una conducta o un hecho adecuados al tipo, se les tendrá como antijurídicos, en tanto no se pruebe la existencia de una causa de justificación.

Hasta hoy día, así operan los Códigos Penales, valiéndose de un procedimiento de excepción, es decir, en forma negativa, lo cual quiere decir que para la existencia de la antijuridicidad, se requiere una doble condición: positiva una, adecuación de la conducta o hecho a una norma penal; y negativa otra, que no estén amparados por una causa de exclusión del injusto. La conducta o hecho serán antijurídicos si no están protegidos por alguna de las causas que enumera el Código Penal en su propio artículo 15". [22]

En síntesis, cuando el sujeto activo del delito, realiza su conducta para sustraer la información, protegida de una computadora, surge con plenitud, la antijuridicidad. Formal y materialmente, se dan los dos supuestos, porque por un

[22]PORTE PETIT, Celestino, Programa de la Parte General del Derecho Penal, editado por la Universidad Nacional Autónoma de México, México, 1968. p. 285

lado, se lesiona el bien jurídico protegido, que es la información y por otro, se transgrede el mandato de la ley.

4.- LA IMPUTABILIDAD COMO PRESUPUESTO NECESARIO DE LA CULPABILIDAD

Para hablar de la culpabilidad, como cuarto elemento esencial del delito informático, es necesario examinar el presupuesto necesario, para que se dé este elemento del ilícito, que es la imputabilidad.

Será imputable, en el delito informático, el sujeto que al realizar la conducta, tenga condiciones mínimas de salud y desarrollo mental, que lo capacite para actuar en el campo del Derecho Penal. Para ubicar como culpable a una persona, del delito objeto de este estudio, es fundamental que la misma, tenga adecuada salud y desarrollo mentales; por ello es necesario, indispensable, que para cometer el delito informático, el sujeto activo, quiera realizar el acto, sepa lo que hace; es decir, que haya una vinculación o un nexo emocional entre él y el acto o hecho que va a realizar.

Por ello, es importante reflexionar, que el presupuesto necesario de la culpabilidad, en el delito informático, es la imputabilidad.

Atendiendo al concepto que el penalista mexicano, Ignacio Villalobos, propone, para definir la culpabilidad, estamos de acuerdo con él, en que ésta surge en general, cuando el sujeto activo del delito, en este caso, el informático, desprecia el sistema jurídico y los mandatos legales y prohibiciones, lo cual puede hacer abiertamente, lo que traería como consecuencia, una actuación con dolo, “o indirectamente por indolencia y desatención, nacidas del desinterés o subestimación del mal ajeno frente a los propios deseos, en la culpa”. [23]

[23] VILLALOBOS, Ignacio, Derecho Penal Mexicano, Editorial Porrúa, México, 1960. p. 272

En resumen, podemos afirmar, que el sujeto activo del delito informático, es quien tiene un comportamiento típico, antijurídico y culpable, al cual el Estado impone penas privativas de la libertad, atendiendo a la gravedad del delito cometido.

Por la esencia de los supuestos jurídicos de los delitos informáticos, que regula el Código Penal Federal, debemos dejar constancia de que la culpabilidad, se puede presentar en forma dolosa o culposa, "según que el sujeto encamine su voluntad consciente a la ejecución de un hecho típico y antijurídico, -delito informático- o que sin pretender la producción del resultado, éste surja porque no fueron puestos en juego las cautelas y precauciones necesarias exigidas por el Derecho para la conservación del orden de la vida gregaria. Será dolosa la conducta –en el delito informático- si se realiza con la voluntad dirigida hacia el hecho ilícito; habrá culpa, cuando se obra con torpeza, negligencia, impericia, irreflexión, falta de precaución o de cuidado, produciendo un resultado típico y antijurídico, previsible y evitable". [24]

5.- ELEMENTOS COMPLEMENTARIOS DEL DELITO INFORMÁTICO

Para darle más contundencia a nuestra aportación en esta materia, debemos reflexionar, sobre los otros elementos que hemos agregado a nuestro concepto, ya que esa conducta, debe ejecutarse por una persona jurídica física; que además, al realizarla, desde cualquier lugar en el mundo, le da la posibilidad de sustraer, destruir, modificar, utilizar o copiar la información digital protegida. También es un elemento que debe sumarse a esta definición, que para realizar esa acción, se puede utilizar cualquier equipo informático, incluyendo en esto, las computadoras, Internet o alguno semejante.

Siempre con la preocupación, de que el bien jurídico protegido en el delito informático, esté claramente definido, subrayamos la hipótesis de que el delito se cometa contra la propiedad intelectual o sistemas de seguridad o financieros, sean

[24] GÜITRÓN FUENTEVILLA, Julián, Ob. Cit. p. 98

públicos o privados, haciendo extensiva esta hipótesis a actividades semejantes a las mencionadas.

C) REALIDAD EN MÉXICO

La proliferación de los ciberdelitos en nuestro país, obligaron al Estado Mexicano, a que en el año de 1999, el 17 de mayo, se publicara en el Diario Oficial de la Federación del Código Penal Federal, el Título Noveno, que se le denominó, “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática”, que en dos Capítulos; el primero, referido a la revelación de secretos y el segundo, que es el objeto de esta tesis, se le denominó “Acceso Ilícito a Sistemas y Equipos de Informática”; en éste, se crearon los artículos 211 Bis-1 al 211 Bis-7 y en ellos, se establecieron varios tipos, cuyo propósito fue castigar a los sujetos activos de esos delitos por modificar, destruir o provocar pérdida de información que estuviera contenida en los sistemas o equipos de informática.

Hay diferentes situaciones, que comentaremos más adelante, que agregan las hipótesis de estar o no autorizados para acceder a esos sistemas, o concretarse a conocer o copiar la información citada. Otros supuestos, mencionan, en unos casos, sin y en otros con autorización, a introducirse a esos sistemas que fueran financieros o de seguridad pública, con penas, que desde nuestra perspectiva no fueron lo suficientemente severas, para prevenir y en su caso, sancionar estos hechos ilícitos penales.

Por la trascendencia que tiene para esta investigación, la exposición textual de motivos del Título mencionado, la reseñaremos a continuación, agregando algunos comentarios, que consideramos son trascendentes y sobretodo, que si bien México ingresó a la era cibernética de los delitos a finales del siglo XX, han transcurrido casi tres lustros y la aportación que en su momento, hizo el legislador penal federal, ha quedado rebasada.

Razón ésta, entre otras, por la que nos hemos dado a la tarea de elaborar este trabajo, y hacer en el mismo, algunas recomendaciones, que van desde la exposición de motivos nuestra, hasta la creación y nueva redacción, con algunos agregados, de los preceptos penales, que deben reformar los artículos originales

del año 1999, a que nos hemos referido antes, así como las adiciones que en el año 2009, se hicieron en cuanto a los párrafos tercero del artículo 211 Bis-2 y del 211 Bis-3.

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

Atender este fenómeno delictivo, por parte de las autoridades federales, estatales y organismos internacionales, es complejo, en atención a que en algunos casos, las conductas se realizan con equipos electrónicos, situados en algún país, que no es el mismo, donde se genera el daño o perjuicio.

Esta nueva modalidad, para la comisión de ilícitos, permite a los criminales, lograr sus objetivos sin arriesgar su integridad física, basta tener un equipo electrónico, red de Internet y capacidad técnica, para usar éstos, en la comisión de un delito informático, en cualquier parte del mundo.

Por ello, diversos países han emitido disposiciones jurídicas, para penalizar esas prácticas que se dan en el mundo virtual, con una perspectiva global, para buscar y lograr una efectiva cooperación internacional, para perseguir y sancionar esas conductas ilícitas.

D) VISIÓN INTERNACIONAL

Siguiendo este derrotero, algunos organismos internacionales, como las Naciones Unidas, la Organización para la Cooperación y el Desarrollo Económicos, la Unión Europea, el Consejo de Europa y la Organización de los Estados Americanos, entre otros, han propuesto acciones técnicas, y jurídicas y de cooperación multilateral, de investigación, persecución y prevención, para combatir la ciberdelincuencia, atendiendo a su carácter transnacional.

En nuestro sistema jurídico, el delito informático, tiene más de diez años, en comparación con otros sistemas jurídicos, en los que su regulación, deviene desde los inicios de la segunda mitad del siglo pasado, verbigracia, Estados Unidos de América, con la propuesta del Senador Abraham Ribicoff de 1977, para legislar en materia de ciberdelitos.

Posteriormente, en 1983, la Organización para la Cooperación y el Desarrollo Económicos, designó un comité de expertos para estudiar el tema, quienes emitieron un dictamen para recomendar a los países miembros de la misma, incorporar la regulación de los delitos informáticos en su legislación penal.

En 1989, el Consejo de Europa, recomendó considerar los delitos mínimos, que debería agregar a su legislación, cada país miembro.

Tener una regulación específica de delitos informáticos, ha sido parte de la agenda, en diversos foros internacionales; así, el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal, Canadá (1990), el Octavo Congreso Criminal de las Naciones Unidas (1990) y la Conferencia de Wurzburgo, en Alemania (1992).

Con base en estos antecedentes, la comunidad internacional, creó en 1996, el Comité Especial de expertos, sobre delitos relacionados con el empleo de

computadoras, integrado por especialistas para luchar contra los delitos cibernéticos, en particular, los cometidos usando las redes de telecomunicaciones.

E) CONVENCIÓN DE BUDAPEST SOBRE DELITOS INFORMÁTICOS

El Comité citado, elaboró un proyecto jurídico internacional, para atender ese fenómeno delincuencial. En noviembre del 2001, el Consejo de Ministros de Europa, junto con los de Estados Unidos de América, Sudáfrica, Canadá y Japón, firmaron en Budapest, Hungría, la Convención sobre Delitos Informáticos; la cual ha sido hasta ahora, la principal directriz, para que los Estados parte, tengan en su ámbito interno, una base jurídica firme en Derecho Penal y una sistematización de instrumentos de investigación, de salvaguardas conexas, que protejan los derechos humanos y procuren darle viabilidad en la lucha contra los ciberdelincuentes.

Los principales temas en la materia, armonizan las leyes penales sustantivas y adjetivas, para adecuar al tipo, las conductas que puedan ser acciones u omisiones delictivas, cuyo escenario sea el entorno informático.

Desde el punto de vista del Derecho Procesal Penal, facultar a las autoridades correspondientes, para ejercer los derechos indispensables, para investigar y perseguir los delitos informáticos con éxito.

La cooperación internacional en la materia, es tan importante, que debe establecerse un régimen que se retroalimente y permita resultados óptimos, en las investigaciones.

En este contexto y derivado de las amenazas a los sistemas informáticos, es preciso tener un marco jurídico de referencia, que permita perseguir y sancionar los delitos informáticos, incluyendo los requerimientos fundamentales de carácter internacional, para elaborar sistemas de coordinación y cooperación internacional, con todos los Estados involucrados en esta importante lucha, atendiendo a los mecanismos más importantes para asistir, desde el punto de vista de la ley, tanto a nivel regional cuanto mundial, para prevenir, investigar y sancionar la comisión de esos delitos.

