Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano

Autor: Lic. Hiram Raúl Piña Libien[**]

SUMARIO: I. Introducción. II. Aproximación conceptual. III. Conductas mundialmente reconocidas como crímenes informáticos. IV. Los Delitos Informáticos previstos y sancionados en el ordenamiento jurídico mexicano. V. Perspectivas de regulación federal. VI. Conclusiones.

I. Introducción

El vertiginoso desarrollo tecnológico, la interdependencia económica, la desmedida informatización de la sociedad y el omnímodo poder de la Informática, han demandado de la moderna Ciencia Penal, la comprensión de las conductas criminales en las que se ve inmersa la informática.

La doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten en: 1) la actualización de la legislación, 2) la evolución jurisprudencial; y, 3) la redacción de leyes de carácter particular.

Amén de ello, ha registrado los fenómenos que por una parte, distorsionan las instituciones jurídicas y por otra, erosionan el ejercicio de los derechos y libertades fundamentales.[1]

[**] Director de Asuntos Legislativos de la Oficina del Abogado General de la Universidad Autónoma del Estado de México.

[1] Antonio-Enrique Pérez Luño, ha sostenido que son: 1) Libertad informática, 2) Criminalidad Informática, 3) Contratos Informáticos, 4) Impactos sociolaborales de la informática, 5) Flujo internacional de datos, 6) Protección del software. *Manual de Informática y Derecho*, Ariel, Barcelona, 1996, pp. 43 y ss. Para Miguel Ángel Davara Rodríguez son: 1) Protección de datos, 2) Protección jurídica del software, 3) Protección jurídica de las bases de datos, 4) Contratación electrónica, 5) Contratos Informáticos, 6) Transferencia electrónica de fondos, 7) Delito Informático, 8) Documento electrónico. *Derecho Informático*, ARANZADI, Pamplona, 1993, pp. 45 y ss. Carlos Barriuso Ruiz, identifica: 1) Intimidad y protección de datos, 2) Normativa protectora de programas de ordenador, 3) Normativa protectora de bases de datos, 4) Contratos Informáticos, 5) Responsabilidad civil derivada de la informática, 6) Contratación realizada por medio electrónicos e informáticos, 7) Prueba por medio de caracteres electrónicos e informáticos, 8) Delito informático, y 9) Informática y mundo laboral. *Interacción del Derecho y la Informática*, Dykinson, Madrid, 1996, pp. 145 y ss. Carlos María Correa y otros, consideran que las problemáticas entre Derecho e Informática son: 1) Protección jurídica del software, 2) Contratos Informáticos, 3) Protección de

Sería interesante profundizar en el estudio de cada una de ellas, pero sumamente inconveniente, pues desbordaría con mucho los objetivos fijados en esta ponencia.

En cambio, nos concentraremos en una de las temáticas que nos convoca a este Segundo Congreso Nacional "*Cultura de la Legalidad e Informática Jurídica*", los denominados Delitos Informáticos.

Veremos enseguida que al considerarse como delitos las conductas por las cuales se hace uso inadecuado, irracional e indiscriminado de la informática y sus avances, ha traído como consecuencia, la actualización del ordenamiento jurídico penal mexicano.

II. Aproximación conceptual

Las contravenciones legales, en el ámbito informático han sido definidas tanto por organizaciones internacionales como por estudiosos de la materia. La Organización para la Cooperación y el Desarrollo Económicos (OCDE), [2]

datos personales, 4) La prueba, 5) Delito informático, 6) Transformaciones en el derecho administrativo y procesal, y 7) Flujos de datos transfrontera. *Derecho Informático*, Buenos Aires, Depalma, 1987, pp. 55 y ss. Olivier Hance, en su criterio considera las siguientes problemáticas: 1) Propiedad Intelectual en Internet, 2) Libertad de expresión, 3) Protección de la privacía en Internet, 4) Internet y las comunicaciones comerciales, 5) Comercio electrónico, 6) Delito, y 7) Responsabilidades en Internet. *Leyes y Negocios en Internet*, Traducción de Yazmín Juárez Parra, México, McGraw Hill, 1996, pp. 77 y ss. Julio Téllez, considera que son: 1) Regulación de los bienes informacionales, 2) Protección de datos personales, 3) Flujo de datos transfronterizos, 4) Protección de los programas, 5) Delitos informáticos, 6) Contratos informáticos, 7) Ergonomía informática, y 8) Valor probatorio de los soportes modernos de información. *Derecho Informático*, McGraw Hill, Serie Jurídica, 2ª edición, México, 1995, pp. 57 y ss. Juan José Ríos afirma que son: 1) Protección jurídica de la información personal, 2) La protección jurídica del *software*, 3) El flujo de datos transfrontera, 4) Los convenios o contratos informáticos, 5) Los delitos informáticos, y 6) El valor probatorio del documento electromagnético. *Derecho e Informática en México: Informática Jurídica y Derecho de la Informática*, UNAM, México, 1997, pp. 69 y ss. Gabriela Barrios Garrido y otros, identifican: 1) Derecho a la información y libertad de expresión, 2) Derecho a la privacidad, 3) Prácticas mercantiles a través de Internet, 4) Propiedad Intelectual en Internet, y 5) Prácticas delictivas a través de Internet. *Internet y Derecho en México*, México, McGraw Hill, 1998, pp. 29 y ss.

[2] Fueron Estados miembros originales de la OCDE: Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos (Holanda), Portugal, Reino Unido, Suecia, Suiza y Turquía. Posteriormente se han incorporado mediante adhesión: Japón (28 de abril de 1964), Finlandia (28 de enero de

estableció en 1983, que el *Computer Crime* que es "*...cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos*."[3]

Antonio-Enrique Pérez Luño, ha sostenido que es "*...aquel conjunto de conductas criminales que se realizan a través de del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos*."[4]

Miguel Ángel Davara lo ha definido como "*...la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*."[5]

Carlos Sarzana considera que son "*...cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo*,"[6]

Por su parte, Julio Téllez los ha conceptualizado como "*...actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)*."[7]

Para los efectos de esta exposición, preferimos proponer un concepto que nos permita entender la complejidad que representa la *Computerkriminalität*.

1969), Australia (7 de junio de 1971), Nueva Zelanda (29 de mayo de 1973), México (18 de mayo de 1994), República Checa (12 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y Eslovaquia (14 de diciembre de 2000).

