

## DELITOS INFORMÁTICOS

ESTRADA GARAVILLA MIGUEL

*[Referencia bibliográfica: Universidad Abierta  
<http://www.universidadabierta.edu.mx>]*

### PRÓLOGO

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee, un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos. Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama del este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los microprocesadores de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso, sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad. Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización de Cooperación y Desarrollo Económico (OCDE) a París, Francia, 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 el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

En la actualidad la informatización 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.

El espectacular desarrollo de 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. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

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, fraudes, 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.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, se han transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden para 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 el casuismo.

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 proporcionar datos e informaciones sobre miles de personas, físicas y morales, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales 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; no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento de ello por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está 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.

## **INTRODUCCIÓN**

Mucho se ha demostrado acerca de los beneficios que los medios tecnológicos y el uso de la informática en particular aportan a la sociedad actual. Es indudable que la vertiginosidad del progreso no se presentaría si no intervinieran de manera directa los elementos electrónicos con los que contamos hoy en día. Sin embargo, la utilización de dichos medios informáticos, al ser destinados al servicio de la sociedad, requieren de una inminente regulación jurídica con respecto a su utilización. El objetivo de este trabajo es analizar las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades, sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese entendido, el presente trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos alcance en México los niveles de peligrosidad que se han registrado en otros países.

Durante la etapa de investigación se encontró que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etc., dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones, las que se han recogido en la primera parte de este trabajo. Además se han señalado los sujetos activos y pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.

Seguidamente, se presenta un estudio comparativo de la problemática de los delitos informáticos en países tanto de Europa como de América, donde mayor incidencia ha tenido este fenómeno, el tratamiento penal que algunos gobiernos le han dado, y la parcial inercia que otros han mantenido sobre el tema, lo que se ha traducido en proyectos que hasta el momento no han fructificado.

A continuación analizamos la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello se estudian los antecedentes que han tenido las regulaciones vigentes en esta materia: Acuerdos celebrados en el marco del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) y El Tratado de Libre Comercio de América del Norte (TLC).

Seguidamente se enuncia el tratamiento administrativo que se realiza a través de la Ley Federal del Derecho de Autor, y en el penal que se ha establecido en el Título Vigésimo Sexto del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Sobre el particular, debe aclararse que esta ley no regula delitos informáticos ya que su competencia es la de sancionar administrativamente conductas ilícitas cuyo bien jurídico a tutelar es la propiedad intelectual.

Para finalizar se incluye una propuesta, sustentada en el estudio comparativo antes mencionado, que trata de adecuar a la realidad existente en México, pero previendo que nuestro país no está exento de la velocidad del desarrollo tecnológico y de los vicios que éste genera.

## **CONCEPTO DE DELITO INFORMÁTICO**

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 robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. 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".

Para Carlos Sarzana, en su obra *Criminalita e Tecnología*, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo define al 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".

María de la Luz Lima dice que el 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 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".

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".

Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

- a) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- j) Ofrecen facilidades para su comisión a los menores de edad.
- k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

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

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

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.

## **CARACTERÍSTICAS DEL 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 laboral 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 delitos 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 informático es tema de controversia ya que para algunos el nivel de habilidades 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.

Sin embargo, teniendo 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, término introducido por primera vez por el criminólogo 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 de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

Asimismo, este criminólogo estadounidense dice que tanto la definición de los delitos informáticos como la 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. Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil 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 tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

## **CARACTERÍSTICAS DEL SUJETO PASIVO**

En primer término tenemos que distinguir que sujeto pasivo ó 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, etc., 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, 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 descubiertos o no son denunciados a las autoridades responsables 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 aplicar el 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 mantengan 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, un 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.

En el mismo sentido, podemos 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 e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe 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 autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

## **CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS**

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

Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
- b) Variación de los activos y pasivos en la situación contable de las empresas.
- c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).
- d) Lectura, sustracción o copiado de información confidencial.
- e) Modificación de datos tanto en la entrada como en la salida.
- f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- h) Uso no autorizado de programas de computo.
- i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- l) Acceso a áreas informatizadas en forma no autorizada.
- m) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo: en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- a) Programación de instrucciones que producen un bloqueo total al sistema.
- b) Destrucción de programas por cualquier método.
- c) Daño a los dispositivos de almacenamiento.
- d) atentado físico contra la máquina o sus accesorios.
- e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

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

a) Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b) Los que utilizan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

c) Los que utilizan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

En lo que se refiere a delitos informáticos, Olivier Hance en su libro *Leyes y Negocios en Internet*, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a) Acceso no autorizado: es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

b) Actos dañinos o circulación de material dañino: una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

c) Interceptación no autorizada: en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

d) Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

## **TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)**

A. Fraudes cometidos mediante manipulación de computadoras.

a) 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.

b) 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 tienen 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.

c) 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 equipos y programas de computadora especializados



para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

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

#### B. Falsificaciones informáticas.

a) Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

b) 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.