También es importante, subrayar las consecuencias de estos delitos, en cuanto a la estabilidad y gobernabilidad de los Estados, ya que, la realización de estos hechos ilícitos, permiten obtener información que afecta las áreas neurálgicas o estratégicas o sencillamente para difundir rumores, mensajes, imágenes, fotografías o videos, cuyo objetivo, sea sembrar el terror y amedrentar a la sociedad, con lo cual se merma la seguridad nacional y en consecuencia, se alteran total o parcialmente, las funciones de las autoridades del Estado.

Es del dominio público, que la delincuencia organizada y sus grupos colaterales, como los terroristas o sujetos individuales, han logrado establecer impresionantes redes sociales, para comunicarse o han creado sistemas electrónicos, para identificar a sus víctimas, para realizar planes de ataque, para obtener información en páginas de los diferentes gobiernos, de los partidos políticos, de los sectores sociales, de los privados o para hacer propaganda y lograr adeptos y ampliar su base social, en cuanto a sus postulados terroristas.

Estas consideraciones, obligan a proponer sanciones contra los actos terroristas, que utilizan las diferentes redes de comunicaciones o los sistemas electrónicos, aprovechando la falta de legislación y los vacíos legales que como consecuencia, afectan la integridad, la gobernabilidad, la estabilidad o la durabilidad de los Estados.

F) EL IMPACTO DE LOS DELITOS INFORMÁTICOS A NIVEL INTERNACIONAL

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

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

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

El informe apunta que cerca del 65 por ciento de adultos, en el mundo, han sido víctimas de algún tipo de estos delitos, tales como, estafas *online,* ataques de *phishing,* actividades de piratas informáticos en perfiles de redes sociales y fraudes con tarjetas de crédito.

En cuanto a los responsables de estas conductas ilícitas, un 56 por ciento son delincuentes anónimos y un 21 por ciento grupos organizados.

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

En cuanto al daño económico, que representa la comisión de estos hechos ilícitos, la encuesta afirma que el monto por las actividades de estos delitos, supera los 388 mil millones de dólares.

Asimismo, subraya que se gastaron directamente 114 mil millones de dólares, debido al dinero robado por los delincuentes, o bien, al monto gastado en resolver los ataques cibernéticos. Igualmente, se determina que el gasto equivalente al tiempo perdido, valuado por las víctimas, se estima en 274 mil millones de dólares.

G) LOS DELITOS INFORMÁTICOS EN MÉXICO, DEL 2009 AL 2012

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

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

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

La Secretaría de Seguridad Pública, en su Cuarto Informe de Labores (Septiembre de 2009-julio de 2010) refiere que en México, las principales conductas delictivas en Internet registradas son el *hackeo, phreaking,* asesinatos a sueldo, venta de droga, ciberterrorismo, así como programación de virus y códigos maliciosos.

En dicho informe, se destaca el incremento importante en la propagación de estos últimos, ya que en el 2008, se tuvo un registro de 1 millón 691 mil 323 y en 2009, de 2 millones 895 mil 802 casos.

En un quinto Informe de Labores (Septiembre de 2010-julio de 2011) de la misma dependencia, a través de la División Científica de la Policía Federal, se afirma que se realizaron acciones para prevenir, investigar y combatir los delitos cibernéticos, mediante la atención y asesoría a la ciudadanía con base en un monitoreo permanente a la red pública de internet.

De ello, derivaron 5 mil 582 denuncias ciudadanas, las cuales fueron recibidas a través de diferentes medios de captación, a saber: 3 mil 389 vía correo electrónico, 1 mil 432 mediante el Centro Nacional de Atención a la Denuncia Ciudadana de la Policía Federal y 761 por teléfono. Al respecto, las conductas que presentaron un mayor índice de denuncias, fueron el fraude al comercio electrónico y *phishing.*

Si se atiende a las principales conductas delictivas, que se suscitan en nuestro país, conforme a lo narrado por los reportes de la Secretaría de Seguridad Pública, es propio considerar, que en materia de delitos informáticos, se han afectado diversos bienes jurídicos, como el patrimonio, la intimidad, la información, la propiedad e incluso la seguridad nacional.

Asimismo, de acuerdo al Sexto Informe de Labores de esa secretaría, las acciones realizadas por la Policía Federal, a través de la División Científica para Combatir el Delito Cibernético, de junio de 2011, a septiembre de 2012, se detectaron 13 mil 133 incidentes, en materia de ciberdelitos, entre los cuales, han imperado el *phishing,* la negación de servicio, la alteración de contenido*(hacking),* la infección por código malicioso, la propagación de malware y los accesos no autorizados.

Al mismo tiempo, se registró que el promedio de denuncias sobre ciberdelitos, comparado con el periodo de septiembre de 2010 a junio de 2011, se incrementó en un 135 por ciento, ya que pasó de 18 a 44 denuncias, por día aproximadamente.

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

III. ANÁLISIS DE DIVERSAS DEFINICIONES Y CONCEPTOS DE LOS DELITOS INFORMÁTICOS

Por la importancia de la reforma propuesta por el Poder Legislativo Federal en México, en relación a los diversos delitos, especialmente los de revelación de secretos y acceso ilícito a sistemas y equipo de informática, citaremos a continuación, las que nos parecen más trascendentes, que podrían complementar la multicitada iniciativa.

A) GABRIEL ANDRÉS CÁMPOLI

Gabriel Andrés Cámpoli, en su obra denominada, Delitos Informáticos en la Legislación Mexicana, subraya la importancia de diferenciar éstos, de los telemáticos. De los primeros, afirma, que "Son aquéllos en los cuales el tipo penal protege la integridad física o lógica de los equipos informáticos o páginas web, es decir, aquellas acciones en las cuales los equipos informáticos o páginas web resultan objeto del delito". [25]

Del concepto anterior, es criticable que al utilizar la expresión tipo penal, como bien jurídico protegido, se refiera a la parte física o lógica de las computadoras o en su caso, las páginas web, pero no existe relación alguna, a lo que hemos sostenido en esta investigación, en cuanto a que el bien jurídico protegido en los delitos informáticos, más que las cuestiones materiales o los equipos software, lo más valioso, debe ser la información que éstos contienen.

El mismo autor, diferencia los delitos informáticos, de los telemáticos y éstos los define, como "aquéllos que, sin afectar expresamente a un equipo informático en particular, disminuyen o anulan su capacidad de transmisión o procesamiento de datos a distancia, ya sea actuando en forma indirecta sobre el equipo, sobre su capacidad de recepción o envío de datos, sobre sus parámetros lógicos o sobre las vías de comunicación necesarias para las funciones normales del mismo a distancia". [26]

Si bien es cierto, que el delito telemático, no es esencia de nuestra tesis, atendiendo a los elementos que menciona el autor en estudio, se puede hacer la misma crítica, en virtud de que no hay un señalamiento expreso de proteger el contenido o la información que se encuentra dentro de ese equipo informático.

[25]CÁMPOLI, Gabriel Andrés, Delitos Informáticos en la Legislación Mexicana, 1ª reimpresión, Ediciones Corunda e Instituto Nacional de Ciencias Penales (INACIPE) México, 2007, p. 66
[26] Ob. Cit. p. 67

B) IVONNE MUÑOZ TORRES

En esta misma materia, encontramos otras definiciones, que en el caso específico, se vinculan a los delitos cibernéticos, electrónicos, computacionales, telemáticos e informáticos. De éstos, Ivonne Muñoz Torres, autora de la obra "Delitos Informáticos. Diez Años Después", revisa el concepto de la Real Academia Española de la Lengua, de la palabra cibernética y afirma, que este delito se puede tipificar como ilegal, si el mismo, "tiene como finalidad afectar las comunicaciones que se llevan a cabo a través de las Tecnologías de Información y Comunicación". [27]

Para continuar con el análisis de diversos conceptos, debe entenderse por delito electrónico, el que "tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar el flujo electrónico de datos, y que en consecuencia, afecte el funcionamiento de Internet así como de los Sistemas de Información que dependen de la electrónica para desarrollarse". [28]

Llama la atención, que en los delitos citados, el cibernético y el electrónico, no haya una referencia al bien jurídico protegido, en la comisión de éstos, que es la protección de la información que contienen.

En cuanto al delito telemático, se define como, el que "tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las telecomunicaciones y/o las tecnologías de información, cuya consecuencia sea la interrupción de la transmisión de información que esté depositada en un sistema de información". [29]

En este concepto, está la falla, ya apuntada, en virtud de que si la telemática consiste en aplicar sus técnicas de telecomunicación, en los términos

[27] MUÑOZ TORRES, Ivonne Valeria, Delitos Informáticos. Diez Años Después, 1ª edición, Editorial UBIJUS, México, 2009, p. 15
[28] Ob. Cit. pp. 15 in fine y 16
[29] Ob. Cit. p. 17

supracitados, se repite el mismo error, en cuanto a que no tiene, como bien jurídico protegido, salvaguardar la información, que esos aparatos contengan.

La autora en estudio, termina sus reflexiones mencionando el delito informático y sigue aplicando el método gramatical, en cuanto a lo que la Real Academia Española de la Lengua, ha sostenido al respecto, al afirmar que el delito informático, "se define como aquél que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información, cuya consecuencia sea el daño directo o indirecto en ellos, así como el mal uso de éstos". [30]

En este supuesto, se analizan los conceptos de informática, información y datos, según palabras de la jurista Muñoz Torres, empero, no se llega a la esencia de que la suma de esos tres elementos, le den cuerpo al delito y que el bien jurídico protegido, sea la información que se contenga en esas computadoras.

[30] Ob. Cit. pp. 18 in fine y 19

C) JESÚS ANTONIO MOLINA SALGADO

Con un enfoque diferente, a lo que hemos reseñado hasta ahora, surgen las opiniones y razonamientos de Jesús Antonio Molina Salgado, en relación a los delitos y otros ilícitos informáticos, que se relacionan con la propiedad industrial; al respecto, expresa, “aunque no existe una fecha precisa del primer ilícito informático, se sabe que los delitos e ilícitos informáticos nacen inmediatamente después del surgimiento de los medios informáticos, a mediados del siglo veinte.

Varios estudiosos del tema sostienen que los primeros actos ilícitos, dentro de la informática, fueron cometidos por error o inadvertencia, e incluso por ocio. Lo cierto es que, además de estas posibles causas, la mala fe y el dolo, fueron la principal razón de la proliferación de tales ilícitos.

De hecho, el principio que reza: “a toda tesis corresponde una antítesis”, fue aplicado a la tecnología informática desde sus inicios, ya que al poco tiempo de su aparición, se creó una antitecnología informática por los *hackers,-programadores habilidosos o allanadores de sistemas informáticos que alteran programas-los crackers -es el sujeto que rompe algo o descifra un código y también a quienes entran simplemente en sistemas informáticos de terceros constantemente- y los ciberpiratas, -son quienes roban propiedades de terceros en la red para después extorsionar a los legítimos titulares o venderlos al mejor postor-* lo cual casi siempre superó, las capacidades y alcances técnicos y legales de la primera.

