Universidad Autónoma de Baja California

Facultad de Derecho Mexicali

“Delitos Electrónicos”

Trabajo terminal que para obtener el Diploma de

ESPECIALIDAD EN DERECHO

Presenta

Juan de Dios Faz Sánchez

Director

Mtro. René Rivas Sánchez

Mexicali, Baja California, México **Noviembre del 2007.**

ÍNDICE

INTRODUCCIÓN

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono.

La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

El auge del Comercio Electrónico evidencia en los tiempos actuales, que constituye un instrumento cuyo crecimiento es impresionante, sobre los cuales es necesario ejercer control que resguarde el desarrollo de la actividad comercial que allí se efectúa. El interés que surja y se establezcan parámetros controladores en beneficio de quienes forman parte de la actividad; es decir, tanto demandantes como comerciantes de bienes y servicios, quienes determinan como usuarios las necesidades reales sobre la cual opera estas actividades, aun cuando los fabricantes de las tecnologías han dado muestras fehacientes del perfeccionamiento en cuanto operatividad; sin embargo, en la actualidad se ha incrementado en el ciberespacio (escenario de la actividad comercial), un gran número de fraudes.

Los daños, perjuicios, desilusiones y otras consecuencias que puede generar los hechos que representan los engaños producidos en la Internet pueden ser in cuantificables y ruinosos para quienes sean defraudados.

Lo mismo ocurre con otras conductas que, aun cuando no son defraudatorias, constituyen una amenaza a la seguridad y confianza con las cuales deben hacerse las

comunicaciones y transacciones entre la gente. Así como también se puede ver seriamente afectadas la intimidad y reputación de las personas por hechos lesivos de distinta índole.

Las ventajas que producen el anonimato, la velocidad de las comunicaciones y la ansiedad de los mercados en un hecho que favorece a quienes medran en la red, buscando incautos y vulnerables internautas. La indefensión legal de las víctimas es un caldo de cultivo para el delito económico y otras variedades de conductas ilícitas.

Por otra parte, gracias a la impunidad reinante, se ha visto estimulado el abuso de la tecnología cibernética por causa de la acción de terroristas, piratas, fanáticos, alucinados, traficantes de drogas y productos prohibidos, lavadores de dinero, el crimen organizado y todo género de personas con diversos intereses ilegítimos. Ello perjudica sensiblemente el sano intercambio de quienes si quieren hacer cosas constructivas, productivas y actúan de buena fe.

El mal uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico. Obliga a pensar seriamente acerca del papel que puede desempeñar el derecho penal, a los fines de tutelar los bienes jurídicos que representan las interacciones en la Internet y, con ello, devolver la confianza y la tranquilidad a quienes desean realizar transacciones productivas, y hasta placenteras, sin el riesgo de verse esquilmados, aterrorizados o afectados en sus derechos e intereses impunemente.

En consecuencia, urge realizar una revisión de las normas penales, su aplicación, vacíos y carencias para proponer las reformas legislativas que correspondan, a los fines de brindar los márgenes indispensables de seguridad en los negocios y las comunicaciones entre la gente de buena fe, para quienes está destinada la red.

Uniendo ambos criterios, es decir el perfeccionamiento tanto de la plataforma operativa, como de la existencia de un marco legal debidamente diseñado que llene las

expectativas de regulación de la actividad comercial a través de la red son los parámetros reguladores sobre los cuales han de diseñarse la estructura proteccionista de quienes participan en dicha actividad Comercial.

PLANTEAMIENTO DEL PROBLEMA.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización para la Cooperación y el Desarrollo Económico a París en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

En la actualidad la informatización en red se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio, e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como criminalidad informática.

La tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial

(estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos. De este modo se pueden conocer los problemas que es necesario soslayar para conseguir una protección jurídica eficaz sin caer en la casuística.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

¿Qué se esta haciendo sobre las acciones tecnológicas desde las perspectivas jurídicas para prever y combatir estos delitos en el ámbito mundial y en México?

¿Cuáles son los principales delitos electrónicos que existen en México?