#### C. Daños o modificaciones de programas o datos computarizados.

a) 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:

i) 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.

ii) Gusanos: se fabrica de 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 eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

iii) 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 en donde se halla la bomba.

b) Acceso no autorizado a servicios y sistemas informáticos: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

i) Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. 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.

c) Reproducción no autorizada de programas informáticos de protección legal: ésta 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. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- a) Acceso no autorizado: uso ilegítimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.
- b) Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- c) Infracción al copyright de bases de datos: uso no autorizado de información almacenada en una base de datos.
- d) Interceptación de correo electrónico: lectura de un mensaje electrónico ajeno.
- e) Estafas electrónicas: a través de compras realizadas haciendo uso de la red.
- f) Transferencias de fondos: engaños en la realización de actividades bancarias electrónicas.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- a) Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- b) Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- c) Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- d) Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

## **POSTURA DE DIVERSOS ORGANISMOS INTERNACIONALES EN MATERIA DE REGULACIÓN INFORMÁTICA**

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de incorporar a la vida jurídica la regulación de dichas conductas.

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 las leyes derechos penales nacionales.

En un primer término, debe considerarse que en 1983, la 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 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.

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 reforma 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) como espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora 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 informe 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 las 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 se "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 Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, 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.

En este contexto, se considera 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 u 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 mundial, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del 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 de 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.

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- d) No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- e) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- f) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Teniendo presente esa situación, 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 Wurzburg, Alemania, 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.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede 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, se 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.

En general, se ha pretendido contribuir mediante recomendaciones a la uniformidad de las normas que sancionan los delitos informáticos en el ámbito internacional, sin dejar de observar la tradición jurídica de cada país.

## **LEGISLACIÓN EN OTROS PAÍSES RELACIONADA CON LOS DELITOS INFORMÁTICOS Y CONDUCTAS SUPLEMENTARIAS**

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.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

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. Éstas 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 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:

### **A. 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:

- a) Espionaje de datos (202 a).
- b) Estafa informática (263 a).
- c) 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).

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

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

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

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.

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

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 de 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 sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

## **B. Austria.**

La Ley de Reforma del Código Penal de 22 de diciembre de 1987 contempla los siguientes delitos:

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

b) 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 o por

actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

### **C. Francia.**

La Ley Número 88-19 de 5 de enero de 1988, sobre el fraude informático, menciona lo siguiente:

- a) 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 funcionamiento del sistema.
- b) Sabotaje informático (462-3): en este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- c) 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 tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.
- d) 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.
- e) 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.

### **D. Gran Bretaña.**

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado hasta con cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

### **E. Holanda.**

El 1 de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

### **F. España.**

En el Nuevo Código Penal de España, el art. 263 señala que se impondrá sanción a quien causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El Nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (violación de secretos, espionaje, divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa, y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el Nuevo Código Penal de España, en su artículo 248, sólo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

#### **G. Chile.**

Chile fue el primer país latinoamericano en sancionar una Ley Contra Delitos Informáticos, la cual entró en vigencia el 7 de junio de 1993. Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1 el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta sea tendiente a impedir, obstaculizar o modificar su funcionamiento. En tanto, el Art. 3 tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

#### **H. 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 al 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, etc., y en qué difieren de los virus, la nueva ley sanciona la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, 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 diez 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.

Dicha ley aclara que el creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar causaría daño a alguien o que él solo quería enviar un mensaje. Con esta inclusión se elimina la concepción de que el sujeto activo debía poseer conocimientos superiores para la realización de estos actos.

En opinión de los legisladores estadounidenses, 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 intimidación que constituyen el objetivo principal de esta Ley. Sin embargo es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en las que, entre otras, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de diez mil dólares por cada persona afectada y hasta cincuenta mil dólares el acceso imprudencial a una base de datos.



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 dependencias relacionadas con el Estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Cabe mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos, 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 datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

En el presente capítulo se han dejado fuera muchos países que en la actualidad regulan las actividades informáticas en sus respectivas legislaciones, sin embargo se han mencionado las naciones que se mostraron más interesadas en incluir de una manera pronta dichos términos y conductas en sus ordenamientos legales.

## **LEGISLACIÓN NACIONAL EN MATERIA DE DELITOS INFORMÁTICOS**

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, es 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.