Es decir, desde los primeros días de la tecnología digital, los sujetos activos de estos delitos, se dieron a la tarea de crear, modificar, destruir e impedir el acceso a la información confidencial de terceros, a través de virus, candados y otros métodos.

Asimismo, tan pronto como el medio informático, llamado Internet estuvo disponible al público, los primeros ciberpiratas, hicieron su aparición registrando nombres de dominio, direcciones y códigos que constituyen signos distintivos, y

poniendo al alcance de los usuarios de la red, cualquier diseño o proceso de patente, propiedad de terceros, para su explotación industrial.

En las actividades ilícitas, es donde surge lo que hoy conocemos, como delitos e ilícitos informáticos.

Los delitos e ilícitos informáticos, son actualmente, estudiados a la luz de varias ramas del derecho, tales como el Derecho Informático, el Derecho Penal, el Derecho de la Propiedad Industrial, el Derecho Internacional, el Derecho Notarial, el Derecho Administrativo, el Derecho Civil, el Derecho de las Comunicaciones y el Derecho Fiscal, entre otras.

Sin duda alguna, en la medida que avance el tiempo y exista una concientización en todas las personas, que participan activa y pasivamente en las tecnologías informáticas, los delitos informáticos irán encontrando cabida en las disposiciones legales relativas a las ramas del derecho arriba citadas, ya sea como delitos típicos y atípicos". [31]

De la información transcrita, es relevante la visión panorámica, que Molina Salgado, nos da de esta materia, y sobre todo, desde la aparición de los medios informáticos a la fecha, han transcurrido aproximadamente setenta años y todavía no hay respuestas legales adecuadas, para combatir a los sujetos activos de los delitos informáticos, que acertadamente este autor, proyecta a otras ramas del Derecho como el Civil, el Notarial y el de las Comunicaciones.

Estamos de acuerdo con él, en que todavía no hay una definición jurídica adecuada, y mucho menos en el Código Penal Federal, que se vincule a los delitos informáticos, ya que, sí se sanciona el acceso ilícito a los sistemas y equipos de informática.

[31] MOLINA SALGADO, Jesús Antonio, Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial, Editorial Porrúa, México, 2003, pp. 17 y 18

D) JULIO TÉLLEZ VALDÉS Y CARLOS SARZANA

Dos autores, Julio Téllez Valdés en México y Carlos Sarzana en Italia, han creado dos conceptos del delito informático y así, el primero, dice que existen el atípico y el típico; el primero, se refiere a "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"; [32] en cambio, el segundo, incluye, "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin". [33] Para el autor italiano citado, surge el delito informático, con "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo". [34]

Para Molina Salgado, los delitos informáticos, están íntimamente vinculados con los Derechos de la Propiedad Industrial, y así para él, aun cuando en el Código Penal Federal, "no hay una referencia expresa a la revelación de secretos como un delito informático, es obvio que dicho acto criminógeno, cometido a través de cualquier medio informático, sigue constituyendo un delito y, en el caso específico, un delito informático. De hecho, amén de considerar dicho delito como un acto violatorio de los Derechos de Propiedad Industrial, la legislación penal pretende asociar o de alguna forma tratar a la revelación de secretos como delitos informáticos, por el hecho de incluir este ilícito en el mismo capítulo en el que se contemplan otros ilícitos relacionados con la informática". [35]

La proliferación de diversos conceptos sobre delitos informáticos, nos obliga a analizar los más trascendentes, en virtud de que los autores que han escrito sobre los mismos, o no están de acuerdo o no han considerado que el Derecho Positivo vigente Penal Federal en México, no ha logrado hasta la fecha, conceptualizarlo adecuadamente.

Se afirma por algunos estudiosos, que los delitos informáticos, son aquéllos, donde el sujeto activo, lesiona un bien jurídico que puede o no "estar

[32] Ob. Cit. p. 19
[33] Loc. Cit.
[34] Loc. Cit.
[35] Ob. Cit. p. 25

protegido por la legislación vigente y que puede ser de diverso tipo por la utilización indebida de medios informáticos". [36] Disentimos de la afirmación anterior, porque es elemento indispensable, que el bien jurídico, esencia del delito informático, esté protegido por la ley, en este caso, como lo hemos reiterado, es la información que contiene la computadora.

Este autor, profundiza en su aportación y proporciona una definición más completa, aun cuando desde ahora, manifestamos nuestra inconformidad con ella. En este sentido, Cámpoli sostiene, que "los delitos informáticos son aquellos realizados por el autor con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o impunidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones". [37] Además de larga, esta definición, no va a la esencia de la tipificación del delito, porque deja de lado, el bien jurídico protegido y podríamos decir, que pierde o que carece de género próximo y diferencia específica, en su definición.

Julio Téllez Valdés, aporta a esta materia, opiniones muy importantes, que debemos transcribir y comentar. En su obra, "Derecho Informático", específicamente en estos delitos, acude a los orígenes de los mismos, para referirse a las computadoras, a la tecnología informática, al desafío entre el hombre y la máquina y al respecto, sostiene, que "es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos.

Este tipo de actitudes concebidas por el hombre y no por la máquina, como algunos pudieran suponer, encuentran sus orígenes desde el mismo surgimiento

[36] CÁMPOLI, Gabriel Andrés. Ob. Cit. p. 14
[37] Ob. Cit. p. 17

de la tecnología informática, ya que es lógico pensar que de no existir las computadoras, estas acciones no existirían.

Por otra parte, la misma facilitación de labores que traen consigo dichos aparatos propician que, en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo, sin darse cuenta, una serie de ilícitos.

Por último, por el mismo egoísmo humano se establece una especie de "duelo" entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionados, por ese 'deseo' del hombre de demostrar su superioridad frente a las máquinas, y en este caso específico las computadoras.

De esta forma podemos decir que estas acciones, más que resultado de una situación socioeconómica, se derivan de una actitud antroposíquica, aunque en el terreno de los hechos son una realidad sociológica bien determinada y que requiere, por ende, de un tratamiento jurídico específico". [38]

La sencillez de los comentarios anteriores, nos obligan solamente a dejarlos citados, porque además, consideramos que es una información muy valiosa, para quienes quieran profundizar en la materia de los delitos informáticos. En reflexiones anteriores, aludimos a este autor y parafraseamos algunas de sus propuestas, verbigracia, cuando afirma, que los delitos informáticos, "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".[39]

[38] TÉLLEZ VALDÉS, Julio, Derecho Informático. Editado por el Instituto de Investigaciones Jurídicas de la UNAM y de la Universidad Nacional Autónoma de México, 1987, p. 104
[39] Ob. Cit. p. 105

E) JAIME VILLA ESCOBOSA

Otra definición de delito informático, es sostenida por Jaime Villa Escobosa, quien lo define, “como cualquier actividad o conducta ilícita, susceptible de ser sancionada por el Derecho Penal, que en su realización involucre el uso indebido de medios o sistemas informáticos”. [40]

[40] VILLA ESCOBOSA, Jaime. Ob. Cit. p. 231

F) MARÍA DE LA LUZ LIMA MALVIDO

La jurista María de la Luz Lima Malvido, habla de delitos informáticos, en sentido amplio y en sentido estricto; “el primero es cualquier conducta criminógena o criminal, que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin. El segundo, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones, desempeñan un papel ya sea como método, medio o fin”. [41]

[41] Ob. Cit. p. 232

G) ALEXANDER DÍAZ GARCÍA

Alexander Díaz García, especialista en informática jurídica, en su obra "Derecho Informático", que ya mencionamos anteriormente, acude a Orlando Solano Bárcenas, a Alicia Raquel Lilli y a María Amalia Massa, para definir el delito informático en general.

También reseña la opinión de Claudio Líbano Manssur, y de los tres, relata en la obra citada, lo siguiente: el delito informático se puede definir, desde dos puntos de vista diferentes; "Uno restringido que tiene como aquel hecho en el que independientemente del perjuicio que puede causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal, se atacan elementos puramente informáticos. Tales serán los casos del uso indebido del software, apropiación indebida de datos, interferencias en sistemas de datos ajenos y en el sentido amplio, es la acción típica, antijurídica y culpable para cuya consumación se utiliza o se afecta a una computadora o sus accesorios.[42]

[42]Loc. Cit.

H) CLAUDIO LÍBANO MANSSUR

Este jurista, que también opina sobre los delitos informáticos, es analizado por Díaz García, en cuanto a su propuesta en esta materia y lo describe, “como todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima, a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral, lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro”. [43]

[43]DÍAZ GARCÍA, Alexander. Ob. Cit. p. 155

CAPÍTULO TERCERO

PROYECTO DE REFORMAS AL CÓDIGO PENAL FEDERAL MEXICANO EN LOS DELITOS COMETIDOS POR REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

A) **COMENTARIO**

B) **CRÍTICA**

C) **PROPUESTA**

VIII. ESTUDIO DEL ARTÍCULO 211 BIS 7 DEL CÓDIGO PENAL FEDERAL Y PROPUESTA DE REFORMA.

A) **COMENTARIO**

B) **CRÍTICA**

C) **PROPUESTA**

I. EXPOSICIÓN DE MOTIVOS

En el Título Noveno del Código Penal Federal, denominado Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, en el Capítulo II, que regula el acceso ilícito a sistemas y equipos de informática, se concentra la posición ideológica original de esta tesis, que consiste en proponer un proyecto de reformas a los artículos que comprende el Capítulo citado, que incluyen los numerales 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis-4, 211 Bis-5, 211 Bis-6 y 211 Bis-7 y la Exposición de Motivos correspondiente.

El proyecto de reformas que estamos proponiendo en esta tesis, incluye la justificación de las modificaciones al Código Penal Federal mexicano, que partiendo de un sistema adecuado, entendido éste, como "conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí"; [44] permita que las acciones u omisiones, en los delitos informáticos, se vinculen con el tipo, la antijuridicidad y la culpabilidad como elementos esenciales del delito, relacionados con el bien jurídico protegido en estos delitos, que es la información digital, que se contenga en las computadoras correspondientes.

Respecto al artículo 211 Bis-1, debemos subrayar que en los supuestos de modificar, destruir o provocar pérdida de información, deben reformarse e incluir los elementos fundamentales de la teoría general del delito, empezando por regular la acción u omisión y que éstas, puedan causar un perjuicio o un daño a una persona jurídica física o jurídica colectiva, con el propósito de obtener información automática, que puede ser digital o cibernética, que se guarde en sistemas o equipos informáticos, que a su vez, éstos tengan una protección adecuada, que puede ser de contraseñas o claves de seguridad y también se justifica, en nuestra propuesta, que la pena privativa de libertad, sea mayor a la que originalmente regula el numeral mencionado.