[3] OECD. *Computer related criminality: analysis of legal policy in the OECD Area*, ICCP, 1984.

[4] *Manual de Informática y Derecho*, Ariel, Barcelona, 1996, p. 70. De este mismo manual, existe una edición mexicana, bajo el título de *Ensayos de Informática Jurídica*, Fontamara, México, 1996.

[5] *Derecho... op. cit. supra*, nota 1, p. 318.

[6] "Criminalita e Tecnologia", *Computer Crimes, Resegna Penitenzíaria e Criminología* Nos. 1-2. Anno 1, Gennanio-Giugno, 1979, Roma, Italia, p. 59, *apud* Téllez Valdés, Julio. *Derecho Informático*, 2ª edición, Mc Graw Hill, México, 1996, p. 104.

[7] *Derecho Informático*, 3ª edición, Mc Graw Hill, México, 2004, p. 163.

Sostenemos que, el Delito Informático es una conducta humana ilícita que jurídicamente es reprochable; puesto que busca dolosamente por una parte, vulnerar bienes jurídicos relacionados con la informática, en sus aspectos lógicos y físicos, y por otra atentar y restringir los derechos y libertades individuales fundamentales.

III. Conductas mundialmente reconocidas como crímenes informáticos

La doctrina del Derecho de la Informática, ha realizado diversas clasificaciones de los Delitos Informáticos; entre ellas destacan las de Irving J. Sloan, Ulrich Sieber, Olivier Hance, Pablo Andrés Palazzi, Gabriela Barrios, Esther Morón Lerma, Antonio-Enrique Pérez Luño y Miguel Ángel Davara Rodríguez.

Podemos dar cuenta que entre dichas conductas criminales de cuello blanco, auspiciadas bajo la denominación de Delito Informático, destacan: *hacking*,[8] *cracking*,[9] *phishing*,[10] *evil twins*,[11] *pharming*[12] y *spamming*;[13] robo de identidad;[14]

[8] Se caracterizan este tipo de conductas criminógenas por el acceso no autorizado a un equipo o sistema informático. En el debate que representa la tipificación de los denominados *Delitos informáticos* y en particular de las conductas de *hacking*, se ha llegado a señalar la existencia de un tipo penal de acceso no autorizado simple y otro agravado, es decir, la conducta se agrava si tiene por objeto la producción de daños, que la intrusión tenga un fin específico, que a consecuencia de ello se tenga un resultado específico y, que la conducta tenga por objeto la violación de derechos intelectuales. *Cfr*. Cámpoli, Gabriel Andrés. *Principios de Derecho penal Informático*, Ángel Editor, México, 2004, p. 29-35. De esta misma obra, existe edición bajo el titulo *Derecho Penal Informático*, Editorial Investigaciones Jurídicas, S. A., San José, Costa Rica, 2003, p. 33-42. Morón Lerma, Esther. *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, ARANZADI, Pamplona, 1999, pp. 36 y ss. Palazzi, Pablo A. *Delitos Informáticos*, Ad-Hoc, Buenos Aires, 2000, pp. 85 y ss.
El Código Penal Federal tras la reforma del 19 de mayo de 1999, por la que se adicionó el Capítulo II al Título IX, para contener en los artículo 221 bis 1 al 211 bis 7 el delito de acceso ilícito a equipos y sistemas de informática, pretende ser una respuesta a la acuciosa necesidad por normar las conductas de *hacking*; como también la fracción I del artículo 217 del Código Penal del Estado de Sinaloa contempla el *hacking* como Delito Informático.
Recientemente el Consejo de Europa ha adoptado la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, sean sancionados como infracción penal. Por medio de esta Decisión, se obliga a los Estados miembros de la Unión a que adopten las medidas necesarias para punir el acceso e intromisión ilegal intencionado no autorizado a sistemas de información, así como la intromisión ilegal a los datos.
[9] A diferencia del *hacker*, el *cracker* "*...desconoce los sistemas informáticos y sus retos se limitan a la vulneración del software comercial acometiendo conductas de piratería informática*." Morón Lerma, Esther. *op. cit. supra*, nota 8, p. 32.

cyberterrorismo;[15] propagación de *Malware*[16] a través de las redes de datos; el empleo de tecnologías *Pop-Up Ads* y *Adware*,[17] la instalación de *sniffers*,[18]

[10] Se trata de correos electrónicos y portales de *Internet* falsos, pero que en apariencia son enviados por instituciones con las cuales una persona tiene contacto, *v. gr*. un banco, pero dichos mensajes son disfrazados por redes bien organizadas de delincuentes informáticos que se hacen pasar por la institución con la que se está acreditado, y en el que piden al usuario que actualice sus datos. Sin embargo, el usuario no estará actualizando sus datos, sino más bien proporcionándoselos a la delincuencia informática.

[11] Señala Kevin J. Delaney, que: "Los *evil twins* son redes inalámbricas *Wi-Fi* que aparentan ofrecer conexiones a Internet tan confiables como las que hay disponibles en muchas cafeterías y salones de conferencias. En la pantalla de una computadora portátil, un punto de conexión *evil twin* tiene el mismo aspecto que el de decenas de miles de redes públicas inalámbricas a las que acceden los consumidores cada día, a veces incluso copiando el aspecto de la página de acceso al sistema. Pero es sólo una fachada que sirve a los autores de la estafa para robar cualquier número de tarjeta de crédito y contraseñas que se digite usando la conexión." REFORMA. *Nuevas amenazas en la Web vienen por partida doble. Los criminales de Internet han inventado otros dos métodos más difíciles de detectar, para defraudar a los usuarios: el 'evil twin' y el 'pharming'*, Martes 17 de mayo de 2005, Negocios, p. 8A.

[12] Se presenta esta conducta cuando un criminal informático desvía a un consumidor hacía una página electrónica apócrifa, aún y cuando el usuario halla escrito correctamente la dirección electrónica de la empresa con que desea contactar. *Cfr*. Idem.

