UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

"DELITOS INFORMATICOS"

TESIS

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

PRESENTA:

JORGE REYES LEO

Director de Tesis:
LIC. MIGUEL ANGEL GORDILLO GORDILLO

Revisor de Tesis:
LIC. HECTOR MANUEL ESTEVA DIAZ

BOCA DEL RIO, VER. 2005

DEDICATORIAS

A MI PADRE

"Por ser mi inspiración en la vida y de tener el privilegio de ser tu hijo"

Gracias Papá
Te quiero muchísimo

A MI MADRE

"Por ser la que me trajo al mundo y enseñarme los valores de la vida"

Gracias Mamá
Te quiero muchísimo

A MI HERMANA

"Por ser en todo momento la persona mas comprensible y cariñosa del mundo y que en todo momento me apoyó"

Gracias Pau
Te quiero como a nadie

A MIS ABUELITOS

"Gracias por todo lo que me han dado y el cariño con el que me corresponden"

Los quiero muchísimo
Papito y Mamita

INDICE

INTRODUCCIÓN

Mucho se habla de los beneficios que los medios de comunicación y el uso de la Informática han aportado a la sociedad actual, pero el objetivo de nuestro trabajo será analizar la otra cara de la moneda, o sea, 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 aquella.1 En ese entendido, nuestro trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que consideramos 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 dado en otros países.

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

Seguidamente, realizamos un estudio comparativo de la problemática de los delitos informáticos en los 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 estudiamos los antecedentes que a nuestro juicio han tenidos las regulaciones vigentes en esta materia.

Después nos detenemos tanto en el tratamiento administrativo, como en el penal que se ha establecido en los Códigos Penales en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

Para finalizar el presente trabajo, hacemos algunas consideraciones sustentadas en el estudio comparativo antes mencionado, que tratamos de adecuar a la realidad existente en México, pero previendo que no estamos exentos de la velocidad del desarrollo tecnológico y de las exageraciones que éste genera.

CAPITULO I

METODOLOGÍA DE LA INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad la búsqueda por encontrar recursos más eficientes para combatir las diversas figuras delictivas que se presenten por la implantación del Internet, desde la década de los 90, como nuevos retos jurídicos. La inicial desregulación del ciberespacio, como nuevo medio de comunicación, será uno de los motivos que favorezca, el alarmante incremento de los casos de delitos informáticos que se han ido desarrollando en nuestro país.

El uso frecuente de computadoras y de la posibilidad de su interconexión a nivel global da lugar a un verdadero fenómeno de nuevas dimensiones denominado: *El Delito Informático.* Como respuesta a esta necesidad surge el

estudio de que no estamos, exclusivamente, ante un delito material de información relacionado con un determinado contenido ilícito, sino que, a menudo, está vinculado a la delincuencia organizada tanto internacional como nacional.

En la legislación Penal para el Estado de Veracruz que en su artículo 181 que manifiesta los delitos informáticos, los maneja en forma general, en la cual las sanciones no son muy severas, y en consideración se debe incrementar la penalidad de esta figura delictiva.

Es por ello que surge el interés por plantear *si la tipificación de los delitos informáticos es suficiente para prevenir y combatir las conductas ilícitas que se derivan de este en sus diferentes modalidades.*

1.2 JUSTIFICACIÒN

Para la ciencia jurídica y el derecho penal es un delito moderno, por ello manifiesta conductas antes no establecidas en las legislaciones del país, por lo cual se necesita aportaciones de la tecnología actual para la comprobación de diversas actividades que se realizan, y de bases e información de los países que tienen conocimiento pleno de este ilícito para poder enfrentarlo en situaciones que se lleven a cabo.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Determinar si la tipificación de los delitos informáticos es suficiente para prevenir y combatir las conductas ilícitas que se derivan de este en sus diferentes modalidades.