[44]Real Academia Española. Diccionario de la Lengua Española. 22ª edición. Tomo 9, Editorial Mateu Cromo. Artes Gráficas, España, 2001. p. 1408

En la proposición que hacemos, respecto al numeral 211 Bis-2, se destaca, que el bien jurídico protegido, es la información contenida en los sistemas o equipos de informática, que sean propiedad del Estado, en este caso, el Gobierno Federal.

Además de mejorar la redacción, sostenemos que en los cuatro supuestos de la comisión de este delito, se subraye que la conducta, puede ser de acción u omisión y que cuando la misma pretenda modificar, destruir o provocar, que se pierda la información contenida en los sistemas o equipos citados, y que por supuesto, estén protegidos por mecanismos de seguridad, estimamos que la pena privativa de la libertad, debe ser de tres a ocho años de prisión y de seiscientos a mil ochocientos días multa.

Cuando la hipótesis jurídica se refiera a conocer o copiar la información de los sistemas o equipos de informática del Estado, por ser menos grave que la anterior, agregamos como elementos de la propuesta del artículo comentado, que la pena privativa de la libertad sea de dieciocho meses a seis años de prisión y los días multas de trescientos a novecientos.

En el tercer supuesto del ilícito en comento, proponemos que por tratarse de información de seguridad pública del Estado, la pena de prisión sea de doce a treinta años y la multa de mil quinientos a tres mil días de salario mínimo vigente en el Distrito Federal para prevenir y desalentar la comisión de estos delitos.

La última hipótesis de este delito, se agrava, si el sujeto activo del mismo es o hubiera sido servidor o funcionario público, de cualquier nivel, en alguna institución de seguridad pública del Estado, proponemos agregar a las penas anteriores, su destitución e inhabilitación, que puede ser de doce a treinta años, para prohibir el desempeño de cualquier puesto, cargo, comisión pública o un empleo semejante.

Respecto al artículo 211 Bis-3, nuestra principal preocupación, atendiendo a que el sujeto pasivo del delito es el Estado, es imponer penas más severas, en cuanto a la prisión y los días multa.

También se maneja en forma adecuada la expresión gramatical, en virtud de que estamos en presencia de un sujeto, por lo que se debe utilizar el pronombre quien, y no una cosa, que el actual Código Penal Federal, usa una pobre expresión al decir, “al que”.

En las diferentes hipótesis que ordena el precepto citado, hemos puesto especial énfasis, en cuanto a que, por tratarse de causar daños intencionales a bienes propiedad del Estado, cuyo propósito sea perder información, se deben imponer penas de prisión, de seis a veinticuatro años y de mil ochocientos a dos mil setecientos días multa. Proponemos reducir la pena, cuando sólo se copie indebidamente la información, haciendo hincapié en que, en el comentario anterior, se incluye el supuesto de dañar, modificar, destruir o hacer de cualquier manera, que se pierda la información.

Por ello, nuestra propuesta es pena privativa de la libertad, de tres a doce años y de cuatrocientos cincuenta a mil trescientos cincuenta días multa. Los tipos descritos en estas normas, se agravan, cuando se trata específicamente de instituciones de seguridad pública, considerando que la obtención de información de sus equipos o medios de almacenamiento digitales, puede traer graves perjuicios no solo al Estado, sino también a los mexicanos.

Se propone la pena de prisión de doce a treinta años de cárcel y de mil quinientos a tres mil días multa y si fuera el caso de que el sujeto activo de estos delitos, sea o hubiere sido funcionario o servidor público, en instituciones de seguridad pública, se le debe inhabilitar, sustituir y agregar una pena de prisión, de seis a quince años, con lo que el sujeto multimencionado, podría alcanzar de dieciocho a cuarenta y cinco años de cárcel.

Cambiando las hipótesis mencionadas, el artículo 211 Bis-4, regula el ataque que se realice a sistemas financieros, sin especificar, si se trata de instituciones del Estado o privadas.

Al respecto, proponemos para la primera parte de esta reforma, la pena privativa de la libertad de dieciocho meses a doce años y multa de trescientos a ochocientos días, para quienes sin tener autorización, accedan a las instituciones financieras, con el propósito de modificar, destruir o provocar pérdidas de la información, que esté contenida en esos sistemas.

También en el caso de que el sujeto activo del delito, sin estar autorizado, sea capaz de usar medios, para conocer o copiar esa información, haciendo hincapié en que pueden ser instituciones públicas o privadas, la pena privativa de la libertad, será de nueve meses a seis años y de ciento cincuenta a novecientos días multa.

Por la vinculación que hay entre los párrafos séptimo y último del artículo 400 Bis del Código Penal Federal, debe subrayarse que el sistema financiero mexicano, lo integran de acuerdo a nuestra propuesta, los Bancos, las Intermediarias, los Mercados Financieros, las Aseguradoras, Afianzadoras, Casas de Bolsa, Administradoras de Fondos de Inversión, Almacenes Generales de Depósito, Sociedades de Ahorro y Préstamo, Uniones de Crédito, Empresas de Factoraje Financiero, Administradoras de Fondos de Retiro y cualesquiera otras, que realicen funciones semejantes de desarrollo y financiamiento de la economía, con el objetivo de crear instrumentos variados, que le den movilidad a los ahorros y los canalicen a los usos productivos, económicos y el bienestar de la población.

En cuanto al artículo 211 Bis-5, hemos mejorado la redacción de los tres supuestos de la comisión de los delitos informáticos, que en este caso, se refieren al sistema financiero.

Nuestra proposición, es que como estamos hablando de una persona, que trabaja en la institución donde va a perpetrar el delito, es decir, las instituciones del sistema financiero, cualquier situación es más grave, porque el sujeto activo del delito, actúa porque tiene autorización, para ingresar a los sistemas computacionales respectivos y que su conducta, tenga como consecuencia, modificar, destruir o provocar pérdida de la información relevante. Por ello, en este primer caso, proponemos la pena de prisión de dieciocho meses a nuevE años de prisión y multa de trescientos a mil ochocientos días.

Se justifica, según nuestra propuesta, que si el sujeto activo del delito sólo copia la información financiera correspondiente, irá a la cárcel, haciéndose acreedor a una pena de prisión de nueve meses a seis años y una multa de ciento cincuenta a novecientos días.

Para nosotros, es una agravante que debe tomarse en cuenta en este delito, para incrementar en dos terceras partes las penas respectivas, tratándose de que los delincuentes, a la vez, tengan el carácter de funcionarios públicos o empleados de las instituciones financieras, que hayan resentido los efectos de estas acciones.

En el artículo 211 Bis-6, se aclara, que en relación a los dos preceptos anteriores, el concepto instituciones del sistema financiero, son las que se definen en el artículo 400 Bis del Código Penal Federal.

En nuestra propuesta, además de mejorar la redacción del artículo en comento, se enumeran las instituciones que integran el sistema financiero de manera enunciativa y en general, la iniciativa propone, que tratándose de otras instituciones u organismos, que realicen funciones semejantes de desarrollo y financiamiento de la economía, deben incluirse en el sistema financiero.

Analizando lo que podrían calificarse como agravantes, en los delitos informáticos, el artículo 211 Bis-7, ordena, que debe incrementarse hasta en un cincuenta por ciento la pena, si quien obtiene la información, la usa en su provecho o la de un tercero.

Nuestra proposición, es que tanto las penas privativas de la libertad, cuanto los días multa, deben aumentarse no a la mitad, sino en dos terceras partes, si se acredita que los sujetos activos de los delitos informáticos, son parte o pertenecen a cárteles o sociedades de delincuencia organizada.

II. ESTUDIO DEL ARTÍCULO 211 BIS-1 DEL CÓDIGO PENAL FEDERAL Y PROPUESTA DE REFORMAS

Textualmente, este precepto ordena lo siguiente: "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." [45]

A) COMENTARIO

Del texto anterior, hay que subrayar, que sus tres supuestos, no son adecuados para tipificar este delito, considerando que el primero, habla de modificar, destruir o provocar pérdida de información; al respecto, es criticable que ni la penalidad ni la forma en que está redactado, tipifique adecuadamente este delito, señalando una pena de seis meses a dos años de prisión y cien a trescientos días multa; pena y multa insuficientes, porque la comisión de este delito, va en aumento y no ha logrado, entre otros, el artículo citado, de previene esas infracciones, por lo que sería recomendable y así lo proponemos más adelante, que tanto la pena de prisión, cuanto la multa, se incrementaran considerablemente.

El segundo tipo,se relaciona con conocer o copiar información, tampoco es adecuado, porque el legislador no explica, en qué consisten esas conductas e igualmente, la pena de prisión y la multa son tan leves, que no han surtido los efectos, que el legislador mencionó en la Exposición de Motivos correspondiente.

[45] Compilación Penal Federal y del Distrito Federal. Diccionario de Términos y Plazos. Raúl Juárez Carro Editorial, 51ª edición. México, marzo 2013, p. 177.

En el tercer supuesto, no específica la clase de contenidos que estén en sistemas o equipos de informática y que deban estar protegidos por alguno de los múltiples mecanismos de seguridad que existen.

B) CRÍTICA

De manera general, el precepto en comento, tiene una pésima redacción, lo que impide a los sujetos activos y pasivos de este delito, entender con toda claridad, lo que la ley pretende y a los juzgadores, les da demasiadas facilidades para tergiversar la aplicación del texto de la ley, en virtud de que las penas mínimas y máximas son tan distantes, que todo queda al arbitrio del juzgador, lo que obviamente propicia corrupción y pésima administración de justicia, lo recomendable sería, darle a las palabras su verdadero sentido gramatical y sobre todo, el técnico-jurídico, que exige el derecho y específicamente el penal.

Por otro lado, es necesario imponer penas más severas, que prevengan la comisión de los delitos, que a nuestro juicio, es más trascendente el Derecho Penal preventivo, que el sancionador. Igualmente, es necesario definir con toda nitidez, cuál es el bien jurídico protegido, para que en el momento de la comisión del ilícito, se tipifiquen con toda claridad, los cuatro elementos fundamentales de la teoría general del delito.

La cuantificación del daño ocasionado por el sujeto activo del delito, debe tener parámetros y no dejarlo sólo a juicio del Juez, por las razones ya expuestas. Seguramente, que será una aportación trascendente de nuestra parte, lo que podamos agregar, en virtud de que el precepto en análisis, no trae los elementos necesarios y suficientes, para probar la comisión de este delito.

Entre otros instrumentos y personas, tomar en cuenta a los testigos, consultar las bitácoras de cada computadora y considerar que las acciones para la comisión de estos delitos exigen, como requisito indispensable, estar conectadas a Internet, para poder robar la información en cuestión.

Es evidente que se comete un daño e la propiedad de otro y en este caso, hay que considerar si también se tipifica ese delito.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-1

En atención a las consideraciones anteriores y reflexiones correspondientes, nos permitimos someter a la consideración de este Honorable Jurado, nuestra propuesta, para definir el numeral citado.

"A quien por su acción u omisión, dañe o perjudique a una persona jurídica física jurídica o persona jurídica colectiva, al obtener información automática, digital o cibernética, contenida en sistemas o equipos informáticos, protegidos por cualquier mecanismo de seguridad o contraseñas, será castigado con pena de trece meses a cinco años de prisión y quinientos días multa".