## **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 Sexta 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.

De esta forma, debe mencionarse que los tres Estados 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 infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

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 denominado 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, 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 éstos consten en medios electrónicos o magnéticos.

En resumen, las provisiones insertas en el articulado del TLC se ocupan básicamente de la protección a la propiedad intelectual, dejando a las legislaciones de cada país las sanciones a los delitos que se desprendan de las acciones contra los mencionados derechos.

## **ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO**

Al inicializar el contenido de este apartado, debemos aclarar que si bien la institución del GATT se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.

En este entendido, cabe mencionar que 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.

Es de 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, 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 5, 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 que a continuación se analiza.

## **LEY FEDERAL DEL DERECHO DE AUTOR Y CÓDIGO PENAL PARA EL DISTRITO FEDERAL EN MATERIA DE FUERO COMÚN Y PARA TODA LA REPUBLICA 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, 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.

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 Decreto de Reforma al Código Penal para el Distrito Federal y para toda la República en Materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los Delitos en Materia 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, etc.

En este sentido, importante analizar los artículos 102 y 231. 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.

Se aprecia 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.

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 virus.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un delito informático debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etc.

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, fracciones 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".

La redacción de estas fracciones trata 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 trescientos a tres 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 se ha sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Constantemente la prensa publica informes sobre las pérdidas que sufren las compañías fabricantes de programas informáticos, las que se remontaban a sumas que alcanzan cifras de varios 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 prensa, podríamos sorprendernos al saber que empresas mexicanas enfrentan juicios administrativos por el uso de programas piratas.

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las 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 las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información. Asimismo, 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.

Por lo anterior, el análisis de este artículo corrobora la posición que aquí se ha sostenido respecto a que en las conductas ilícitas relacionadas con la informática el bien jurídico a tutelar no es únicamente la propiedad intelectual sino la intimidad por lo que este artículo no debería formar parte de una ley de derechos de autor sino de una legislación especial tal y como se ha hecho en otros países.

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 facultado 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 Federal del Derecho de Autor 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, 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 para incluir la reproducción y su comisión en una forma dolosa.

## **CÓDIGO PENAL DEL ESTADO DE SINALOA**

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

"Título Décimo

Delitos contra el patrimonio

Capítulo V

Delito Informático.

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa".

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Es claro que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

## CONCLUSIONES

Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, 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 (microprocesadores, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

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 el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

## PROPUESTA

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, es necesario a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países, regular penalmente las conductas ilícitas derivadas del uso de la computadora.

En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, se sugiere que en el Título Vigésimo Segundo sobre los Delitos en Contra de las Personas en su Patrimonio del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal se añada un capítulo especial para los delitos informáticos.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, se establece que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste, con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

## AUTOEVALUACIÓN

1. ¿Cómo se ha tratado de encuadrar al delito informático?

2. ¿Qué comenta Julio Téllez Valdés con respecto a la elaboración de la definición de los delitos informáticos?
3. ¿Qué comprenden para Carlos Sarzana los crímenes por computadora?
4. ¿Cómo define Nidia Callegari al delito informático?
5. ¿Qué es para Rafael Fernández Calvo el delito informático?
6. ¿Cómo describe María de la Luz Lima al delito electrónico?
7. ¿Cómo conceptualiza Julio Téllez Valdés al delito informático?
8. Mencionar algunas de las características principales de las conductas que señala Julio Téllez Valdés.
9. ¿Cuáles son las características más relevantes de los sujetos activos de los delitos informáticos?
10. ¿Cuáles son las características que dan origen a la comparación de los delitos informáticos con los delitos de cuello blanco?
11. ¿Qué comenta Edwin Sutherland respecto a las definiciones de delitos informáticos y delitos de cuello blanco?
12. ¿Qué es el sujeto pasivo en acto delictivo informático?
13. ¿Cómo clasifica Julio Téllez Valdés a los delitos informáticos?
14. ¿Cuáles son las tres categorías que señala María de la Luz Lima de los delitos electrónicos?
15. En lo que se refiere a delitos informáticos, Olivier Hance considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos, ¿cuáles son éstas?
16. ¿Cuáles son los fraudes cometidos mediante manipulación de computadoras?
17. ¿Cómo pueden ser las falsificaciones informáticas?
18. Enunciar los tipos de daños o modificaciones de programas o datos computarizados.
19. Enunciar otros tipos de delitos que se pueden dar por medio de sistemas informáticos.
20. ¿Cuáles han sido las iniciativas que ha tomado la Organización de Cooperación y Desarrollo Económico (OCDE) en materia de delitos informáticos?
21. ¿Qué recomendaciones emitió la Asociación Internacional de Derecho Penal en 1992 respecto a los delitos informáticos?
22. ¿Qué señala el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos?
23. Resumir los delitos que ha contemplado Alemania en su legislación penal.
24. ¿Qué delitos se han tipificado en el Código Penal de Austria?
25. ¿Qué aspectos regula la Ley 88-19 de Francia en relación al fraude informático?
26. ¿Cuál es el cambio más importante que se registra en el Acta Federal de Abuso Computacional?