¿Cuál es la necesidad de que se legisle sobre los delitos informáticos y/o electrónicos en el Código Penal de Baja California?

OBJETIVO DE LA INVESTIGACIÓN

A) Objetivo General:

Acceder a un conjunto de conceptos e informaciones diversas, que permita en forma general y en especial, cuales son objeto de fraudes en la realización de las actividades cibernéticas; que permitan entender los orígenes, causa y consecuencias del fraude electrónico, y los delitos y abusos que ocurren en la Internet.

B) Objetivos Específicos:

- Evaluar la tecnología utilizada, conocer como inciden en el proceso como medio de ejecución, para la comprensión del delito electrónico a partir de analizar los ilícitos de la materia en otros países y México que nos permita la detección y lucha contra los delitos electrónicos.
- Determinar las condiciones necesarias para el establecimiento de la actividad comercial en red, que permita una actividad segura, sin riesgos desde el punto de vista jurídico.
- Tipificar el delito informático en el Código Punitivo del Estado regulando Penalmente las actitudes antijurídicas para editar su impunidad

METODOLOGÍA

Es un estudio documental ya que se basa en el análisis de la normatividad legal del uso indebido de los sistemas informáticos, fundamentalmente en el Código Penal del Estado de Baja California

b) Objeto de estudio

Análisis y estudio del Código Penal del Estado de Baja California para que se legisle sobre el uso indebido de sistemas informáticos

c) Material

Bibliográfico, hemerográfico y medios electrónicos, así como el análisis basado en el estudio de legislación y Derecho Comparado, además en de la aplicación de la teoría de la legislación, teoría de la argumentación jurídica y lineamientos de técnica legislativa

Para ello el trabajo se desarrolló en tres capítulos, en el primero se presentan las bases teóricas de los delitos electrónicos, en el segundo, se analizan las propuestas internacionales sobre los mismos y en el tercero, se presenta un análisis de la legislación nacional sobre los delitos electrónicos.

I. Bases Teóricas de los Delitos Electrónicos.

1.1 Concepto de delitos informáticos

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.
A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".[1]

Para Carlos Sarzana, en su obra Criminalista e tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora

[1] Téllez Valdez Julio. *Derecho Informático.* Segunda edición. México. Mc. Graw. Hill 1996 Pp. 103-104

ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".[2]

Nidia Callegari (1985) define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas"[3]

Rafael Fernández Calvo que en" tratamiento de llamado delitos electrónicos" en el proyecto de ley Orgánico del Código Penal define el delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la constitución española delito Electrónico "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[4]

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[5]

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos

---

[2] Sarzana, Carlo. "Criminalita e Tecnologia, en computers Crime". Rassagna Penitenziaria e Crimiminologia. Nos. 1-2 Año1. Roma Italia. P. 53

[3] Callegari, Lidia. "Delitos Informáticos y Legislación". En Revista de la Facultad de Derecho y Ciencias Políticasde la Universidad Pontificia Bolivariana. Medellín, Colombia.No70 julio-agosto-septiembre.1985.P115.

4 Lima De La Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

5 Téllez Valdez Julio. *Derecho Informático*. 2ª ED. México. Mc. Graw. Hill 1996 Pp. 103-104

informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador.

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

1.2. Sujeto activo

Las personas que cometen los Delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación labora se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.[6]

Sin embargo, tendiendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco"[7] término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".[8]

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

---

[6] Téllez Valdez Julio**.** *Derecho Informático*. 2ª ED. México. Mc. Graw. Hill 1996 Pp. 103-104

[7] Aniyar De Castro, Lolita. "El delito de cuello blanco en América Latina: una investigación necesaria". Ilanu al DÍA. Año 3 No.8 Agosto 1980. San José, Costa Rica.

[8] Téllez Valdez Julio**.** *Derecho Informático*. 2ª ED. México. Mc. Graw. Hill 1996 Pp. 103-104

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La cifra negra es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.[9]

En este sentido, consideramos que a pesar de que los delitos informáticos no poseen todas las características de los delitos de cuello blanco, si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

1.3. Sujeto pasivo

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas

[9] Del Pont K., et al., ***Delitos de cuello blanco y reacción social*****,** Instituto Nacional de Ciencias Penales. México. 1981

debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables"[10] y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada cifra oculta o cifra negra.