III.ESTUDIO DEL ARTÍCULO 211 BIS-2 DEL CÓDIGO PENAL FEDERAL Y PROPUESTA DE REFORMAS

La última reforma publicada en el Diario Oficial al precepto, que vamos a comentar, se realizó el 24 de junio del año 2009, ordenando lo siguiente: "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 informático 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 o inhabilitación de cuatro a diez años para desempeñarse en otro empleo; puesto, cargo o comisión pública".[46]

A) COMENTARIO

El precepto anterior, repite los supuestos del artículo 211 Bis-1, en lo referente a la pérdida de la información por modificación, destrucción o provocación que la ocasione, debiendo poner especial énfasis en que en este caso, lo que la ley protege, son los sistemas o equipos de informática que

[46] Loc. Cit.

pertenezcan al Estado; es decir, al Gobierno Federal; por ello, le ha dado nuevos enfoques a las penas privativas de la libertad y a las multas.

La primera diferencia, es que en este artículo, se elevan la pena de prisión y la multa; el legislador ordena que la primera, sea de uno a cuatro años y la segunda, de doscientos a seiscientos días multa.

Para la comisión del delito, que dé por resultado conocer o copiar la información, en este caso, son seis meses a dos años de prisión y cien a trescientos días multa.

El tercer supuesto, tipifica el delito, al decir que quien conozca, obtenga, copie o utilice información, se hará acreedor a una pena de prisión de cuatro a diez años y de quinientos a mil días multa.

La aplicación del método comparativo, a las hipótesis anteriores, nos da como resultado, saber que el legislador agravó la pena, al incluir al Estado, como el sujeto pasivo que ha resentido las acciones u omisiones del activo y en este caso, desde nuestra perspectiva, consideramos que las sanciones no son las adecuadas.

Una cuarta situación, no contemplada en el precepto anterior, que consiste en que si se dan algunas de las siguientes hipótesis, las penas y la multas serán superiores. No debe perderse de vista, que el Código punitivo federal, de manera general, se refiere al Estado y nosotros pensamos que debe ser más específico, para que la tipificación de las conductas delictivas se den adecuadamente.

El numeral en cuestión, agrega para el caso de las agravantes, que el sujeto activo del delito, sea o haya sido servidor público en una institución de seguridad pública, lo que traerá como consecuencia, su destitución; su

inhabilitación y una pena de cuatro a diez años, impuesta como sanción, para prohibirle desempeñar otro cargo, empleo, puesto o comisión pública.

B) CRÍTICA

La trascendencia de castigar el acceso ilícito a sistemas y equipos de informática, pertenecientes al Estado; a instituciones de seguridad pública o ser o haber sido, funcionario o servidor público, no puede reducirse, como lo hizo el legislador federal penal, a repetir hipótesis de delitos cometidos entre particulares, con el supuesto de este artículo, donde la figura central es el Estado, su organización y la seguridad pública, puede ser tan grave la modificación, la destrucción, la provocación, el conocimiento, la copia, la obtención del conocimiento y su utilización, respecto a las funciones del Estado, de la Nación, del Gobierno Federal y sus dependencias, que este precepto, como lo vamos a proponer a continuación, debe tener medidas que protejan mejor los sistemas informáticos del Gobierno Federal; de la seguridad pública y sancionar severamente a quienes por su calidad de servidores públicos, se hayan aprovechado de esa posición para obtener y utilizar en su propio beneficio, la información citada, que como lo estamos viviendo y presenciando en la actualidad, las acciones delictivas para robar, espiar o tener acceso a información privilegiada, como podrían ser las medidas de seguridad nacional del Estado, deben ser mejor protegidas, podrían llevar a una crisis gubernamental, como está ocurriendo hoy en día, con los descubrimientos de quienes se han apropiado de información privilegiada, particular, de personalidades políticas importantes o afectando naciones, como ocurre con el “Obamagate”.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-2

En atención a las consideraciones anteriores y reflexiones correspondientes, nos permitimos someter a la consideración de este Honorable Jurado, nuestra propuesta para definir el numeral citado.

“A quien sin tener autorización, por su acción u omisión, modifique, destruya y/o provoque la pérdida de información contenida en sistemas o equipos de informática del Estado, que estén protegidos por algún mecanismo de seguridad, se le impondrán de tres a ocho años de prisión y seiscientos a mil ochocientos días multa.

A quien sin tener autorización, por acciones u omisiones, conozca y/o copie información, contenida en sistemas o equipos de informática del Estado, que estén protegidos por algún mecanismo de seguridad, se le impondrán dieciocho meses a seis años de prisión y trescientos a novecientos días multa.

A quien sin tener autorización, conozca, obtenga, copie y/o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de cualquier institución de seguridad pública del Estado, protegido por algún medio de seguridad, se le impondrá pena de doce a treinta años de prisión y multa de mil quinientos a tres mil días de salario mínimo general vigente en el Distrito Federal.

Si el sujeto activo de los delitos, tipificados en los párrafos anteriores, es o hubiera sido servidor o funcionario público de cualquier nivel, en una institución de seguridad pública del Estado, se le impondrán además de las penas anteriores, la destitución o inhabilitación de doce a treinta años para desempeñar cualquier puesto, cargo, comisión pública o empleo semejante.”

IV. ESTUDIO DEL ARTÍCULO 211 BIS-3 DEL CÓDIGO PENAL FEDERAL Y PROPUESTA DE REFORMAS

La última reforma de este precepto, se realizó el 24 de julio del año 2009; el texto actual, involucra como sujeto pasivo del delito al Estado; diferencia las hipótesis en cuanto a la autorización que tenga el sujeto activo del delito, para acceder al sistema computarizado.

También se protegen las instituciones de seguridad pública, con penas más severas de prisión y de multa. Incluso, para el supuesto de ser o haber sido, servidor o funcionario público en alguna institución de seguridad pública, se establece una agravante.

El nuevo texto del precepto citado, ordena lo siguiente: “Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la

pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión público". [47]

A) COMENTARIO

Del texto anterior, debe destacarse que el sujeto activo del delito, actúe con autorización, para tener acceso a los sistemas computarizados; diferencia que en la primera hipótesis, su actuación sólo tenga como propósito, modificar, destruir o provocar pérdidas de información, que sea propia del Estado y la pena que en suma es de diez años de prisión; en un momento dado, permitiría al presunto delincuente, enfrentar el juicio en libertad, es una de las hipótesis que a nuestro juicio debe modificarse, incrementando la sanción, supuesto al que nos referiremos al hacer nuestra propuesta, que forma parte de la tesis o posición ideológica original de esta investigación.

El segundo caso, también habla de que el sujeto activo del delito, esté autorizado por el Estado y que se concrete al acceder a los sistemas y equipo de informática de aquél, a copiar la información y no modificarla ni destruirla, por ello, la pena de prisión, es equivalente a la mitad de la anterior, es decir, uno a cuatro años.

En la tercera hipótesis, se regresa a los supuestos de copiar o utilizar la información correspondiente, por un sujeto autorizado por el propio Estado y que su pretensión sea acceder a los sistemas, equipos o medios de almacenamientos informáticos, cuya materia sea seguridad pública, en este caso, el legislador ha considerado que se le debe imponer una pena de prisión de cuatro a diez años, lo que impediría que en su caso, el sujeto activo del delito, enfrentara la acusación que se hiciere en su contra en libertad; en virtud de que la mínima son cuatro y diez la máxima de años de prisión.

A las hipótesis anteriores, hay que agregar y es importante destacar lo que dice la ley, que se estará en presencia de agravantes, si el sujeto activo del

[47] Compilación Penal Federal y del D. F. Ob. Cit. p. 177.

delito,es o fue servidor o funcionario público en instituciones de seguridad pública. En este caso, el Código ya no diferencia, si hay o no autorización y tampoco, si se modifica, destruye, se provoca su pérdida, se copia o se utiliza, por parte del presunto delincuente, sino que la ley, suma a las penas anteriores, una mitad más de pena de prisión, que en relación al supuesto anterior, sería incrementar de dos a cinco años, lo que nos daría seis años como pena mínima y quince, como máxima; agregando que habrá destitución del puesto, cargo o comisión pública.

B) CRÍTICA

Consideramos que el legislador penal federal, a pesar de incluir las agravantes, por la comisión de los delitos multicitados, debería crear hipótesis más genéricas, que se puedan tipificar como delitos, si el sujeto activo de los mismos, se ubica en cualesquiera de las de hacer mal uso de la información, no sólo en general del Estado o en instituciones de seguridad pública, sino de cualquier otro caso, en que el sujeto pasivo del delito sea el Estado y cualesquiera de sus instituciones y no sólo de seguridad pública; verbigracia podría ser de la Secretaría de Hacienda; del Instituto Mexicano del Seguro Social o de cualquier otra institución, que al ser despojada de su información, contenida en sus sistemas o equipos de informática, podrán causarle daños graves, que además, podrían ser irreparables.

En los cuatro casos específicos, del precepto en análisis, y desde nuestra perspectiva, dada la gravedad de los mismos, las penas privativas de la libertad, deben ser más severas e involucrar supuestos en general y no específicos, como los que actualmente están legislados, que se refieren al Estado y a las instituciones de seguridad pública; enseguida, desarrollaremos nuestra propuesta concreta, proponiendo un nuevo texto para este artículo.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-3

“A quien teniendo autorización para ingresar a los sistemas, equipos de informática y otros semejantes, propiedad del Estado, con la intención de dañar,

modificar, destruir, provocar o de cualquier manera que su conducta origine perder la información, que los sistemas contienen, se le impondrá una pena de prisión de seis a veinticuatro años y mil ochocientos a dos mil setecientos días multa.

En el mismo supuesto del párrafo anterior, quien copie indebidamente la información que contengan aquéllos, se le impondrá una pena de prisión de tres a doce años y de cuatrocientos cincuenta a mil trescientos cincuenta días multa.

A quien teniendo autorización, acceda a los sistemas, equipos o medios de almacenamiento informáticos en instituciones de seguridad pública e indebidamente obtenga aquélla, la copie o la utilice, se le impondrá la pena de prisión de doce a treinta años de cárcel y de mil quinientos a tres mil días multa.

Al sujeto activo del delito de las normas anteriores, se le impondrán penas más severas, si es o hubiera sido funcionario o servidor público en seguridad pública; además de la inhabilitación y destitución que se le haga, en cuanto a su empleo, puesto, cargo o comisión pública, se le agregará una mitad más de la pena de prisión establecida en el supuesto anterior; es decir, de seis a quince años, lo que podría sumar dieciocho a cuarenta y cinco años de cárcel”.

V. ESTUDIO DEL ARTÍCULO 211 BIS-4 DEL CÓDIGO PENAL FEDERAL Y PROPUESTA DE REFORMAS

A diferencia de los preceptos anteriores, éste se refiere a las hipótesis de atacar los sistemas financieros, sin especificar si se trata de instituciones del Estado o privadas. Es un precepto que no se modificó en el año 2009, como ocurrió con los anteriores.