1.3.2 OBJETIVOS ESPECÍFICOS

- Conocimiento de una ciencia nueva para el derecho mexicano.
- Realizar investigaciones sobre la tecnología del medio informático.
- Establecer sanciones mayores de acuerdo con la conducta presentada

1.4 FORMULACION DE HIPOTESIS

- La tipificación de los delitos informáticos es suficiente para prevenir y combatir las conductas ilícitas que se derivan de este en sus diferentes modalidades.
- La tipificación de los delitos informáticos no es suficiente para prevenir y combatir las conductas ilícitas que se derivan de este en sus diferentes modalidades.

- La tipificación de los delitos informáticos debe manifestar mayores sanciones y estudios para prevenir y combatir las conductas ilícitas que se derivan de este en sus diferentes modalidades.

1.5 DETERMINACIÓN DE VARIABLES

1.5.1. VARIABLE DEPENDIENTE

Conductas ilícitas que se derivan en sus diferentes modalidades.

1.5.2. VARIABLE INDEPENDIENTE

Tipificación de los delitos informáticos

1.6 TIPO DE ESTUDIO

1.6.1 INVESTIGACION DOCUMENTAL

Para elaborar el trabajo de investigación, se consultaron libros, textos, revistas, artículos necesarios para fundamentar el presente estudio.

1.6.1.1 BIBLIOTECAS PUBLICAS

Unidad de Servicios Bibliotecarios y de Información de la Universidad Veracruzana (USBI) ubicada en la Avenida Ruiz Cortínes y Juan Pablo II en la localidad del Municipio de Boca del Río, Estado de Veracruz.

1.6.1.2 BIBLIOTECAS PRIVADAS

Biblioteca de la Universidad Autónoma de Veracruz – Villa Rica ubicada en la calle Urano esquina Progreso, Ylang Ylang en la localidad del Municipio de Boca del Río, Estado de Veracruz.

1.6.1.3 BIBLIOTECAS PARTICULARES

Biblioteca del Bufete Corporativo Reyes Peralta y Reyes Leo ubicada en la calle de Ocampo 234 Despacho 127 entre Independencia y 5 de Mayo en la localidad del Municipio de Veracruz, Estado de Veracruz.

1.6.2 TECNICAS EMPLEADAS

Se recopiló la información de todo lo consultado a través de diversas fichas bibliográficas y de trabajo.

1.6.2.1 FICHAS BIBLIOGRAFICAS

Se estructuraron las fichas bibliográficas, cumpliendo con todos los requisitos metodológicos aplicables, que son:

1. Nombre del autor
2. Titulo del libro
3. Edición
4. Editorial
5. Lugar y fecha de edición

1.6.2.2 FICHAS DE TRABAJO

Se redactaron las fichas de trabajo necesarias, cumpliendo los requisitos metodológicos sugeridos.

CAPITULO II

ANTECEDENTES DE LA INFORMATICA

2.1. CONCEPTO DE DELITOS INFORMATICOS

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

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

Para Carlos Sarzana, en su obra Criminalista de tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción criminal, como mero símbolo".[2]

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

---

1 Téllez Valdés, Julio, *Derecho Informático*. 2ª. ed., México, McGraw Hill, 1995, p.283.
2 Sarzana, Carlos, *Criminalista e Tecnología*, 1ª. ed., Gennaio-Giugno, 1979, Roma, Italia, p.59.
3 Callegari, Nidia., *Delitos Informáticos y Legislación en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Boliviana*. Medellín, Colombia. No. 70 Julio-Agosto-Septiembre. P.115.

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".[4]

María de la Luz Lima dice que el "delito Electrónico" "en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[5]

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

---

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. p.125

5 Lima De La Luz, María. *Delitos Electrónicos en Criminalia.* México. Academia Mexicana de Ciencias Penales. Porrúa. . No. 1-6. Año L. Enero-Junio 1984. p.56

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

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

Sin embargo, tendiendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano *Edwin Sutherland* en el año de 1943.[6]

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la

6 Sutherland Edwin, *El Delito de Cuello Blanco*, 5ª. Edición, E.U.A., Junio 2000, p.234

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

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

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

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

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte

de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

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

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 y la 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, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.[7]

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

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

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

Los que utilizan la tecnología electrónica como método;
Los que utilizan la tecnología electrónica como medio; y
Los que utilizan la tecnología electrónica como fin.