[13] El *Spam* o también llamado correo basura o chatarra, consiste en el envío masivo de información no solicitada por medio del correo electrónico. Generalmente la información que se difunde tiene fines publicitarios. *Cfr*. Molina Salgado, Jesús Antonio. *Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial*, Porrúa, México, 2003, pp. 52-55. Sobre las pérdidas que acarrea en México esta conducta, *Cfr*. Cardoso, Victor. *En México los correos basura ocasionan pérdidas por $6.5 millones al mes*, Internet, http://www.jornada.unam.mx/2005/mar05/050324/019n1eco.php.

[14] Sobre cómo se produce y qué debe hacerse, en los Estados Unidos de Norteamérica, en caso de que ser objeto del robo de identidad, *Vid*. Federal Trade Commission. *Robo de Identidad. Algo malo puede pasarle a su buen nombre*, Internet, http://www.ftc.gov/bcp/conline/spanish/credit/s-idtheft.htm. El robo de identidad, no solamente opera en contra de personas físicas, las personas jurídicas y en especial las jurídicas de derecho público han sido frecuentemente víctimas de esta conducta; así v. gr. el robo de identidad que sufriera la Secretaria de Relaciones Exteriores de México, mediante una página apócrifa en Internet (*http://www.sre-empleos-gob.mx.gs*), a través de la cual se ofrecía a los incautos la realización de tramites para la regularización de indocumentados, mediante el pago de $ 5,850.00 pesos que deberían ser depositados en una cuenta bancaria. Amén del robo de identidad, se pedía a los "interesados", enviar 3 Fotografías tamaño pasaporte, 3 Copias del Acta de Nacimiento, 3 Copias de la Credencial de Elector y 1 Comprobante de Domicilio.

[15] El término se ha empleado fundamentalmente para hacer referencia a la posibilidad de que sean atacados tanto los sistemas de información como las redes de datos o que estos sean utilizados por y para perpetrar actos terroristas. *Vid*. Secciones 223 y 224 de la *Homeland Security Act of 2002*.

[16] Proveniente de los términos ***MAL****icious soft****WARE***, se constituye por programas, documentos o mensajes que pueden causar daños a los equipos de los usuarios.

[17] Se caracterizan por ser programas que se instalan con o sin el consentimiento de los usuarios informáticos; a través de ellos se despliegan en intervalos de tiempo anuncios y mensajes publicitarios que se sobreponen a la aplicación informática que se tenga en ese momento en uso.

[18] Los rastreadores o *sniffers*, "*...suelen ser usados para penetrar en el disco duro de los ordenadores conectados a la red, buscando cierto tipo de información*." Morón Lerma, Esther. *op. cit. supra*, nota 8, p. 33.

spyware, o programas espía en las computadoras personales para conocer los hábitos y actividades de familiares o empleados; [19] así como la vigilancia internacional de las comunicaciones electrónicas a través de programas gubernamentales como *ECHELON* [20] o los de control fronterizo como el *US-VISIT*, [21] son tan sólo algunas de las tantas expresiones de tan variada fenomenología que han hecho que la seguridad jurídica de las personas y de las transacciones comerciales electrónicas, dependan de las medidas de seguridad de los sistemas informáticos de información y comunicación.[22]

Huelga decir que los Delitos Informáticos se caracterizan por ser conductas criminales altamente tecnificadas con innegables repercusiones económicas.

[19] El *Spyware* y el *software* espía se caracterizan por ser aplicaciones informáticas cuyo objetivo es la recopilación de información personal sin consentimiento del usuario, para ser en el primer caso transmitida a terceros interesados en las actividades del usuario; y, en el segundo, para vigilar silenciosamente las conductas, actividades e información que una persona realiza u obtiene mientras pasa tiempo frente a la computadora, y con ello obtener *passwords*, estados de cuenta bancarios, conocimiento de su correspondencia electrónica, etcétera.

[20] ECHELON es el nombre de un sistema de vigilancia desarrollado por la Agencia Nacional de Seguridad (NSA) de Estados Unidos junto a los servicios secretos del Reino Unido, Australia, Nueva Zelanda y Canadá, cuyo objetivo radica en interceptar las comunicaciones establecidas entre los gobiernos, las organizaciones y las empresas de todos los países del mundo. El sistema intercepta cantidades ingentes de mensajes cuyo contenido explora, utilizando sistemas de inteligencia artificial, con el fin de encontrar palabras clave significativas objeto de vigilancia. *Cfr*. Galindo, Fernando. *Derecho e Informática*, LA LEY-ACTUALIDAD, Madrid, 1998, p. 110.

[21] El programa *US-VISIT* implica que a todos los viajeros que ingresen a los Estados Unidos de Norteamérica, se les revisará su visa, su pasaporte y además se les tomarán huellas dactilares y una fotografía. Al terminar el viaje, los pasajeros deberán dejar constancia de su salida. Con este esquema, Estados Unidos busca mejorar la seguridad de sus ciudadanos y de los visitantes, agilizar el tránsito de los viajeros y facilitar el comercio legítimo; pero sobre todo verificar e identificar mediante mecanismos biométricos la identidad de las personas, misma que es corroborada con la lista de sospechosos de terrorismo que mantiene el Departamento de Seguridad Interior de Estados Unidos. *Cfr*. U.S. Department of Homeland Security. *Department of Homeland Security to Begin Biometric Exit Pilot as Part of US-VISIT Program*, Internet, http://www.dhs.gov/dhspublic/display?content=3875; así mismo, REFORMA. *Inicia EU el 5 de enero el 'fichaje' de visitantes*, 23 de diciembre de 2003, disponible en: http://www.reforma.com/edicionimpresa/notas/031223/primera/451898.htm. *Vid*. Título IV de la *Homeland Security Act of 2002*.

[22] *Cfr*. Galindo, Fernando. *op. cit. supra*, nota 20, pp. 67 y ss; también A.A. V.V. Mir Puig, Santiago (Comp.). *Delincuencia Informática*, Promociones y Publicaciones Universitarias, IURA-7, Barcelona, 1992, en especial la colaboración de Sieber, Ulrich. *Documentación para una aproximación al Delito Informático*, pp. 65-98, en particular la Parte II en donde el Profesor de la Universidad de Beirut, establece los objetivos y el ámbito para el establecimiento de los elementos más importantes que permitan diseñar una estrategia de seguridad informática efectiva.

Bajo el anterior marco de referencia, es posible adentrarnos al conocimiento de los Delitos Informáticos previstos y sancionados en el ordenamiento jurídico mexicano.