También maneja las hipótesis de modificar, destruir o provocar con las acciones del sujeto activo, la pérdida de información que esté en los sistemas o equipos de informática, que sean parte de las instituciones del sistema financiero y la segunda, se diferencia de la anterior, en que en este caso, careciendo de la autorización de quien debe darla, el sujeto activo del delito conozca o copie la información de sistemas financieros; para tener con más claridad y sobretodo, emitir nuestros puntos de vista, críticas y propuestas, transcribiremos a continuación el texto del numeral citado al rubro, que ordena: “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". [48]

A) COMENTARIO

En los tipos descritos, ambos se refieren a que el sujeto activo del delito, modifique, destruya o provoque pérdida de la información, que contengan sistemas o equipos informáticos, que pertenezcan a las instituciones que formen parte del sistema financiero, exigiendo además, que esté protegido por algún

[48]Compilación Penal Federal y del D. F. Ob. Cit. p. 177.

mecanismo de seguridad, se propone una pena de seis meses a cuatro años de prisión y cien a seiscientos días multa, lo que a nuestro juicio, debería incrementarse para este caso y así, establecer que la pena mínima de prisión, sea dieciocho meses y la máxima doce años, con el propósito de que los sujetos activos de este delito, enfrenten los procedimientos privados de la libertad y consideramos también, que en cuanto a la multa, la mínima debe ser trescientos días y las máxima mil ochocientos.

La otra hipótesis, en la que el sujeto activo del delito, sólo conozca o copie la información que contengan las computadoras o los equipos correspondientes, que pertenezcan a las instituciones del sistema financiero, a que la pena privativa de la libertad, se establezca de nueve meses a seis años de prisión y la multa elevarla también de ciento cincuenta a novecientos días.

B) CRÍTICA

El precepto transcrito, no fue modificado como los otros artículos en el año 2009, sin que el legislador hubiere expresado alguna opinión, para no realizar ese trabajo. Comete el error de no aclarar, si se trata de instituciones del Estado o privadas y tampoco diferencia los supuestos en los que en uno se habla de autorización y en otro, de copiar o conocer la información que se obtendrá del sistema de computadoras respectivo.

Asimismo, es criticable que el supuesto de este delito, sólo se refiera al sistema financiero, sin aclarar, si el mismo es público o privado. En atención a estas observaciones, citamos a continuación, otros supuestos jurídicos, para que queden bien tipificados los delitos y los bienes jurídicos protegidos por esas normas, proponiendo el texto que a continuación mencionamos.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-4

“A quien no esté autorizado para acceder a las instituciones que pertenezcan al sistema financiero, y con su conducta de hacer o no hacer, logre

modificar, destruir o provocar pérdidas de la información que esté contenida dentro de los sistemas o equipos de informática del sistema financiero y sus instituciones, que además, se hayan establecido mecanismos de seguridad para su protección, se le impondrán penas privativas de la libertad de dieciocho meses a doce años y multas de trescientos a ochocientos días.

Para el caso de que el sujeto activo del delito, igualmente sin autorización, utilice los medios que le permitan conocer o copiar la información contenida en sistemas o equipos de informática de las instituciones públicas o privadas, que formen parte del sistema financiero y además, que existan mecanismos protectores de esa seguridad, se hará acreedor a la pena privativa de la libertad de nueve meses a seis años y de ciento cincuenta a novecientos días multa.

El sistema financiero mexicano, está integrado por todas las instituciones de crédito públicas o privadas, que realicen operaciones de financiamiento, sea cual fuere su giro, así como las casas de bolsa, de cambio, intermediarias o cualquiera otra semejante”.

VI. ESTUDIO DEL ARTÍCULO 211 BIS-5 DEL CÓDIGO PENAL FEDERAL

Este precepto, a diferencia del anterior, maneja tres supuestos, respecto al sistema financiero; en el primero, habla de que el sujeto activo, tenga autorización y que con ésta, su acción modifique, destruya o provoque pérdidas de la información; en el segundo, repite la hipótesis de estar autorizado, y que la conducta sea solo de copiar la información y la tercera, incluye agravantes, en virtud de que las penas se van a incrementar, si quien estando autorizado para ingresar al sistema financiero, sea funcionario público o empleado de esas instituciones financieras; que en este caso, damos por reproducido aquí el comentario hecho en el artículo precedente, en relación al precepto 400 Bis del Código Penal Federal, que describe, qué instituciones integran el sistema financiero.

El texto del precepto en análisis, es el siguiente: “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”. [49]

[49] Compilación Penal Federal y del D. F. Ob. Cit. pp. 177 y 178.

A) COMENTARIO

Dada la trascendencia de los delitos cometidos contra las instituciones integrantes del sistema financiero y los graves efectos que se pueden producir, proponemos que en el primer supuesto, del artículo supracitado, que tiene una penalidad de seis meses a cuatro años de prisión y de cien a seiscientos días multa; se incremente el primero, a dieciocho meses como mínimo y doce años como máximo, para evitar que los sujetos activos de este delito, enfrenten su proceso en libertad; porque de alguna manera, una pena mayor, también tendrá carácter preventivo, al impedir que los delincuentes puedan gozar de plena libertad, a pesar de los delitos cometidos y respecto a la sanción económica, nuestra propuesta, es elevar la mínima a trescientos y la máxima a mil ochocientos días multa.

Para el caso del sujeto activo del delito comentado, que copie la información del sistema financiero, estando autorizado para ello, la sanción es mínima, en virtud de que se imponen tres meses a dos años de prisión, que sigue siendo baja la pena, ya que cuando se trate de un funcionario público o empleado de las propias instituciones financieras, se incrementará en una mitad la pena señalada, para quedar la mínima en cuatro meses y medio y la máxima en tres años y de cincuenta a trescientos días multa.

Nuestra propuesta para este delito, es incrementar la pena de nueve meses a seis años y con el supuesto de las agravantes, aquélla se elevaría a trece meses y medio como mínimo y la máxima a nueve años de prisión; por lo que hace a los días multa, se incrementarían de ciento cincuenta a novecientos días y con la agravante, de doscientos veinticinco a mil trescientos cincuenta días.

B) CRÍTICA

Es criticable el precepto citado, porque igual que los anteriores, carece de técnica legislativa adecuada; no define con claridad los bienes jurídicos protegidos

por la norma y los diferentes tipos, son confusos y difícilmente podrán encuadrarlo que es la tipicidad propiamente dicha.

Las calificativas que hace el legislador, cuando se refiere al sistema financiero y que los sujetos activos del delito, estén autorizados, nos parece ambiguo, como ya lo expresamos, losverbos modificar, destruir, provocar o copiar, tienen connotaciones tan diferentes, como determinar la penalidad de cada uno de los delitos.

También debe ser objeto de análisis, lo que en técnica jurídica, se conoce como agravantes, porque en este supuesto, le dan el mismo nivel a los funcionarios públicos, que a los empleados de esas instituciones y es evidente, que tienen accesos y funciones diferentes, lo que deberá tener efectos jurídicos en la calificación de las penas agravadas.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-5

"A quien trabaje en instituciones del sistema financiero, y esté autorizado para ingresar a los sistemas computacionales respectivos, modifique, destruya o provoque, que por sus conductas se pierda la información relevante, se le aplicarán de dieciocho meses a nueve años de prisión y multa de trescientos a mil ochocientos días.

En el supuesto anterior, si el sujeto activo del delito, solo copia la información financiera correspondiente, se hará acreedor a una pena de nueve meses a seis años de prisión y ciento cincuenta a novecientos días multa.

Las penas mencionadas, se incrementarán en dos terceras partes, si los responsables son funcionarios públicos o empleados de las instituciones financieras, que hayan resentido las acciones de los responsables".

VII. ESTUDIO DEL ARTÍCULO 211 BIS-6 DEL CÓDIGO PENAL FEDERAL

El texto de este precepto, que además, tiene una pésima redacción, aclara los supuestos que en el propio numeral se mencionan, especificando cómo deben definirse y entenderse las instituciones que forman parte del sistema financiero mexicano y alude al 400 Bis del mismo ordenamiento. Este artículo ordena lo siguiente: “Para los efectos de los artículos 211 Bis-4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código". [50]

A) COMENTARIO

La intención del legislador, ha sido que no quede duda, ni que pueda haber alguna interpretación errónea, de lo que debe entenderse por institución y en segundo lugar, que ésta o éstas, forman parte del sistema financiero.

B) CRÍTICA

Desde nuestro punto de vista y procurando buscar las expresiones más claras, es criticable que el legislador, use las palabras, “se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código”; en lugar de buscar el género próximo y la diferencia específica, para definir, qué significan las palabras instituciones y sistema financiero.

Si bien es cierto, que remite al numeral 400 Bis y en éste, se enumeran casuísticamente las que se consideran como tales, no se puede admitir, que siendo el precepto citado tan importante, el legislador no sea capaz, de legislar adecuadamente esas expresiones, que son esencia de las reformas que venimos comentando, por ello, a continuación, proponemos una nueva redacción del numeral analizado, que a la vez, nos llevará a ser lo propio con el artículo 400 Bis, todos del Código Penal Federal.

[50] Compilación Penal Federal y del D. F. Ob. Cit. p. 178.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-6

“Para los efectos de los artículos 211 Bis-4 y 211 Bis-5, de este ordenamiento, las instituciones que integran el sistema financiero, son los bancos, intermediarias, mercados financieros, aseguradoras, afianzadoras, casas de bolsa, administradoras de fondos de inversión, almacenes generales de depósito, sociedades de ahorro y préstamo, uniones de crédito, empresas de factoraje financiero, administradoras de fondos de retiro y cualesquiera otras que realicen funciones semejantes de desarrollo y financiamiento de la economía, para crear una gran variedad de instrumentos para mover los ahorros hacia los usos productivos, económicos y el bienestar de la población”.

VIII. ESTUDIO DEL ARTÍCULO 211 BIS-7 DEL CÓDIGO PENAL FEDERAL

El texto de este delito, está expresado en los siguientes términos: “Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno”. [51]

A) COMENTARIO

Los supuestos jurídicos de este precepto, son tan absurdos, que es necesario proponer una nueva redacción. Es ilógico pensar, que quienes se ubiquen en cualesquiera de las hipótesis, como sujetos activos de estos delitos, vinculados con las instituciones del sistema financiero mexicano, no lo hagan para beneficiarse o en segunda instancia, para que resulte a favor de terceras personas; por ello, decimos que las acciones delictivas en estos ilícitos, siempre tendrán como fin primero o último, beneficiar personalmente a quien comete el delito o a un tercero.

Dadas las graves consecuencias de estos delitos y sus efectos en el patrimonio de las personas jurídicas físicas, de las jurídicas colectivas o del propio Estado, como lo hemos propuesto en los artículos, objeto de esta investigación, las penas deben incrementarse en dos terceras partes, de las que se hayan establecido, dependiendo de los supuestos de los delitos cometidos.