Por lo anterior, se reconoce que "para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, una análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento"[11].

En el mismo sentido, se puede decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas

[10] Bierce, B William. "El delito de violencia tecnológica en la legislación de nueva York" Derecho de la Alta Tecnología. Año 6 No. 66 Febrero 1994. Estados Unidos. P.20.
[11] ***idem.,*** p. 20.

conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las

1.4.- Clasificación

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.[12]

Como instrumento o medio: se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

Como medio y objetivo: en esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber. [13]

Los que utilizan la tecnología electrónica como método;

Los que utilizan la tecnología electrónica como medio;

Los que utilizan la tecnología electrónica como fin.

Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio: son conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

---

12 Téllez Valdez Julio. *Derecho Informático*. 2ª ED. México. Mc. Graw. Hill 1996 Pp. 103-104

13 Lima De La Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100 y 102.

Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

1.5. Tipos de delitos informáticos reconocidos por Naciones Unidas.[14]

1.5.1. Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

La manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de

[14] Naciones Unidas. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos. Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos.43 y 44. Naciones Unidas, Nueva York.1994.

computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica de salchichón en la que rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

1.5.2.- Daños o modificaciones de programas o datos computarizados.

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. las técnicas que permiten cometer sabotajes informáticos son:

Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos. Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente

del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

1.5.3.- Acceso no autorizado a servicios y sistemas informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en

los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

1.5. 4.-Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Una vez conocido las dimensiones reales del problema, su entorno, dimensión, así como el conocimiento de los demás elementos evidenciados en el marco teórico es de manifiesto que es un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos informáticos cometidos implica actividades criminales que no se contemplan en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

II.- TRATAMIENTO INTERNACIONAL DE LOS DELITOS ELECTRONICOS

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de que contribuyan al desarrollo del trabajo.

2.1 Organismos Internacionales

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.[15]

[15] Comisión de las ComunidadeS Europeas. Europa en la vanguardia de la sociedad mundial de la información: plan de actuación móvil, Bruselas, 21.11.1996 COM (96) 607 final.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reformas en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informa de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité Especial de Expertos sobre Delitos relacionados con el empleo de computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989. Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estado pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.[16]

Adicionalmente debe mencionarse que en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, considero que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México y otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del

[16] Comisión de las Comunidades Europea S. Comunicación de la Comisión. Seguimiento del Libro Verde sobre Derechos de Autor y Derechos afines en la sociedad de la información. Bruselas, 20.11.1996 COM (96) 568 Final.

Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal —hasta ese entonces— era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.[17]

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, deben mencionarse la ausencia de la equiparación de

[17] Primer Congreso Internacional de Delitos Cibernéticos. España. 1982

estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, considero que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Asimismo, considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de

acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.[18]

2.2.- Legislación en otros países

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

2.3.- Alemania

En Alemania para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

[18] Comisión de las Comunidades Europeas. Comunicación de la Comisión. Seguimiento del Libro Verde sobre Derechos de Autor y Derechos afines en la sociedad de la información. Bruselas, 20.11.1996 COM (96) 568 Final.

Espionaje de datos (202 a); Estafa informática (263 a); Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273);

Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;

Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa;

Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.[19]

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha

[19] *Idem*.,.1996 COM (96) 568 Final.

castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.[20]

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación a determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistema informáticos. El tipo de daños

[20] Naciones Unidas. " Prevención del delito y justicia penal en el contexto del desarrollo: realidades y perspectivas de la cooperación internacional". Documento de trabajo preparado por la Secretaría (A/CONF. 144/5). Octavo Congreso de las Naciones Unidas sobre Prevención del delito y tratamiento del delincuente. La Habana, Cuba, 27 agosto-7 septiembre 1990.

protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.[21]

2.4.- Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987.

Esta ley contempla los siguientes delitos:

Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

2.5.- Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos (462-2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionario del sistema.