IV. Los Delitos Informáticos previstos y sancionados en el ordenamiento jurídico mexicano

Debemos advertir que cuando empleamos la expresión “ordenamiento jurídico” lo hacemos para significar la normativa de derecho público, mediante la cual se regula de manera dispersa una materia; pero que desde la perspectiva epistemológica puede ser vista como una unidad normativa.

Hemos observado que la informatización de la sociedad y los fenómenos que se desarrollan en el seno de la Sociedad de la Información, han demandado a nivel mundial la actualización de los marcos legales, a fin de que se reconstruyan las hipótesis jurídicas en que se disponen diversas conductas criminales frente al uso de la informática.

Al respecto, el ordenamiento jurídico mexicano no ha sido la excepción. En adelante, veremos cuáles son las conductas que se prevén y sancionan en el ámbito nacional. Ello permitirá por una parte, conocer la clasificación legal de los Delitos Informáticos en México, y por otra, delatar la existencia de previsiones legales respecto a los denominados Delitos Informáticos.

De manera recurrente, en el ámbito académico, existe la inquietud entre los noveles egresados de la Licenciatura en Derecho, para considerar como probable objeto de investigación el tema de los Delitos Informáticos, es decir, sugieren su inclusión, ya sea en el Código Penal Federal o en uno de carácter estatal, en razón a que perciben la ausencia de un Capítulo o un delito con tal denominación.

Con el fin de que la exposición sea lo más nítida posible, expondremos las conductas ilícitas que se identifican como Delitos Informáticos, y que se encuentran previstas y sancionadas en los Códigos Penales de las Entidades Federativas y posteriormente las que se prevén en la legislación penal federal.

1. Códigos Penales de las Entidades Federativas

A. Distrito Federal

El artículo 336 del Nuevo Código Penal del Distrito Federal,[23] relativo a la *Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje*, dispone que se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello, altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V); adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma (fracción VI); y a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos. (fracción VII).

[23] Publicado en la *Gaceta Oficial del Distrito Federal* el 16 de julio de 2002. La denominación del Capítulo I del Título Vigésimo Cuarto, del Libro Segundo; así como la adición de la fracción VIII del artículo 336 del Nuevo Código Penal para el Distrito Federal, fueron publicadas en la *Gaceta Oficial del Distrito Federal* el 20 de diciembre de 2004.

Por otra parte, el artículo 355 del Nuevo Código Penal, dispone que se impondrán de cuatro a nueve años de prisión y de doscientos cincuenta a cuatrocientos días multa, al funcionario electoral que altere, expida, sustituya, destruya o haga mal uso de documentos públicos electorales o archivos oficiales computarizados o relativos al registro de electores que corresponda.

B. Estado de México

El artículo 174 del Código Penal del Estado de México,[24] relativo a la *Falsificación y Utiilización Indebida de Títulos al Portador, Documentos de Crédito Público y Documentos Relativos al Crédito*, prevé que se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios (fracción IV); y a quien acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo (fracción V).

No obstante lo anterior, se tiene prevista la imposición de las mismas penas, a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios.

Este delito presenta dos singularidades, que radican en el hecho de que admite las reglas del concurso de delitos, para el caso de que se actualicen otras conductas y el aumento de las penas en una mitad, si el sujeto activo es empleado o dependiente del ofendido.

[24] Aprobado el 29 de febrero del 2000, Promulgado el 17 de marzo del 2000, Publicado el 20 de marzo del 2000 y vigente a partir del 25 de marzo del 2000.

Finalmente, cabe decir que las conductas contenidas en el artículo 174 del Código Penal del Estado de México, son calificadas por disposición del artículo 9 como graves.

C. Jalisco

El artículo 170 Bis del Código Penal para el Estado Libre y Soberano de Jalisco,[25] relativo a la *Falsificación de Medios Electrónicos o Magnéticos* dispone que se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente en la época y área geográfica en que se cometa el delito, al que, sin consentimiento de quien esté facultado para ello, altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal (fracción II); acceda, obtenga, posea o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo (fracción III); y a quien adquiera, utilice, posea o detente equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I del artículo (fracción IV).

Finalmente, dispone que las mismas penas se impondrán a quien utilice o revele indebidamente información confidencial o reservada de la persona física o jurídica que legalmente esté facultada para emitir los boletos, contraseñas, fichas u otros documentos, con el propósito de realizar operaciones ilícitas y no autorizadas por

[25] Aprobado el 2 de agosto de 1982, Publicado el 2 de septiembre de 1982 y vigente a partir del 2 de noviembre de 1982.

la persona emisora, o bien, por los titulares de los boletos, contraseñas, fichas u otros documentos.

D. Nuevo León

El artículo 242 Bis del Código Penal para el Estado de Nuevo León,[26] relativo a la *Falsificación de Títulos al Portador, Documentos de Crédito Público y relativos al Crédito*, dispone que se impondrán de tres a nueve años de prisión y multa de ciento cincuenta a cuatrocientas cincuenta cuotas al que, sin consentimiento de quien esté facultado para ello, altere, tarjetas de crédito o de débito, o la información contenida en éstas, esqueletos de cheque o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo (fracción I); altere los medios de identificación electrónica de cualquiera de los objetos referidos en la fracción I (fracción IV); o acceda indebidamente a los equipos electromagnéticos de las instituciones emisoras de cualquiera de los objetos referidos en la fracción I (fracción V).

Al igual que el Código Penal del Estado de México, prevé la imposición de penas, a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios; así como la admisión de las reglas del concurso de delitos, para el caso de que se actualicen otras conductas; que las penas aumenten en una mitad si el sujeto activo es funcionario o empleado del ofendido; pero también considerado como delito grave en términos del artículo 16 Bis.

Por otra parte, en el Código Penal para el Estado de Nuevo León, se equipara al robo y se castiga como tal, en términos del artículo 365, el apoderamiento material

[26] Publicado en el Periódico Oficial de 26 de marzo de 1990. El artículo 242 Bis, fue adicionado, según publicación en el Periódico Oficial de 28 de julio de 2004, entrando en vigor al día siguiente de su publicación.

de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Por lo que respecta a los delitos por medios electrónicos,[27] los artículos 427, 428 y 429, disponen que se le impondrá de 2 meses a 2 años de prisión y multa de 200 a 1000 cuotas, a quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos; de 2 a 8 años de prisión y multa de 300 a 1500 cuotas, a quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos; y de 2 a 8 años de prisión y multa de 350 a 2000 cuotas, a quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos, respectivamente.