B) CRÍTICA

Es criticable que el legislador penal federal, haya tenido como única preocupación, que las penas en la comisión de estos delitos, se pudieran incrementar hasta en la mitad, lo que significa que pudiera ser menos, si el sujeto activo del delito, se hubiera aprovechado personalmente o de un tercero; lo que resulta absurdo, porque si el bien jurídico protegido es esa información, al violar éste, el presunto delincuente o sujeto activo del delito, no tendrá más remedio que beneficiarse o vender esa información, lo que daría dividendos o ventajas a un tercero; es grave que el precepto deje la opción jurídica, acudiendo a la

[51] Compilación Penal Federal y del D. F. Ob. Cit. p. 178.

presunción “iuris tantum” –salvo prueba en contrario- de que durante el proceso penal, el presunto responsable, demuestre que sustrajo la información, pero que ni él ni un tercero, se beneficiaron; lo que resulta infantil e irrisorio y debemos insistir en la crítica, en cuanto a que el legislador penal federal, realizó estas reformas improvisadamente y en las rodillas.

C) PROPUESTA DEL NUEVO TEXTO DEL ARTÍCULO 211 BIS-7

Las penas privativas de la libertad, previstas en este Capítulo y el número de días multa, se incrementarán en dos terceras partes, de las sanciones reguladas en cada uno de los artículos que integran este Capítulo, si se acreditara que los sujetos activos de estos delitos, son parte o pertenecen a sociedades de delincuencia organizada.

CAPÍTULO CUARTO
LOS BIENES JURÍDICOS PROTEGIDOS EN LOS DELITOS INFORMÁTICOS

I. NECESIDAD DE PROTECCIÓN DEL ESTADO A LOS EQUIPOS INFORMÁTICOS Y LOS DATOS QUE CONTENGAN

Uno de los más graves problemas, a que se enfrentan los investigadores de Derecho Penal y al mismo tiempo, los expertos en el manejo de información digital, de acuerdo a la realidad que estamos viviendo en pleno siglo XXI, es aceptar que la globalización y el avance de la cibernética, han creado nuevos satisfactores, para darle contenido y resolver las necesidades que el desarrollo tecnológico ha traído consigo.

Siguiendo la tradición de los diferentes Códigos Penales, que a lo largo de la historia, se han puesto en vigor en diferentes países, incluido México, el común denominador en ellos, ha sido que todos los delitos, tienen como requisito, sine qua non, definir con toda claridad, el bien jurídico protegido de cada uno de ellos, porque esta característica permite conceptualizarlos y adaptarlos a la realidad que en cada país exige que se legislen los nuevos delitos que van surgiendo, con el desarrollo humano, cultural, social, familiar, económico, científico y en el caso concreto de esta investigación, el de la información digital.

Si vamos de lo simple a lo complejo, citaríamos como ejemplos clásicos de bienes jurídicos protegidos, el del homicidio, que corresponde a la vida; el de lesiones, a la integridad física; el de robo o fraude, al patrimonio; el de violación, a la libertad sexual y hoy, en nuestro siglo, traeríamos a colación, el tema de los delitos informáticos, que según los estudios que hemos realizado, no hay acuerdos sobre cuáles son los bienes jurídicos protegidos que deben ser tutelados por la ley en la materia mencionada, porque hay quienes, sin entender qué significa la expresión bien jurídico protegido, hacen propuestas y en la materia digital, hay una gran proliferación de ellas, de pretender, que el bien jurídico

protegido o en plural, los bienes jurídicos protegidos, en los delitos informáticos son plurales, son múltiples, son diversos, lo que desde nuestra perspectiva, le quitan su esencia a la tipificación del delito informático, ya que como lo dijimos antes, para nosotros, este delito se define, como toda acción u omisión típica, antijurídica y culpable, realizada por una persona jurídica física, desde cualquier lugar, para sustraer, destruir, modificar, utilizar o copiar, información digital, utilizando cualquier equipo informático, computadora, internet o alguno semejante, para cometer un delito contra la propiedad intelectual, sistemas de seguridad, sistemas financieros públicos o privados o actividades semejantes.

El bien jurídico protegido, debe ser la información; pretender que se tutela el patrimonio, es desconocer la esencia del robo, que consiste en el apoderamiento de una cosa ajena mueble, sin consentimiento de la persona que puede disponer de ella conforme a la ley.

Varios tratadistas, han derivado del delito informático, que como lo dijimos y ahora lo reiteramos, la esencia de su bien jurídico protegido, debe ser la información, algunos agregan la pornografía infantil; otros el fraude cibernético; hay quienes llevan este delito a la divulgación de secretos, vida privada, intervención de comunicaciones telefónicas, perdiendo todos ellos, el rumbo, que debe ser esencia del delito informático en cuanto a ese o esos bienes jurídicos protegidos.

Se podría argumentar, que quien penetra en una computadora y dispone de la información, si materialmente se apoderara de ella, efectivamente cometería el delito de robo; pero debe diferenciarse claramente, que para tipificar el delito informático, esencia de nuestra tesis, debe quedar claro y referirse a que es la información, la que contiene esa computadora o ese sistema digital, la que está protegida; incluso, el valor económico que se le pretendiera dar a esa información, podría ser una causa agravante del delito, pero que no sería elemento fundamental para su tipificación primaria.

La razón de ser del bien jurídico protegido en el delito informático, es impedir que alguien se apodere de esa información, que tiene como características una confidencialidad, una integridad y que en este caso, el Derecho Penal debe ser capaz de crear la norma que la proteja.

Es fundamental, que el jurista valore los alcances de la conducta del sujeto activo del delito, en este supuesto del informático, porque eso permitirá, que la acción u omisión realizada por esta persona, reciba la sanción adecuada a lo que ha realizado.

Es indiscutible, que el nuevo desarrollo de nuestra sociedad, exige la actualización de las leyes penales y en el caso concreto de los tipos jurídicos, para que siguiendo las técnicas legislativas más adecuadas, se puedan crear las normas propias, que en el siglo XXI, den respuesta, como decíamos, a esos nuevos satisfactores, creados, verbigracia para mejorar la comunicación entre personas jurídicas físicas y personas jurídicas colectivas y ahí el Derecho Penal, debe estar a la vanguardia, no a la retaguardia de la prevención, en cuanto a que nuevos hechos ilícitos, que se conviertan en delitos, puedan ser proyectados al futuro, para mejor proteger a la sociedad.

Educar a las nuevas generaciones de estudiantes de Derecho Penal específicamente y de manera general, a quienes aspiran a convertirse en licenciados en Derecho, es tan trascendente, como lo es el objeto de la tesis de nuestra tesis, la posición ideológica que sostenemos en esta investigación, que consiste en que una vez hecha la revisión de la reforma del 17 de mayo de 1999, en relación al acceso ilícito a sistemas y equipos de informática, estamos proponiendo un proyecto de reformas que incluyen del Código Penal Federal, los artículos 211 Bis, 1, 2, 3, 4, 5, 6, 7 y el séptimo y último párrafo del 400 Bis.

Nuestra propuesta, en relación al bien jurídico protegido, en el delito informático, se refiere a la información. Este concepto es esencial, para que no

haya desviaciones ni dudas, en cuanto a querer incluir en este supuesto jurídico, los bienes jurídicos protegidos de delitos colaterales, vinculados a la información digital, pero que no son esencia de ésta, por ejemplo, el robo, ya expresamos de éste, una opinión y seguimos sosteniendo, que la información contenida en una computadora, no es un bien mueble ni tampoco es una cosa.

Si bien es cierto, que hay una afectación patrimonial, en la protección de la información, ésta no encuadra en el concepto de patrimonio, entendido como un conjunto de bienes, derechos, obligaciones y cargas, valuables en dinero y susceptibles de apropiación económica, porque quien sustrae la información de una computadora, no puede precisar, cuál es el valor en dinero de la misma, situación que se tendría que dar como consecuencia de la comisión de ese delito, cuando el Juez Penal emitiera una resolución en ese sentido.

Ratificamos nuestra postura personal, en cuanto a que el bien jurídico protegido, así expresado, en particular, es la información digital contenida en una computadora.

Rechazamos que esta expresión, tenga un sentido plural, porque se perdería la esencia de este delito, si aceptáramos que son varios los bienes jurídicos protegidos, como ha ocurrido en algunas legislaciones a nivel mundial, que incluyen delitos contra el honor, el patrimonio, la vida privada, la confidencialidad, la pornografía infantil, la pederastia, el espionaje en sus diferentes expresiones, que puede ser político, industrial, económico o de índole diversa, porque debemos centrar nuestra atención en la trascendencia de que se proteja la información, sea cual fuere la especie o género de ésta, para que quede bien tipificado el delito, cuando alguien lo consuma o incluso se ubique en alguna de las fases del iter criminis, en cuanto a la tentativa inacabada, acabada y el delito imposible, en los delitos informáticos.

C O N C L U S I O N E S

PRIMERA.- Los antecedentes históricos de los delitos informáticos, que analicé a la luz de diversos métodos científicos y de investigación, me han permitido evaluar a nivel internacional, cuál es la situación de México, en cuanto a su forma de legislar y sancionar los delitos cometidos por revelación de secretos y acceso ilícito a sistemas y equipos de informática.

SEGUNDA.- En mi propuesta de reforma, la información extranjera de estos delitos, ha sido básica para saber cuál es el nivel y el desarrollo que las leyes mexicanas de la materia, tienen al respecto y debemos aceptar, que estamos desfasados, atrasados y que las normas del Código Penal Federal, vinculadas a la comisión de estos delitos, son anacrónicas y van a la saga del avance extraordinario y positivo que el mundo de la información digital, desarrolla día tras día.

TERCERA.- En el capítulo segundo de esta tesis, analizo la Exposición de Motivos del Título Noveno del Libro Segundo del Código Penal Federal, subrayando que desde el 17 de mayo de 1999, en el Diario Oficial de la Federación, se creó el Título antes mencionado en los artículos 211 Bis-1 al Bis-7. En esta información, citamos lo que diversos organismos internacionales han hecho en la materia, por ejemplo, la Organización de las Naciones Unidas, la de la Cooperación y Desarrollo Económicos, la de la Unión Europea, el Consejo de Europa y la Organización de los Estados Americanos.

CUARTA.- En cuanto al impacto de los ciberdelitos, en el ámbito nacional e internacional, las estadísticas afirman que cerca del 65% de adultos en el mundo, han sido víctimas de algún tipo de delito informático, tales como estafas on line, ataques de phishing, actividades de piratas informáticos en perfiles de redes sociales y fraudes con tarjeta de crédito; en cuanto a los sujetos activos de estos

delitos, se ha identificado que el 56% de ellos, son delincuentes anónimos y un 21%, pertenecen a grupos organizados.