---

7 Tellez Valdez, Julio, *Derecho Informático.* 2ª ed., México, McGraw Hill, 1995, p.283

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

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

Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.[8]

2.1.1. DESARROLLO INFORMATICO

Internet surge desde los años 60's dentro del ejército norteamericano, como un proyecto, dentro del área de defensa para crear un sistema de información imposible de destruir debido a su complexión: intangible.

Antes de 1991 Internet era exclusivo del gobierno norteamericano y de instituciones educativas. En 1991 se fundo la asociación de intercambio comercial de Internet (CIX), con el objetivo de proveer una "carretera libre de barreras" para empresas y personas de todo tipo.

---

8 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

A pesar de que Internet fue creado para ayudar a la milicia y a la investigación educacional ahora Internet esta constituida por 21,000 redes de información, 15 millones de usuarios, 2 millones de computadoras, con un crecimiento del 7 al 10% mensual.

Internet no es algo tangible ni una organización. Nadie es su dueño, nadie la corre. Simplemente Internet es una telaraña de computadoras interconectadas que tomado forma con muy poco planteamiento.

Pero Internet es más que una simple conexión de computadoras y cables, es una comunidad mundial de personas que comparten una gran variedad de intereses y necesidades.

2.1.2. INFORMATIZACIÓN DE LA SOCIEDAD Y DERECHO

Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un verdadero instrumento de actos ilícitos. Éste tipo de actitudes concebidas por el hombre encuentran sus orígenes desde el mismo surgimiento de la tecnología informática.

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

La evolución tecnológica ha generado un importante número de conductas nocivas que, aprovechando el poder de la información, buscan lucros ilegítimos y causan daños. El Derecho que por esencia se muestra reticente al cambio, no ha reaccionado adecuadamente a las nuevas circunstancias.

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 OCDE a PARIS 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.

Se define al delito o crimen informático es toda interrupción, uso indebido, modificación, o fabricación de datos ajenos que se encuentren en sistemas de computación, sin autorización expresa o implícita de su dueño y/o de quien ostente la propiedad intelectual, con el objeto de obtener un provecho económico o no.

De la definición arriba descrita podemos diferenciar entre dos clases de delitos Informáticos:

Ataques Pasivos

- Divulgación del contenido de mensajes ajenos
- Análisis del tráfico de información de terceros

Ataques Activos

- Utilización de passwords ajenos
- Modificación o alteración de mensajes y/o archivos

- Obstaculización de accesos legítimos

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, 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, los ha 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.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos

en los que, en base a, las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, 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 ha 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 esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos" este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

2.1.3. INFORMÁTICA JURÍDICA

Es una disciplina bifronte en la que se entrecruzan una metodología tecnológica con sus posibilidades y modalidades de tal aplicación. La *informática* jurídica estudia el tratamiento automatizado de: las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (informática jurídica documental);las fuentes de producción jurídica, a

través de la elaboración informática de los factores lógico-formales que concurren en proceso legislativo y en la decisión judicial (informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el *Derecho* (informática jurídica de gestión).

2.1.4. DERECHO DE LA INFORMÁTICA

Es el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática. Asimismo integran el Derecho Informático las proposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho Informático afectan las ramas del Derecho Tradicionales.

Asimismo se inscriben en el ámbito del Derecho Público: El problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público; la Libertada Informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo; o los delitos informáticos, que tienden a configurar un ámbito propio en el Derecho Penal Actual.

Mientras que inciden directamente en el Ámbito del Derecho Privado cuestiones, tales como: Los contratos informáticos, que pueden afectar lo mismo al hardware que al software, dando lugar a una rica tipología de los negocios en la que pueden distinguirse contratos de compraventa, alquiler, leasing, copropiedad, multicontratos de compraventa, mantenimiento y servicios; como los distintos sistemas para la protección jurídica de los objetos tradicionales de los Derechos Civiles y Mercantiles.