E. Quintana Roo

El artículo 189 Bis del Código Penal para el Estado Libre y Soberano de Quintana Roo,[28] relativo a la *Falsificación de documentos y uso de documentos falsos*, dispone que se impondrá hasta una mitad más de las penas previstas en el artículo 189 (prisión de seis meses a tres años y de quince a noventa días multa), al que copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios para disposición en efectivo (fracción III); y a quien accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo (fracción IV).

[27] Adicionados, según publicación en el Periódico Oficial de 28 de julio de 2004, entrando en vigor al día siguiente de su publicación.
[28] Adicionado, según publicación en el Periódico Oficial de 29 de diciembre de 2000.

Al igual que los Códigos Penales de los Estados de México y Nuevo León, prevé la imposición de penas, a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo; la admisión de las reglas del concurso de delitos, para el caso de que se actualicen otras conductas; y que las penas aumenten en una mitad si el sujeto activo es funcionario o empleado del ofendido.

.

F. Sinaloa

Cronológicamente el artículo 217 del Código Penal para el Estado de Sinaloa,[29] fue el primero en tipificar el Delito Informático; y casualmente es el único que lo denomina así. En dicho artículo, se dispone que al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa. Establece que comete delito informático, la persona que dolosamente y sin derecho, use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información (fracción I); o; Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red (fracción II).

2. Legislación penal federal

Por otra parte, en el Código Penal Federal se encuentran previstos entre otros, los delitos de Revelación de Secretos, Acceso ilícito a equipos y sistemas de informática y los Delitos contra los Derechos de Autor.

[29] Decreto Número 539, Publicado en el Periódico Oficial No. 131 de 28 de octubre de 1992.

En este tenor, el Delito de revelación de secretos se tipifica cuando en perjuicio de alguien, sin justa causa y sin consentimiento, se revele, divulgue o utilice algún secreto, comunicación, información o imágenes, que hayan sido conocidas o recibidas con motivo de un empleo, cargo o puesto, por la prestación de un servicio profesional o técnico, por ser funcionario o empleado público; cuando dicho secreto sea de carácter industrial, o bien, se hubiese obtenido de una intervención de comunicación privada.[30]

Mientras que el de acceso ilícito a sistemas y equipos de informática, se recogen en los artículos 211 bis 1 al 211 bis 7, conductas que pueden considerarse como *hacking informático*; mismas que consisten en la modificación, destrucción, la provocación a perder, el conocer o copiar información que esté contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean de particulares, del Estado o de las instituciones que integran el sistema financiero.

Por otra parte, en la fracción II del artículo 424 bis se dispone que constituye un delito contra los Derechos de Autor, la fabricación con fin de lucro de un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación; tipo penal que puede ser considerado como *cracking informático*. Por su parte, el artículo 426 prevé que se constituyen como ilícitos en materia de Derechos de Autor, la fabricación, importación, venta o arrendamiento de dispositivos o sistemas que descifren señales satelitales cifradas, y que sea portadora de programas, sin autorización del distribuidor

[30] El criterio contenido en el artículo 211bis del Código Penal Federal, fue legitimado por vez primera, por la Sala Primera de la Suprema Corte de Justicia de la Nación, en el mes de agosto de 2005, al negar los juicios de amparo promovidos por Carlos Maillard Estañol y Samuel Morales Lozano, en su carácter de contralores internos de la empresa PMI Comercio Internacional, subsidiaria de Petróleos Mexicanos, y quienes fueran denunciados en 1999 por el espionaje telefónico que sufriera Luis Arturo Guzmán Villaseñor, quien estaba sujeto a un procedimiento administrativo. En la resolución de los amparos, se reveló la existencia de un Sistema de Grabación de Conversaciones Telefónicas que opera por normatividad interna de PMI.

legítimo de dicha señal, y cualquier acto con fines de lucro, cuya finalidad sea descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Otro ordenamiento en el que se prevé la protección de bienes jurídicos, frente a la informática y sus avances, es la Ley Federal contra la Delincuencia Organizada (LFDO);[31] en ella se establece la existencia de una unidad especializada de la Procuraduría General de la República para la investigación y persecución de delitos cometidos por miembros de la delincuencia organizada. Dicha unidad especializada, puede previa solicitud por escrito a un juez de distrito, intervenir las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores, misma que podrá ser verificada en cualquier momento por el juzgador que autorizó la intervención. La LFDO establece sanciones que podrán ser aplicadas a quienes participen en la intervención de comunicaciones privadas, a los servidores públicos del Poder Judicial Federal que participen en los procesos que se incoen en contra de los delincuentes organizados, y a quienes con motivo de su empleo, cargo o comisión público, revelen, divulguen o utilicen en forma indebida o en perjuicio de otro la información o imágenes obtenidas en el curso de una intervención de comunicaciones privadas, autorizada o no; o que tengan conocimiento de la existencia de una solicitud o autorización de intervención de comunicaciones privadas y revelen su existencia o contenido; por lo tanto, dicha información tiene carácter de reservado.

La recientemente promulgada Ley de Seguridad Nacional (LSN),[32] establece que las acciones que se establezcan de manera inmediata y directa, dirigidas a

[31] Publicada en el Diario Oficial de la Federación de 7 de noviembre de 1996, y reformada por última ocasión el 21 de diciembre de 2004.
[32] Publicada en el Diario Oficial de la Federación de 31 de enero de 2005.

mantener la integridad, estabilidad y permanencia del Estado Mexicano, se rigen por los principios de legalidad, responsabilidad, respeto a los derechos fundamentales de protección a la persona humana y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación. En este sentido, establece que los datos personales otorgados a una instancia por servidores públicos, así como los proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional, son Información gubernamental confidencial, es decir, que las autoridades, personal de las instancias de Seguridad Nacional y servidores públicos que laboren en las instancias que integren el Consejo Nacional de Seguridad Nacional o del Centro de Investigación y Seguridad Nacional, deben guardar secreto y confidencialidad respecto a la información que conozcan o tengan acceso en o con motivo de su función; [33] para lo cual, deberán otorgar por escrito una promesa de confidencialidad que observarán en todo tiempo, aún después de que hayan cesado en el cargo.[34]

[33] Respecto al carácter confidencial de determinada información en relación con la seguridad nacional, ha sostenido el Pleno de la Suprema Corte de Justicia de la Nación, mediante tesis aislada, que: *El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados*. Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XI, abril de 2000, Tesis P. LX/2000, página 74, bajo el Rubro: *Derecho a la información. Su ejercicio se encuentra limitado tanto por los intereses nacionales y de la sociedad, como por los derechos de terceros*.