QUINTA.- En la iniciativa comentada, se han propuesto adhesiones y reformas al Código Penal, en cuanto a los artículos 139, 178 Bis y los preceptos 211 Bis-2,Bis 3 y Bis-7. El legislador ha ido más allá y propone agregar, siempre en relación a la interceptación ilícita de datos informáticos, los artículos 211 Bis-8, Bis-9, Bis-10, Bis-11, Bis-12, Bis-13 y Bis-14, y define como datos informáticos, toda representación de hechos, actos, información o conceptos expresados de cualquier forma, que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema de informática, ejecute una función, extendiendo la imputación a personas morales en la comisión de delitos informáticos.

SEXTA.- En este mismo capítulo, proponemos el análisis de diversas definiciones y conceptos de los delitos informáticos. Citamos autores nacionales e internacionales de reconocido prestigio, entre los que destacan Gabriel Andrés Cámpoli, Ivonne Valeria Muñoz Torres, Julio Téllez Valdés, Carlos Sarzana y Jesús Antonio Molina Salgado; también debemos agregar, entre los mexicanos distinguidos en esta materia, a María de la Luz Lima Malvido, a Alexander Díaz García, a Orlando Solano Bárcenas, a Alicia Raquel Lilli y a María Amalia Massa.

SÉPTIMA.- En el capítulo tercero de esta investigación, proponemos un proyecto de reformas al Código Penal Federal mexicano, en los delitos cometidos por revelación de secretos y acceso ilícito a sistemas y equipos de informática. Analizando, comentando y proponiendo nuevos textos, del artículo 211 Bis-1 al Bis-7, todos del Código Penal Federal. En este capítulo, que a mi juicio es la esencia de esta tesis, he elaborado la Exposición de Motivos de las reformas y en forma metódica y sistemática, analizo cada artículo y expreso mi aportación.

OCTAVA.- En el capítulo cuarto, desarrollo el estudio de los bienes jurídicos protegidos en los delitos informáticos, donde afirmo que uno de los más graves

problemas, a que se enfrentan los investigadores de Derecho Penal y al mismo tiempo, los expertos en el manejo de información digital, de acuerdo a la realidad que estamos viviendo en pleno siglo XXI, es aceptar y dar las respuestas adecuadas, que la globalización y el avance de la cibernética, han creado nuevos satisfactores, para darle contenido y resolver las necesidades que el desarrollo tecnológico, ha traído consigo.

P R O P U E S T A

CÓDIGO PENAL FEDERAL **TÍTULO NOVENO** **Revelación de secretos y acceso ilícito a sistemas y equipos de informática**	
Capítulo II **Acceso ilícito a sistemas y equipos de informática** **(Texto Vigente)**	**Capítulo II** **Acceso ilícito a sistemas y equipos de informática** **(Texto Propuesto)**
Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. 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 1**.- A quien por su **acción, dañe o perjudique a una persona jurídica física jurídica o persona jurídica colectiva**, **al obtener información automática, digital o cibernética, contenida en sistemas** o equipos informáticos, protegidos por cualquier mecanismo de seguridad **o contraseñas**, será castigado con pena **de trece meses a cinco años de prisión y quinientos 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	**Artículo 211 bis 2**.- A quien sin tener autorización, **por su acción u omisión**, modifique, destruya y/o provoque la pérdida de información contenida en sistemas o equipos de informática del Estado, que estén protegidos por un

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.	algún mecanismo de seguridad, se le impondrán de **tres a ocho años de prisión y seiscientos a mil ochocientos días multa.** A quien sin tener autorización, **por acciones u omisiones** conozca **y/o** copie información, contenida en sistemas o equipos de informática del Estado, **que estén** protegidos por algún mecanismo de seguridad se le impondrán **dieciocho meses a seis años de prisión y trescientos a novecientos días multa.** A quien sin autorización, conozca, obtenga, copie **y/o** utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de **cualquier institución** de seguridad pública del Estado, protegido por algún medio de seguridad, se le impondrá **pena doce a treinta años de prisión y multa de mil quinientos a tres mil días de salario mínimo general vigente en el Distrito Federal.** Si el **sujeto activo de los delitos, tipificados en los párrafos anteriores**, es o hubiera sido servidor o funcionario público de cualquier nivel, en una institución pública del Estado, se le impondrán a demás de las penas anteriores la destitución o inhabilitación **de doce a treinta años** para desempeñar cualquier puesto, cargo, comisión público o **empleo semejante**.
Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y	**Artículo 211 bis 3**.-A quien **teniendo autorización para ingresar a los**

equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.	**sistemas,** equipos de informática y **otros semejantes, propiedad** del Estado, **con la intención de dañar, modificar, destruir, provocar o de cualquier manera que su conducta origine perder la información, que los sistemas contienen, se le impondrá una pena de prisión de seis a veinticuatro años y mil ochocientos a dos mil setecientos días multa.** **En el mismo supuesto del párrafo anterior, quien copie indebidamente la información que contengan aquellos, se le impondrá una pena de prisión de tres a doce años y de cuatrocientos cincuenta a mil trescientos cincuenta días multa.** A quien **teniendo autorización, acceda** a los sistemas, equipos o **medios de almacenamiento informáticos en instituciones de seguridad pública e indebidamente obtenga aquélla, la copie o la utilice, se le impondrá la pena de prisión de doce a treinta años de cárcel y de mil quinientos a tres mil días multa.**
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A	Al **sujeto activo del delito** de las normas anteriores, se le impondrán penas más severas, si es o hubiera sido funcionario o servidor público en seguridad pública; **además de inhabilitación y destitución que se le haga, en cuanto a su empleo, puesto, cargo o comisión pública, se le agregará la mitad más de la pena de prisión establecida en el supuesto anterior; es decir, de seis a quince**

quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.	**años, lo que podría sumar dieciocho a cuarenta y cinco años de cárcel.**
Artículo 211 bis 4.- Al que sin autorización modifique, destruya o	**Artículo 211 bis 4**.- A **quien no esté autorizado para acceder a las**

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.	**instituciones que pertenezcan al sistema financiero, y con su conducta de hacer o no hacer, logre** modificar, destruir o provocar la pérdidas de la información **que esté contenida dentro de los sistemas** o equipos de informática del sistema financiero y sus instituciones, que además, se hayan establecido mecanismos de seguridad para su protección, **se le impondrán penas privativas de la libertad de dieciocho meses a doce a doce años y multa de trescientos a ochocientos días**. **Para el caso de que el sujeto activo del delito, igualmente** sin autorización, utilice los medios que le permitan conocer o copiar la información contenida en sistemas o equipos de informática **de las instituciones públicas o privadas, que formen parte del sistema financiero y además, que existan mecanismos protectores de esa seguridad, se hará acreedor a la pena privativa de la libertad de nueve meses a seis años y de ciento cincuenta a novecientos días multa.** **El sistema financiero mexicano, está integrado por todas las instituciones de crédito públicas o privadas, que realicen operaciones de financiamiento, sea cual fuere su giro, así como las casas de bolsa, de cambio, intermediarias o cualquier otra semejante.**
Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las	**Artículo 211 bis 5.- A quien trabaje en instituciones del sistema financiero, y esté autorizado para**

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.	**ingresar a los sistemas computacionales respectivos, modifique, destruya o provoque, que por sus conductas se pierda la información relévate, se le aplicarán de dieciocho meses a nueve años de prisión y multa de trescientos a mil ochocientos días.** **En el supuesto anterior, si el sujeto activo de delito, solo copia la información financiera correspondiente, se hará acreedor a una pena de nueve meses a seis años de prisión y ciento cincuenta a novecientos días multa**. Las penas mencionadas, se incrementarán **en dos terceras partes**, **si los responsables** son funcionarios públicos o empleados de las instituciones financieras, que hayan resentido las acciones de los responsables.
Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.	**Artículo 211 bis 6.-** Para los efectos de los artículos 211 Bis-4 y 211 Bis-5, de este ordenamiento, **las instituciones que integran el sistema financiero, son los bancos, intermediarias, mercados financieros, aseguradoras, afianzadoras, casas de bolsa, administradoras de fondos de inversión, almacenes generales de depósito, sociedades de ahorro y préstamo, uniones de crédito, empresas de factoraje financiero, administradoras de fondos de retiro**

	y cualesquiera otras que realicen funciones semejantes de desarrollo y financiamiento de la economía, para crear una gran variedad de instrumentos para mover los ahorros hacia los usos productivos, económicos y el bienestar de la población.
Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.	**Artículo 211 bis 7**.- Las penas privativas de la libertad previstas en este **Capítulo y el número de días multa, se incrementarán en dos terceras partes, de las sanciones reguladas en cada uno de los artículos que integran este Capítulo, si se acreditara que los sujetos activos de estos delitos, son parte o pertenecen a las sociedades de delincuencia organizada.**

B I B L I O G R A F Í A

CÁMPOLI, Gabriel Andrés, Delitos Informáticos en la Legislación Mexicana, 1ª reimpresión, Ediciones Corunda e Instituto Nacional de Ciencias Penales (INACIPE) México, 2007.

CASTELLANOS TENA, Fernando, Lineamientos Elementales de Derecho Penal. Editorial Jurídica Mexicana, México, 1959.

DÍAZ GARCÍA, Alexander. Derecho Informático. Editorial Leyer. 1ª reimpresión. Bogotá, Colombia, 2012.

GONZÁLEZ DE LA VEGA, Francisco, El Código Penal Comentado, 9ª edición. Editorial Porrúa, México, 1989.

GÜITRÓN FUENTEVILLA, Julián, El Delito de Atentados al Pudor (Estudio Dogmático), Universidad Nacional Autónoma de México, Facultad de Derecho, Talleres Gráficos Galesa, México, 1961.

GÜITRÓN FUENTEVILLA, Julián et al. Compendio de Términos de Derecho Civil. Editorial Porrúa y el Instituto de Investigaciones Jurídicas de la UNAM. México, 2004.

GÜITRÓN FUENTEVILLA, Julián. Tesis. Editado por Promociones Jurídicas y Culturales. México, 1991.

MOLINA SALGADO, Jesús Antonio, Delitos y Otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial, Editorial Porrúa, México, 2003.

MUÑOZ TORRES, Ivonne Valeria, Delitos Informáticos. Diez Años Después, 1ª edición, Editorial UBIJUS, México, 2009.

PORTE PETIT, Celestino, Programa de la Parte General del Derecho Penal, editado por la Universidad Nacional Autónoma de México, México, 1968.

TÉLLEZ VALDÉS, Julio, Derecho Informático, Editado por el Instituto de Investigaciones Jurídicas de la UNAM, México, 1987.

VILLA ESCOBOSA, Jaime, et al. Derecho y Medios Electrónicos. Editorial Porrúa, México, 2012.

VILLALOBOS, Ignacio, Derecho Penal Mexicano, Editorial Porrúa, México, 1960.

L E G I S L A C I Ó N

Compilación Penal Federal y del Distrito Federal. Diccionario de Términos y Plazos. Raúl Juárez Carro Editorial, 51ª edición. México, 2014.

D I C C I O N A R I O S

Real Academia Española. Diccionario de la Lengua Española. 22ª edición. Tomo 9, Editorial Mateu Cromo. Artes Gráficas, España, 2001.

Í N D I C E