Ese mismo carácter interdisciplinario o "espíritu transversal", que distingue al derecho informático, ha suscitado un debate teórico sobre: si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de normas (fuentes), dirigidas a regular un objeto bien delimitado, que se enfoca desde una metodología propia, en cuyo supuesto entraría una disciplina jurídica autónoma.

2.2. IMPORTANCIA DE LA INFORMÁTICA

2.2.1. REGULACIÓN JURÍDICA DEL BIEN INFORMÁTICO

Los intereses difusos, que bien pueden llamarse asimismo intereses de "pertenencia difusa", porque pertenecen a muchos en común, integrando todos ellos un conjunto difuso, con lo que "lo difuso" es el grupo humano que coparticipa

en el interés, y no tanto el interés mismo, que se puede percibir como concreto, se confunden con frecuencia con los intereses colectivos; en ambos casos, el bien jurídico protegido es indivisible.

Sin embargo, mientras entre los titulares de un interés difuso no existe relación jurídica alguna (pensemos por ejemplo en los consumidores y usuarios, si bien es cierto que últimamente han surgido organizaciones de tales, o en quienes reclaman que cesen las agresiones al medio ambiente), sí que existe una relación de base entre los titulares de un interés colectivo, relación que viene dada por la vinculación directa de los miembros del colectivo (una asociación o conjunto de asociaciones) o por un vínculo jurídico que les relaciona con la parte contraria, por así llamarla (los disidentes universitarios, por ejemplo).

En todo caso, la diferencia tiende a atenuarse porque cada vez son mayores los intentos de amplios sectores sociales de vertebrarse, de organizarse jurídicamente con vistas precisamente a una defensa más eficaz de esos intereses difusos.

Al tratarse de un interés comúnmente compartido por muchas personas, su afectación plantea de inmediato la problemática de su accionabilidad, esto es, de la legitimación procesal para recurrir, que con los criterios individualistas tradicionales requiere de una afectación actual y directa en la esfera jurídica (derechos o intereses legítimos) de una determinada persona, con lo que la pervivencia, en estos supuestos de interés difuso, de un criterio de legitimación procesal clásico puede poner en peligro la tutela de tales intereses.

Aun cuando admitiéramos con Bidart Campos que estamos ante "situaciones jurídicas subjetivas", que no se esfuman ni pierden la naturaleza de tales por la circunstancia de que cada uno de los sujetos que las titularicen compongan un grupo o conjunto humano al que le es común ese mismo interés (la afectación del interés perjudica al conjunto, y, por lo mismo, también a cada persona que forma parte de él), si mantenemos, en coherencia con ello, los criterios de legitimación procesal tradicionales y entendemos que un individuo está legitimado para recurrir en defensa de un interés difuso que, sin embargo, en cuanto tal también le es propio, es más que probable que nos encontremos con notabilísimos desequilibrios entre las partes de ese proceso: una persona en defensa del medio ambiente frente a los vertidos contaminadores de una gran empresa multinacional; un consumidor enfrentado a un gran grupo de distribución de mercado...etcétera.[9]

9 Bidart Campos, Germán José, *Teoría General de los Derechos Humanos*, 1ª. ed., 1991 pag. 425.

A la vista de todo ello, se impone, pues, una radical mutación de los esquemas tradicionales de la tutela jurisdiccional, una, como dice Cappelletti, profunda metamorfosis del derecho procesal para evitar que permanezcan prácticamente desprovistos de protección los intereses difusos, cambio que posiblemente exija un abandono en ciertos casos de la idea de subjetividad como categoría del derecho público, cuya insuficiencia y efectos negativos;[10] como bien apunta De Cabo, se han manifestado en diversos sectores, uno de ellos, desde luego, el que ahora nos ocupa.[11]

Parece necesario, consecuentemente, la búsqueda de nuevas categorías jurídicas que vinculen en estos casos la protección no tanto a un sujeto cuanto a un elemento objetivo como puede ser la protección del interés colectivo, difuso o general. A ello se vincula íntimamente la necesaria revisión del concepto tradicional de legitimación procesal, que también Fix-Zamudio ha reivindicado últimamente.[12]

En la misma dirección, Haberle ha entendido que el reconocimiento de una legitimación para recurrir a ciertos grupos u organizaciones podría tener una indudable virtualidad instrumental en orden a la efectividad práctica de los derechos fundamentales, porque tal efectividad se produce también a través del pluralismo de la opinión pública.