[34] En relación con estás obligaciones, el artículo 47 de la Ley Federal de responsabilidades de los servidores públicos, dispone que: Todo servidor público tendrá las siguientes obligaciones, para salvaguardar la legalidad, honradez, lealtad, imparcialidad y eficiencia que deben ser observadas en el desempeño de su empleo, cargo o comisión, y cuyo incumplimiento dará lugar al procedimiento y a las sanciones que correspondan, sin perjuicio de sus derechos laborales, así como de las normas específicas que al respecto rijan en el servicio de las fuerzas armadas. Y en

En el ámbito financiero, el artículo 112 Bis de la Ley de Instituciones de Crédito, dispone que se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que altere el medio de identificación electrónica y acceda a los equipos electromagnéticos del sistema bancario, con el propósito de disponer indebidamente de recursos económicos (fracción III); y a quien obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario, y sin contar con la autorización correspondiente (fracción IV).

La pena podrá aumentarse hasta en una mitad más, si quien realice cualquiera de estas conductas tiene el carácter de consejero, funcionario o empleado de cualquier institución de crédito.

Finalmente, el artículo 113 Bis 1 de la misma Ley, prevé que serán sancionados los servidores públicos de la Comisión Nacional Bancaria y de Valores, con la pena establecida para los delitos correspondientes más una mitad y permitan entre otras cuestiones, que los funcionarios o empleados de la institución de crédito alteren o modifiquen registros con el propósito de ocultar hechos que probablemente puedan constituir delito (inciso b).

V. Perspectivas de regulación federal

El diputado Jesús Aguilar Bueno, del grupo parlamentario del PRI, presentó el jueves 7 de octubre de 2004, la Iniciativa que reforma el Código Penal Federal en materia de pornografía infantil, corrupción de menores, comunicación y correspondencia, revelación de secretos y acceso ilícito a sistemas y equipos de informática, falsificación de documentos en general, amenazas y revelación de datos personales, delitos en contra de las personas en su patrimonio; el Código

particular su fracción IV dispone que es: Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebidas de aquéllas.

Federal de Procedimientos Penales en materia de aseguramiento del inculpado y careos, así como la Ley Federal Contra la Delincuencia Organizada, en materia de la naturaleza, objeto y aplicación de la ley.[35]

Respecto al contenido y alcances de esta iniciativa, cabe señalar, que el pasado 28 de abril de 2005, fue aprobado en primera lectura el Dictamen de las Comisiones Unidas de Justicia y Derechos Humanos, y de Atención a Grupos Vulnerables, con proyecto de decreto que reforma, adiciona y deroga diversas disposiciones del Código Penal Federal, del Código Federal de Procedimientos Penales y de la Ley Federal contra la Delincuencia Organizada, en materia de explotación sexual infantil, [36] entre cuyos antecedentes figuran la Iniciativa que adiciona los artículos 201 bis y 205 del Código Penal Federal, presentada por el Diputado Jesús González Schmal, del Grupo Parlamentario de Convergencia por la Democracia Partido Político Nacional;[37] otra por la que se reforman diversas disposiciones del Código Penal Federal en materia de protección a la niñez, presentada por el Diputado Álvaro Burgos Barrera, del Grupo Parlamentario del Partido Revolucionario Institucional;[38] como también, la Iniciativa de Reformas a diversas disposiciones del Código Penal Federal y al Código Federal de Procedimientos Penales, para establecer como figuras con propia definición y sanción a la pornografía y lenocinio infantil, presentada por los Diputados Manlio Fabio Beltrones Rivera y María de Jesús Aguirre, ambos del Grupo Parlamentario del Partido Revolucionario Institucional;[39] y, finalmente la Iniciativa que Reforma, Deroga y Adiciona diversas disposiciones del Código Penal Federal, del Código Federal de Procedimientos Penales y de la Ley Federal contra la Delincuencia

[35] Gaceta Parlamentaria, número 1600-I, jueves 7 de octubre de 2004; disponible en http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html.
[36] Gaceta Parlamentaria, número 1742-III, jueves 28 de abril de 2005, disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2005/abr/Anexo-III-28abr.html#Dicta20050428ExplotacionInfantil.
[37] Gaceta Parlamentaria, número 1474-I, martes 13 de abril de 2004, disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2004/abr/Anexo-I-13abr.html#Ini20040413Schmal.
[38] Gaceta Parlamentaria, número 1484-II, martes 27 de abril de 2004, disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2004/abr/Anexo-II-27abr.html#Ini20040427Varo.
[39] Gaceta Parlamentaria, número 1522, viernes 18 de junio de 2004, disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2004/jun/20040618.html.

Organizada, en materia de Protección a la Niñez y Personas con Discapacidad Intelectual, presentada por la Diputada Evangelina Pérez Zaragoza, a nombre de varios Diputados integrantes del Grupo Parlamentario del Partido Acción Nacional.[40]

Así las cosas, en el Dictamen en el que se contiene el Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Penal Federal, del Código Federal de Procedimientos Penales y de la Ley Federal contra la delincuencia organizada, en materia de explotación sexual infantil, se propone la reforma del inciso c) del artículo 85; las denominaciones del Título Octavo y de sus correspondientes Capítulos Primero, Segundo, Tercero y Cuarto del Libro Segundo; los artículos 200; 201 bis; 202; 203; 204; 205; 206, 207, 208 y 209; la adición de los artículos 202 bis, 203 bis, 204 bis, 205 bis y 206 bis; tres nuevos Capítulos Quinto, Sexto y Séptimo al Título Octavo, un Capítulo Tercero al Título Décimo Octavo ambos del Libro Segundo; la derogación de los artículos 201 bis 1, 201 bis 2 y 201 bis 3, todos del Código Penal Federal; la reforma de los incisos 13) y 23) de la fracción I del artículo 194 del Código Federal de Procedimientos Penales; y, la reforma de la fracción V del artículo 2 de la Ley Federal contra la Delincuencia Organizada.