Sabotaje informático (462-3). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de

[21] Naciones Unidas**.** Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990. (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

2.6.- Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas. (18 U.S.C. Sec. 1030 [a][5][A]). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses en su momento, manifestaron que la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Considero importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 dlls por cada persona afectada y hasta $50,000 dlls el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios,

agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir

Por lo anterior se concluye que en el ámbito internacional no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún no existe una definición de carácter universal, esta realidad se convierte en un verdadero obstáculo o limitante, al que hay que vencer, por lo que se recomienda llevar a discusión en un escenario internacional toda la temática vinculada con la actividad de la informática.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse que el papel del Estado, debe ser el principal promotor quien asuma la indelegable regulación de la actividad de control del flujo informativo a través de las redes informáticas; sin que ello implique violación alguna.

Todos estos argumentos deben tomarse en cuenta, pues de ello depende la gran solución que demanda el problema del Estado, en caso general de los países, pero que también debe referirse como materia de importancia a ser tomada para un criterio universal del tema y de sus variaciones

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización

abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores y es ello precisamente lo que justifica la presente apreciación. Los cambios son necesarios impulsarlos desde todos los rincones donde tenga presencia la tecnología, e ir moldeando la concepción que tenga la sociedad en su conjunto, siendo necesario que esta, sepa, identifique, censure, y condene los actos fraudulentos y por ninguna razón considerar a sus ejecutantes como celebridades de la informática

III.- DELITOS INFORMATICOS EN MÉXICO

3.-1 LEGISLACIÓN NACIONAL

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos. En este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

3.2.- Tratado de Libre Comercio de América del Norte (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.[22]

De esta forma, debe mencionarse que los tres Estados que forman parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que

[22] Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993

infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.[23]

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo 2 habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos consten en medios electrónicos o magnéticos.

Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, incluso el comercio de mercancías falsificadas.

El Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta nuestros días.

[23] Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas suscrito por México el 23 de noviembre de 1974, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección u, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias.

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

En este entendido, cabe destacar que el mismo tratamiento que le han conferido esos acuerdos internacionales a las conductas antijurídicas antes mencionadas, es otorgado por la Ley Federal del Derecho de Autor.

3.3.-Derecho de Autor

Ley Federal del derecho de Autor y Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en materia de Fuero Federal.

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados,[24] a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

De esta forma, cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Derecho de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sector denominado "De los delitos en materia de derechos de autor".

[24] Exposición de motivos de la comisión de Justicia de la cámara de Diputados doc.184/LVI/96(I.P.O AÑO III) DICT. durante el análisis de la Ley Federal de derechos de autor

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

En este orden, como se mencionó anteriormente, esta Ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera. En este sentido, consideramos importante detenernos en los artículos 102 y 231 de la presente Ley. El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

Apreciamos que aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

3.4.- Código Penal del Distrito Federal en Materia del Fuero Común

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus.

Entendemos que la redacción de la fracción limita su aplicación, por lo que en el Capítulo IV del presente trabajo, referido a la Propuesta que hacemos sobre el tratamiento de esta problemática en México, sugerimos una nueva redacción para la fracción IV del citado Código Penal, teniendo en cuenta la trascendencia negativa de esta conducta ilícita que amerita un tratamiento más fuerte que el administrativo.

Por otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

Por su parte, el artículo 231, fracción II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

Según nuestra opinión, la redacción de estas fracciones tratan de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses

hasta seis años al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Tal y como hemos sostenido. México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Muchas personas sentirán que el país está ajeno a estas pérdidas por cuanto estas compañías no son mexicanas, sin embargo, si analizamos los sujetos comisores de estos delitos, según la nota de prensa, podríamos sorprendernos al saber que empresas mexicanas como TAESA y Muebles Dico enfrentan juicios administrativos por el uso de programas piratas. [25]

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre los que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y por las implicaciones que traería aparejadas, está totalmente justificada su regulación penal.