---

10 Cappelletti Mauro, *Acces to Justice*; Milán, Italia. 4ª. ed., 1979 p. 281.
11 De Cabo, Filosofía del derecho y filosofía de la cultura. 3ª. ed., 1982. p.154
12 Fix-Zamudio, Héctor y Ovalle Favela, José; *Derecho procesal*; 1ª. Edición, 1991, México, pag. 127

2.2.2. PROTECCIÓN DE DATOS PERSONALES

En México, la privacidad y los datos de las personas en las relaciones entre empresas y consumidores se encuentra regulada en la Ley Federal de Protección al Consumidor y en otras disposiciones sobre privacidad contenidas en ordenamientos jurídicos a nivel federal.

Sin embargo, en la medida en la que se extienda la penetración y uso de Internet, se deberá evaluar la posibilidad de crear un marco jurídico más amplio y eficiente que proteja los datos y la información proporcionada por los ciudadanos no solo a los sitios Web de las empresas comerciales, sino sobre todo a los órganos gubernamentales cuyos servicios y trámites se ofrecerán también en línea en un futuro cercano.

Resulta conveniente, que en sectores altamente sensibles en donde la confidencialidad de la información de las personas es considerada primordial, como son el sector salud, bancario y laboral, se contemple la posibilidad de incluir aspectos puntuales sobre privacidad y protección de datos personales en el ámbito de sus respectivas leyes, reglamentos y ordenamientos.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco jurídico de la privacidad en nuestro país. El primer párrafo de este artículo consagra una de las garantías individuales más importantes que es el

derecho que tenemos a no ser molestados en nuestra persona, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento y en el penúltimo párrafo de este mismo artículo, se contempla que la correspondencia que bajo cubierta circule por las estafetas, deberá estar libre de todo registro y su violación será penada por la ley.

2.2.3. FLUJO DE DATOS TRANSFRONTERIZOS

Las disposiciones tendientes a proteger la información personal y la confidencialidad de los datos correspondientes a los consumidores de bienes o servicios en Internet, la Ley Federal de Telecomunicaciones en su Artículo 49 establece que: la información que se transmita a través de redes y servicios de telecomunicaciones será confidencial, salvo aquella que, por su propia naturaleza sea pública o cuando medie orden de autoridad competente.

Existen otras disposiciones sobre la confidencialidad de los datos que se transmiten electrónicamente tanto de personas como de empresas en la Legislación Bancaria y del Mercado de Valores, así como en otras leyes administrativas en las que los particulares deben proporcionar información confidencial a las autoridades competentes.

No obstante lo anterior, México no cuenta con una legislación específica integral sobre este tema y desde luego, no existe disposición alguna que regule, restrinja o prohíba el flujo de datos transfronterizos de sus ciudadanos.

2.2.4. PROTECCIÓN DE LOS PROGRAMAS DE CÓMPUTO

En el ámbito nacional hasta hace muy poco tiempo se le ha dado la debida importancia a la problemática jurídica derivada del uso de las computadoras y de los programas de computación. Esto se debe fundamentalmente, como ya se mencionó anteriormente, al atraso en la recepción de la tecnología proveniente del extranjero.

Afortunadamente, gracias al esfuerzo de algunos juristas mexicanos se ha hecho resaltar la trascendencia jurídica que trae consigo la falta de una legislación adecuada que proteja tanto a los autores de los programas de cómputo como a los usuarios de los mismos. Al efecto, existen dos ordenamientos jurídicos que contienen disposiciones referentes a los programas de cómputo y que son: la Ley sobre el Control y Registro de la Transferencia de Tecnología y el Uso y Explotación de Patentes y Marcas y la Ley de Derechos de Autor.