Una vez que sean cubiertos los restantes requisitos que exige el proceso legislativo y por consiguiente su entrada en vigor, se considerarán los delitos de corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo; pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo; turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de

[40] Gaceta Parlamentaria, número 1608, martes 19 de octubre de 2004, disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-19oct.html.

personas que no tienen capacidad para resistirlo; Lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo; trata de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo; y trata de personas; todos estos considerados como graves y de delincuencia organizada.

Sin embargo, es necesario apuntar el posible exceso en que eventualmente pueden estar incurriendo los párrafos primero y tercero del artículo 202, pues en ellos se establece que se impondrá una pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, a quien realice la reproducción de material (video grabación, la fotografía, la filmación, exhibición o descripción a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos) en que se realicen actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados.

Esta posible exuberancia del párrafo tercero del artículo 202, radica básicamente en imputar como conducta delictiva la reproducción de dicho material, sobre todo cuando dicho acto se realiza mediante la ejecución que se haga de los archivos de datos de una red pública o privada de telecomunicaciones o de sistemas de cómputo o electrónicos. Para comprender el extremo que resulta de la interpretación de esta disposición, es necesario recurrir a la definición que la fracción VI del artículo 16 de la Ley Federal del Derecho de Autor obsequia respecto a lo que es la reproducción de una obra; en este sentido, reproducción es *la realización de uno o varios ejemplares de una obra, de un fonograma o de un videograma, en cualquier forma tangible, incluyendo cualquier almacenamiento permanente o temporal por medios electrónicos, aunque se trate de la realización bidimensional de una obra tridimensional o viceversa*.

En vista de esta correlación entre el Código Penal Federal y la Ley Federal del Derecho de Autor, los párrafos primero y tercero del artículo 202, estaría considerando *v. gr*. a todo individuo, que sin su consentimiento y por cuestión de haber leído un mensaje de correo electrónico no solicitado o *spam*, de cuyo contenido se anexa una video grabación o fotografía, o bien, se describan en su texto a manera de publicidad anuncios en los que se exhiba a una o varias personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, para realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, estará cometiendo –a pesar de que inmediatamente el mensaje sea borrado tanto de la cuenta de correo electrónico como del *cache* de la computadora– el delito de pornografía en agravio de cualquiera de esos sujetos pasivos, es decir, que el simple acto de *download* de una imagen o texto en el que encuentre una mínima referencia a la Pornografía Infantil, constituye en sí mismo un acto de *pedofilia*.

La crítica se finca a este tipo penal, no radica como pudiera pensarse a primera vista en la complejidad técnica que implica la demostración del hecho punible, sino en que, para los efectos de sus alcances, podrá inclusive considerarse que una imagen o video grabación familiares en las que se muestre el cuerpo desnudo de menores de edad y se den a conocer a diversos familiares mediante su transmisión a manera de archivos de datos, a través de una red pública o privada de telecomunicaciones, o de un sistema de cómputo o electrónico, podría ser considerado como un acto de pornografía infantil.

También debe darse cuenta de la Iniciativa de Ley del Mercado de Valores, que fuera presentada por el Poder Ejecutivo Federal al Senado de la República el 31 de marzo de 2005; misma que fuera dictaminada por las Comisiones Unidas de Hacienda y Crédito Público y de Estudios Legislativos y aprobada favorablemente por dicho órgano legislativo el 27 de abril de 2005 con 77 votos. En esta próxima

ley (actualmente se encuentra turnada en la Cámara de Diputados para sus efectos constitucionales), se norman entre otras cuestiones, el impedir tanto a los miembros y al secretario del consejo de administración de las sociedades anónimas bursátiles, para que no destruyan u ordenen destruir, total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión de la CNBV o dichos actos tengan como propósito, manipular u ocultar datos o información relevante de la sociedad a quienes tengan interés jurídico en conocerlos.[41]

El pasado 30 de marzo de 2005 el Poder Ejecutivo Federal, envió a la Cámara de Diputados de la LIX Legislatura Federal la Iniciativa de decreto que reforma y adiciona diversas disposiciones de la Ley Federal contra la Delincuencia Organizada, del Código Penal Federal, del Código Federal de Procedimientos Penales y de la Ley Orgánica del Poder Judicial de la Federación.[42] En dicha ley, se pretende perfeccionar la Intervención de Comunicaciones Privadas que derivan de la Ley Federal contra la Delincuencia Organizada, mediante la imposición de una medida de apremio, a los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, que no colaboren eficientemente con la autoridad competente para el desahogo de la intervención ordenada, consistente en una multa de cien a quinientas veces la percepción neta diaria de la persona, empresa o entidad de que se trate, atendiendo al grado de repercusión en la investigación y la gravedad de los hechos penalmente relevantes, materia de la averiguación previa o proceso en que se haya ordenado la intervención.

La Iniciativa del Ejecutivo Federal, pretende exceptuar como delito a las comunicaciones privadas, las grabaciones o registro de sonidos o imágenes que realicen agentes infiltrados, informantes o testigos, así como víctimas u ofendidos,

[41] Gaceta Parlamentaria del Senado de la República, número 111, miércoles 27 de abril de 2005, disponible en: http://www.senado.gob.mx/sgsp/gaceta/?sesion=2005/04/27/1&documento=45.
[42] Gaceta Parlamentaria, número 1720-III, miércoles 30 de marzo de 2005, disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/mar/Anexo-III-30mar.html.

que participen directamente en la comunicación de que se trate, mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, y que dicha comunicación se relacione con miembros de la delincuencia organizada.