En otro orden, el Artículo 109 de la Ley citada, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada

[25] "Incurrieron TAESA y Muebles Dico en delitos informáticos", Iconomia, La Jornada**,** México, sábado 12 de abril de 1997.

que individuos inescrupulosos pueden hacer con esta información. Así, al acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

Asimismo, consideramos que la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

Esta Ley, además establece en el Título X, en su capítulo único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultad para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión “fonogramas, videogramas o libros”, además del verbo “reproducir”, quedando:

Art. 231

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley.

Con las reformas al Código Penal se especifica que:

Art. 424

III. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, videogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos".

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado en el TLC y que por tal razón fue necesaria una segunda modificación, en abril del año en curso para incluir la acción de "reproducción".

De igual forma el artículo 424 que había sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril pasado para incluir la reproducción y su comisión en una forma dolosa.

Las respuestas o soluciones aquí planteados debe provenir de diferentes medios, unos de ellos es el tecnológico (medio originario del problema), alcanzable solo con la avanzada vanguardista, de ella han surgido algunas técnicas que minimizan las posibilidades de fraude en el medio informático a la actividad comercial.

El desarrollo tan amplio de las tecnologías informáticas, ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que asta ahora no era posible imaginar. El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de los sistemas

Por lo que se asume, que no es fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contemplados en textos jurídicos penales, se requiere que la expresión delitos informáticos consignada en los códigos penales, al igual que en otros muchos no ha sido objeto de tipificación aún.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Por lo que debe destacarse que el papel del Estado, debe ser el principal promotor quien asuma la indelegable regulación de la actividad de control del flujo informativo a través de las redes informáticas; sin que ello implique violación alguna.

El aspecto legal debe ser asumido por los países como un factor de importancia capital, entendiéndose la materia como de especial tratamiento dada las características que imprime el comportamiento tecnológico. La Sociedad en su conjunto, ha de hacer sus propias aportaciones en el sentido de no fomentar los procesos que conllevan a la materialización de los delitos vinculados a la informática, entender que como sociedad creciente se debe rescatar los principios rectores que hace posible la constitución de la sociedad misma.

Debe ser el Estado el primer impulsor de los cambios requeridos para dar la batalla en todos sus espacios, la minimización de los problemas vinculados tendrían un mayor control si se llegara a unificar todas las leyes de los distintos países lo cual impide que queden brechas abiertas para el comedimiento de los ya referidos delitos

Sobre el particular, por considerar de gran interés y la complejidad del tema en estos tiempos exige una reforma al ordenamiento Penal del Estado de Baja California con el objeto de tíficas estas conductas como delitos y determinar las sanciones que resulten mas efectivas para evitar su comisión

CONCLUSIONES

Una vez conocidas las dimensiones reales del problema, su entorno, dimensión, así como el conocimiento de los demás elementos evidenciados en el marco teórico concluir con aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos informático cometidos esto implica actividades criminales que no se contemplan en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

Es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países (no contemplados en el caso Venezolano), que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática. Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Un elemento o factor a ser considerado para ello es que no se puede pretender legislar una materia cuya dimensiones son tan dinámicas y cambiantes como la tecnología con leyes estáticas, cuyos cambios al momento de su llegada como instrumento regulador ya es tardío, y más aún, a sabiendas que jamás estarán a la par, ya que la ley tiene un espacio en el cual mantenerse para poder ser aplicada y la tecnología no, lo cual obliga una revisión del marco legal en forma periódica sin dejar que la tecnología por su parte la convierta en obsoleta.

En el ámbito internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del

tema, y aún no existe una definición de carácter universal, esta realidad se convierte en un verdadero obstáculo o limitante, al que hay que vencer, por lo que se recomienda llevar a discusión en un escenario internacional toda la temática vinculada con la actividad de la informática.

Se asume que, no es fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contemplados en textos jurídicos penales, se requiere que la expresión delitos informáticos consignada en los códigos penales, al igual que en otros muchos no ha sido objeto de tipificación aún.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse que el papel del Estado, debe ser el principal promotor quien asuma la indelegable regulación de la actividad de control del flujo informativo a través de las redes informáticas; sin que ello implique violación alguna.