La inclusión de los programas de cómputo en el primero de estos ordenamientos **(LRTT)** se debió en gran medida a la preocupación de las autoridades mexicanas por frenar, en la medida de lo posible, las importaciones de insumos tecnológicos o por lo menos llevarlos a su racionalización. Tratándose específicamente de los programas de cómputo, las autoridades de SECOFIN consideraron que, al importar como obligación la solicitud de aprobación de inscripción de los contratos por los que se comercialicen los programas establecida en la LRTT, se podría controlar su desarrollo en el país en sodas sus facetas, es decir, en su importación, exportación, fomento de desarrollos nacionales y sobre todo el control de flujo de divisas al extranjero.

2.2.5. CONTRATOS INFORMÁTICOS

El desarrollo de las nuevas tecnologías ha propiciado el nacimiento de una nueva forma de contratación y de nuevas modalidades contractuales. En cada uno de los contratos se ha de prestar especial atención a su redacción, formalización y negociación.

Un simple modelo de contrato no garantiza los efectos deseados, ya que una mala redacción de las mismas puede dar lugar a resultados y consecuencias jurídicas no deseadas. Se hace necesario conocer y respetar la legislación contractual a la hora de redactarlos, por ello las empresas y los consumidores en

general han de poner en manos de abogados y profesionales del derecho la redacción de sus contratos, dada la complejidad de la materia y del lenguaje jurídico y técnico empleado en su redacción.

Los centros informáticos tienen varias funciones como aquellas relativas al procesamiento de datos y la entrega de resultados veraces y oportunos para la toma de decisiones; pero eso no es todo, también se realizan estudios previos a fin de satisfacer los requerimientos de equipo y materiales que dichos centros exigen para su adecuado funcionamiento, así como para satisfacer las necesidades de los usuarios. Para que se dé dicha situación, los centros informáticos se ven precisados a establecer contratos con las empresas proveedoras de bienes y servicios informáticos en aquello que se ha tenido a bien en llamar los "contratos informáticos".

Los bienes y servicios informáticos no dejan de ser el "producto" de una "transferencia tecnológica" originaria de los países altamente industrializados, provocando una marcada relación de dependencia en relación a los países en desarrollo.

Por contratos informáticos podemos entender todo acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información.

Para tal efecto se han establecido dos criterios básicos como lo son el funcional en el que las prestaciones se relacionan con el tratamiento sistematizado de la información y el estructural en el que las prestaciones se relacionan con el equipo físico, el soporte lógico, la organización, la información, los suministros, la interacción de los elementos con el medio ambiente y los elementos o relaciones que integran los sistemas.

La importancia de dichos contratos estriba en que ante las lagunas y falta de certeza que presenta el derecho civil contractual, la redacción y negociación de estos contratos se ha convertido en la única "oportunidad" de que las partes se dicten por sus propias normas con el grado de precisión que requieren las circunstancias. Esta situación no se encuentra tan marcada como en otro tipo de contrataciones que llevan a cabo otros sectores que cuentan con legislación jurisprudencia, costumbre y doctrina en grado suficiente como para integrar los casos no previstos e interpretar las cláusulas equívocas.

Tan importantes y especiales son los contratos informáticos que las grandes empresas norteamericanas en su calidad de proveedoras o usuarias suelen tener un área específica integrada por equipos interdisciplinarios de informáticos, contadores y abogados para la redacción y negociación de dichos contratos; sin embargo, en nuestro país aún no se les ha atribuido la debida importancia.

La existencia de sistemas destinados al tratamiento automatizado de la información es el hecho técnico que da fundamento a los llamados "contratos informáticos", ya que se trata del concepto principal que permite predicar la unidad de la nueva rama frente a la multiplicidad aparente de los fenómenos jurídicos que la integran.

La práctica comercial de contratar por separado las prestaciones informáticas no debe hacer perder de vista el enfoque esencial que permite contemplar en su verdadera dimensión a los contratos de bienes y servicios informáticos consistente en tener siempre presente que el objeto de éstos son los sistemas informáticos, subsistemas o elementos en interacción entre sí o con el medio ambiente.