Cabe dar cuenta también de la aprobación que tuvo a bien realizar el Senado de la República, respecto del Dictamen de las Comisiones Unidas de Justicia; y de Estudios Legislativos, por el que se contiene Proyecto de Decreto que se adiciona el artículo 243 Bis el Código Federal de Procedimientos Penales y se adicionan las fracciones XIII y XIV al artículo 215; se reforman las fracciones XI y XII, así como el párrafo tercero del artículo 215; se adiciona una fracción XXIX al artículo 225; se reforman las fracciones XXVII y XXVIII, así como el párrafo tercero del artículo 225, todos del Código Penal Federal. En síntesis, en dicho dictamen se establece el derecho a la secrecía sobre la información que reciban, conozcan o tengan en su poder, los abogados, consultores técnicos y los notarios, respecto de los asuntos en los cuales hubieran intervenido y tengan información que deban reservarse para el ejercicio de su profesión; los ministros de cualquier culto, con motivo de las confesiones que hubieran recibido en ejercicio del ministerio que presten; destaca de manera notable el secreto de los periodistas, respecto de los nombres o datos de identificación de las personas que, con motivo del ejercicio de su actividad, les proporcionen como información de carácter reservada, en la cual sustenten cualquier publicación o comunicado; y, a la que tienen derecho las personas o servidores públicos que desempeñen cualquier otro empleo, cargo, oficio o profesión, en virtud del cual la ley les reconozca el deber de guardar reserva o secreto profesional.[43]

Finalmente, la Cámara Alta del Congreso de la Unión, aprobó el Dictamen de las Comisiones Unidas de Hacienda y Crédito Público; de Justicia; y de Estudios Legislativos, mediante el cual se contiene el Proyecto de Decreto por el que se

[43] Gaceta Parlamentaria del Senado de la República, número 111, miércoles 27 de abril de 2005, disponible en: http://www.senado.gob.mx/sgsp/gaceta/?sesion=2005/04/27/1&documento=32.

reforma el párrafo primero, así como las fracciones I y II del artículo 240 Bis; se deroga la fracción III del artículo 240 Bis, ambos del Código Penal Federal, así como la reforma del artículo 112 Bis, y la adición de los artículos 112 Ter, 112 Quáter y 112 Quintus, todos de la Ley de Instituciones de Crédito, con el objeto de tipificar como delito la producción, reproducción, impresión, introducción al país, la enajenación onerosa o gratuita de tarjetas, esqueletos de cheque o documentos utilizados para el pago de bienes servicios o para la disposición de efectivo (objetos); la adquisición, posesión detentación, utilización o distribución de cualquier objeto que permita la comisión de alguna de esas actividades; la utilización indebida de información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir los objetos; la alteración, copia o reproducción de la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, así como la sustracción, copia o reproducción de la información contenida en alguno de los objetos a que se refiere el párrafo primero, con el propósito de obtener recursos económicos, la posesión, adquisición, utilización, comercialización o distribución de los objetos, a sabiendas de que están alterados o falsificados; el acceso a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario, con el fin de obtener recursos económicos o información confidencial o reservada; la alteración o modificación del mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo que son utilizados por los usuarios del sistema bancario, para obtener recursos económicos o información confidencial o reservada.[44] De ello, se desprende que una vez que sean cubiertos los restantes requisitos que exige el proceso legislativo y por consiguiente su entrada en vigor, se considerarán los delitos Falsificación y utilización indebida de documentos relativos al crédito, como graves.

[44] Gaceta Parlamentaria del Senado de la República, número 111, miércoles 27 de abril de 2005, disponible en: http://www.senado.gob.mx/sgsp/gaceta/?sesion=2005/04/27/1&documento=31.

Esta tendencia a la tipificación de dicho ilícito con el carácter de grave, se encuentra precedida de la consideración hecha con antelación por parte de los Códigos Penales de la Entidades Federativas de México y Nuevo León en los cuales se prevén dichos ilícitos con tal carácter.

Así mismo, se ha presentado la Iniciativa que adiciona un Capítulo al Título Vigésimo, Libro Segundo, del Código Penal Federal, con objeto de tipificar los delitos de inserción y divulgación de datos personales falsos, a cargo de la Diputada Cristina Portillo Ayala, del grupo parlamentario del PRD, y que fuera recibida en la sesión de la Comisión Permanente el miércoles 29 de junio de 2005;[45] así como la Iniciativa que adiciona un articulo 202 bis al Código Penal Federal y reforma la fracción V del artículo segundo de la Ley Federal contra la Delincuencia Organizada, con el objeto de tipificar el delito de utilización o facilitación de medios de comunicación para obtener contacto sexual con personas menores de 18 años de edad, a cargo de la diputada Cristina Portillo Ayala del grupo parlamentario del PRD, y que fuera recibida en la sesión de la Comisión Permanente del miércoles 6 de julio de 2005.[46]

La misma Diputada, entregó el 20 de julio de 2005, la Iniciativa que reforma el Código Penal Federal, en materia de Delitos Informáticos, a través de ella, sugiere se adicionen los artículos 246 Bis, 254 Quáter, 381 Ter y 389 Ter, con objeto de tipificar los delitos de falsificación informática, robo informático, fraude informático y oferta informática engañosa.[47]

VI. Conclusiones

[45] Gaceta Parlamentaria, número 1789, lunes 4 de julio de 2005, disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050704.html.
[46] Gaceta Parlamentaria, número 1793, viernes 8 de julio de 2005, disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050708.html.
[47] Gaceta Parlamentaria, número 1804, lunes 25 de julio de 2005, disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050725.html.

Como puede verse, es falsa la creencia de que en México no están reguladas las conductas criminales identificadas por la doctrina del Derecho de la Informática, bajo el nombre de Delitos Informáticos. El que la legislación penal mexicana no utilice tal denominación, no implica que las conductas previstas y sancionadas en ella, no sean consideradas como Delitos Informáticos.

Pretendimos en esta exposición, arribar a una clasificación legal de los Delitos Informáticos en México, misma que se expresa de la siguiente manera:

1. Acceso ilegal a equipos electromagnéticos.
2. Alteración de medios de identificación electrónica.
3. Fabricación, adquisición, posesión y utilización ilegal de equipos o dispositivos electromagnéticos.
4. Sustracción, uso y revelación de información electrónica confidencial.
5. Intercepción, interferencia, recepción, alteración, duplicación, reproducción, expedición, sustitución, daño, destrucción y uso indebido de archivos oficiales computarizados o de soportes lógicos o programas de computadora.
6. Defraudación electrónica.
7. Descifrar una señal de satélite cifrada.