Todos estos argumentos deben tomarse en cuenta, pues de ello depende la gran solución que demanda el problema del Estado, en caso general de los países, pero que también debe referirse como materia de importancia a ser tomada para un criterio universal del tema y de sus variaciones materializadas en los fraudes del comercio en la Red.

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores y es ello precisamente lo que justifica la presente apreciación. Los cambios son necesarios impulsarlos desde todos los rincones donde

tenga presencia la tecnología, e ir moldeando la concepción que tenga la sociedad en su conjunto, siendo necesario que esta, sepa, identifique, censure, y condene los actos fraudulentos y por ninguna razón considerar a sus ejecutantes como celebridades de la informática.

Las respuestas o soluciones aquí planteados debe provenir de diferentes medios, unos de ellos es el tecnológico (medio originario del problema), alcanzable solo con la avanzada vanguardista, de ella han surgido algunas técnicas que minimizan las posibilidades de fraude en el medio informático a la actividad comercial.

El desarrollo tan amplio de las tecnologías informáticas, ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que asta ahora no era posible imaginar. El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de los sistemas informáticos lo que a propiciado a su vez la necesidad de regulación por parte los legisladores.

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos de esta ley, se dijo que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultan mas efectivas para evitar su comisión, considerándose que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de derecho de reforma al código penal para el distrito federal en materia de fuero federal, proponiendo la adición de un titulo vigésimo sector denominado de los delitos en materia de derechos de autor.

Al respecto, se considero conveniente la inclusión de la materia en el ordenamiento penal, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas otro en un instrumento mas adecuados para la procuración y la administración de justicia, al poderse disponer de los delitos y en su resolución, del instrumento general que orienta ambas funciones publicas.

En este orden como se menciona anteriormente esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y los derechos autorales relacionados con ambos. Define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento cosas en las que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privada a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación publica, y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas las bases de datos, etcétera.

Para el presente trabajo, consideramos importante analizar los artículos 102 y 103 de la presente Ley Federal del Derecho de Autor. El primero de ellos regula la protección de los programas de computación y señales además que tengan por efecto causar algo nocivo a otros programas o equipos, lógicamente no serán protegidos. El segundo de su fracción V sanciona al comercio de programas de dispositivos electrónicos de protección de un programa de cómputo.

Apreciamos que aun cuando la infracción se circunscribe al área del comercio, permite la regulación permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

Por otra parte la Ley en comento en su articulo 215 hace una remisión del titulo vigésimo sexto, articulo 424 fracción IV del código penal para el Distrito Federal en Materia de Fuero Común y para toda la republica en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus.

Considero que la redacción de esta fracción limita su aplicación, es por ello que una de las razones que mediante el presente trabajo se propongan algunas reformas al Código Penal del Estado de Baja California, tomando en cuenta la trascendencia negativa de esta conducta ilícita que amerita un tratamiento mas fuerte que el administrativo.

El articulo 231, fracción II y VII de la multicitada Ley contemplan dentro de las infecciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por la Ley" y " usar, producir o explotar una reserva de derechos protegidos o un programa de computo sin el consentimiento del titular".

Según nuestra opinión, la redacción de esta función tratan de evitar la llamada piratería de programas en el área de comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Es así que la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su articulo 215 al titulo vigésimo sexto del Código Penal Federal, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses asta seis años al que incurra en este tipo de delitos.

Sin embargo, como esta regulación básicamente no completaba el delito informático como tal, sino que se concretaba a la protección de los derechos autorales y de propiedad industrial, con fecha 17 de mayo de 1999, fue publicada la adicción de un titulo noveno al segundo libro del Código Penal Federal denominado: "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática".

La acción en comento tiene como objeto sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la perdida de información que contengan.

Algunos estados de la republica, concientes de la necesidad de legislar en esta materia han adoptado en sus ordenamientos penales normas tendientes a la protección de la información; tal es el caso de Sinaloa, que tipifica el delito informático, o mórelos y tabasco, que protegen la información mediante la tipificación de la violación a la entidad personal.