27. ¿Qué tratamiento le otorga el Tratado de Libre Comercio de América del Norte (TLC) a los delitos informáticos?

28. ¿Cómo se entiende al delito informático en la Ley Federal del Derecho de Autor y el Código Penal para el Distrito Federal y para toda la República en Materia de Fuero Federal?

29. ¿Por qué es relevante el Código Penal del Estado de Sinaloa en materia de informática?

## **BIBLIOGRAFÍA**

### **LIBROS**

Del Pont K., Luis Marco y Nadelsticher Mitrana, Abraham. Delitos de Cuello Blanco y Reacción Social. Instituto Nacional de Ciencias Penales. México. 1981.

Hance, Olivier. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.

Mir Puig, S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.

Téllez Valdés, Julio. Derecho Informático. 2ª. ed. México. Mc Graw Hill 1996. Pp.103-104.

Zavala, Antelmo. El Impacto Social de la Informática Jurídica en México. Tesis. México. UNAM. 1996.

Amoroso Fernández, Yarina. La informática como objeto de derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados en Revista Cubana de Derecho. Unión Nacional de Juristas de Cuba. No. 1. Habana, Cuba. 1991. P.43.

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.

Artega S., Alberto. El delito informático: algunas consideraciones jurídico penales Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela. P. 125-133.

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.

De La Cuadra, Enrique. Regulación Jurídica de la Informática Computacional. Temas De Derecho. Año li No. 3, 1987. Universidad Gabriela Mistral. Santiago De Chile, P. 1-4.

Fernández Calvo, Rafael. El Tratamiento del Llamado "Delito Informático" En el Proyecto de Ley Orgánico del Código Penal: Reflexiones y Propuestas de la Cli (Comisión de Libertades e Informática) En Informática y Derecho. Pp.1150. Pendiente

Garvarino, Alvaro, Curvelo, Carmelo, Et Al. Nuevas Normas Jurídicas en Materia Informática. Revista de la Asociación de Escribanos del Uruguay. Vol. 76 No. 1 - 6. Enero-Junio 1990. Montevideo, Uruguay. P. 68-78.

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

Losano, G., Mario. Anteproyecto de Ley Colombiana De 1987. Una Propuesta de Ley Sobre La Privacy en la República de Colombia. Cuadernos y Debates. No. 21. Colombia. P. 97- 131.



Sarzana, Carlo. Criminalità E Tecnologia En Computers Crime. Rassagna Penitenziaria E Criminologia. Nos. 1-2. Ano 1. 1979. Roma,Italia. P.53

Swanson, R y Territo, Leonard. Computer Crime: Dimensions, Types, Causes, and Investigation Journal Of Police Sciencie and Administration. International Association of Chiefs of Police. Vol. 8, Number 3, September 1980.

Toniatti, Roberto. Libertad Informática y Derecho a la Protección De Los Datos Personales: Principios de Legislación Comparada. Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, España. P.139 -162.

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.

## **HEMEROGRAFIA**

"Tratado de Libre Comercio", Novedades, México, jueves 20 de agosto de 1992.

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

"Tarjetas: súper fraudes". El Sol de México Mediodía. México, lunes 21 de abril de 1997. Primera plana.

"Aprobó el Senado reformas a la Ley sobre Derechos de Autor y el Código Penal", El Universal, México, martes 29 de abril de 1997.

## **LEGISLACIÓN**

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

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. Greca. Tercera Edición. 1996.

Ley de Vías Generales de Comunicación. Colección Porrúa. Porrúa. 23ª edición. México.1993.

Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Porrúa. 19ª 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. 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.

Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc.223/LVI/97 (II. P.O. Año III) DICT. que contiene el proyecto de decreto por el que se reforman la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.

## **BIBLIOTECAS**

New York City Public Library, New York, New York.

New York University School of Law Library, New York, New York.

United Nations Research Center and Library, New York, New York.

Seton Hall University School of Law, Newark, New Jersey.

Legal Research Center of Scarinci & Hollenbeck, LLC, Secaucus, New Jersey.

Website de la Cámara de Representantes del Congreso Norteamericano.

Website de la Biblioteca del Congreso de los Estados Unidos de América.

Website del Instituto de Investigaciones Jurídicas de la UNAM.