En este entendido, considero que la gravedad de la consulta licita en si, y por las implicaciones que traería aparejadas, esta totalmente justificada su regulación penal.

De esta manera y con el objeto de tipificar el delito informático en el código punitivo del Estado, fortaleciendo las tecnologías informáticas en la entidad, regulando penalmente en aquellas actitudes antijurídicas para evitar su impunidad, se propone la adicción al código penal para el estado de Baja California, de un titulo séptimo denominado "uso indebido de sistemas informáticos", con un capitulo único y el articulo 357, para quedar como sigue:

TITULO SEPTIMO

USO INDEVIDO DE SISTEMAS INFORMATICOS

CAPITULO UNICO

ARTUCULO 357 *tipo y punibilidad* se impondrá una pena de uno o tres años de prisión y de noventa a trescientos días de multa, a la persona que dolosamente y sin derecho :

I- 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 fraudar, obtener dinero, bienes o información; o

II- intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de cómputo, los datos contenidos en la misma en la base, sistema o red.

TRANSITORIO

UNICO- las presentes reformas entraran en vigor el día siguiente de su publicación en el periódico oficial del estado

Para concluir con este tema de gran interés y de preocupación, se puede señalar que dado el carácter tan complicado de los delitos informáticos, es conveniente establecer acuerdos de ayuda mutua entre el Gobierno Federal y la Entidades Federativas, que permitan fijar un mecanismo para contrarrestar eficaz y eficientemente el uso indebido de sistemas informáticos, y evitar un conflicto entre la jurisdicción Federal y local.

BIBLIOGRAFÍA

LIBROS

Del Pont K., Luis Marco y Nadelsticher Mitrania, Abraham, *Delitos de cuello blanco y reacción social,* Instituto Nacional de Ciencias Penales. México. 1981.
Téllez Valdés, Julio. *Derecho Informático*. 2a. ed. México. Ed. Mc Graw Hill 1996. Pp. 103-104.

REVISTAS

Aniyar De Castro, Lolita. "El delito de cuello blanco en América Latina: una investigación necesaria". ILANUD AL DÍA. Año 3 No.8 Agosto 1980. San José, Costa Rica.

Bierce, B William. "El delito de violencia tecnológica en la legislación de nueva York" Derecho de la Alta Tecnología. Año 6 No. 66 Febrero 1994. Estados Unidos. P.20.

Callegari, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. P.115.

Lima de la Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

Sarzana, Carlo. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53.

Comisión de las Comunidades Europeas. Europa en la vanguardia de la sociedad mundial de la información: plan de actuación móvil, Bruselas, 21.11.1996 COM (96) 607 final.

Comisión de las Comunidades Europeas. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

Comisión de las Comunidades Europeas. Comunicación de la Comisión. Seguimiento del Libro Verde sobre Derechos de Autor y Derechos afines en la sociedad de la información. Bruselas, 20.11.1996 COM (96) 568 FINAL.

Naciones Unidas. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos. Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos.43 y 44. Naciones Unidas, Nueva York.1994.

Naciones Unidas. Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990. (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

Naciones Unidas. "Prevención del delito y justicia penal en el contexto del desarrollo: realidades y perspectivas de la cooperación internacional". Documento de trabajo preparado por la Secretaría (A/CONF. 144/5). Octavo Congreso de las Naciones Unidas sobre Prevención del delito y tratamiento del delincuente. La Habana, Cuba, 27 agosto-7 septiembre 1990.

Primer Congreso Internacional de Delitos Cibernéticos. España. 1982.

Hemerografía

Iconomia, "Incurrieron TAESA y Muebles Dico en delitos informáticos", La Jornada, México, sábado 12 de abril de 1997.

LEGISLACIÓN

Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993, México.

Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Contiene las reformas conocidas hasta el 20 de enero de 1997. Editores Greca. Tercera Edición. 1996, México.

Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Editorial Porrúa. 19 edición. México 1995.

Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996.

Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México, D.F.

Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 184/LVI/96 (I. P.O. Año III) DICT. durante el análisis de la Ley Federal de Derecho de Autor, México.