Cuando se contratan por ejemplo bienes informáticos, sea en conjunto o por separado, debe ser explícito en cuanto a la interacción anteriormente mencionada, de tal manera que cumplan con la función instrumental para la que fueron diseñados de acuerdo con sus respectivas especificaciones técnicas en el contexto de la finalidad concreta a la cual se destinarán en el sistema informático al que serán integrados como partes componentes.

Por eso cabe afirmar que en la experiencia jurídica, además de la tipicidad legal de algunos contratos como la compraventa, existe también la tipicidad

consuetudinaria de los contratos de equipos, soporte lógico, desarrollo de sistemas, y demás; ya que se plantea una serie de problemas recurrentes que exigen soluciones repetitivas y adecuadas, es decir, "típicas", que solo adquieren pleno sentido cuando se les contempla bajo la perspectiva del sistema informático.

A fin de evitar sorpresas desagradables, los contratos informáticos deben contener en forma explícita y precisa, elementos generales tales como el objeto (creación y transmisión de derechos y obligaciones respecto de los bienes y servicios informáticos), duración, rescisión, precio, facturación y pago, garantías y responsabilidades y disposiciones generales.

Las garantías (obligación inherente a una persona de asegurar a otra el goce de una cosa o derecho, de protegerla contra un daño o de indemnizarla en caso de determinados supuestos). Estas cláusulas señalan la manifestación de compromiso fundamentalmente de los proveedores aunque en nuestro ámbito contractual en la mayoría de las ocasiones se trata de cláusulas limitativas de responsabilidad que constituyen verdaderos contratos de adhesión.

Normalmente las garantías tienen su origen en el contrato, pero en caso de no estar estipuladas, se encuentran previstas por la ley bajo un carácter supletorio o imperativo, con la posibilidad por parte de los contratantes de ampliarlas, limitarlas o suprimirlas.

Las garantías más importantes en los contratos informáticos son las de conformidad por las cuales el proveedor se compromete a entregar al usuario aquello previsto en el contrato conforme a lo pactado por las partes; la de buen funcionamiento, por la cual el proveedor se constriñe a mantener funcionando el equipo en forma adecuada durante un cierto tiempo, luego el cual puede celebrarse un contrato de mantenimiento; la garantía contra vicios, la cual obliga al proveedor a una acción de saneamiento en caso de aparición de vicios ocultos y finalmente la garantía de evicción, referida a la obligación del proveedor a responder contra toda reivindicación por parte de terceros respecto a la propiedad industrial o intelectual de los materiales y/o programas provistos al usuario.

Por otra parte, las responsabilidades que son las que determinan el accionar de las garantías, como es el caso de la obligación de reparar el daño causado al contratante por la falta de ejecución del compromiso adquirido en los contratos informáticos; las responsabilidades más importantes son las referidas a la seguridad material del equipo y aquello concerniente a los daños causados por el material o el personal del proveedor. Lo anterior no exime a los contratantes de convenir otras cosas a manera de disposiciones generales.

El ambiente informático en muchas ocasiones se convierte en fuente de ambigüedades en cuanto que su léxico está integrado por numerosos vocablos de orden técnico, a los que comerciantes, juristas y aún los mismos "expertos" en informática llegan a atribuir contenidos diferentes, lo cual puede traer como

consecuencia que los derechos y obligaciones contractuales lleguen a ser diversos de aquellos que las partes pensaron haber suscrito.

El usuario debe ejercer un estricto control y supervisión en el funcionamiento del equipo informático que adquiera, siendo conveniente un asesoramiento externo por parte de un experto en la materia para que vigile el buen desarrollo de dichas actividades.

Por otra parte, es importante que el usuario le dé un buen mantenimiento a su equipo, y si en este proceso intervienen funcionarios del proveedor deberá tener un control discreto sobre ellos a efecto de prevenir una eventual actitud dolosa que pudiera suscitarse, como por ejemplo que los empleados del proveedor pretexten mal funcionamiento del equipo y pretendan hacer crecer al usuario una "necesaria" reparación y su consiguiente aumento en el cobro de honorarios o llegando aun al extremo de "robar" los programas creados por el usuario.

Los contratos de asistencia técnica al usuario de sistemas informáticos son específicos, sin embargo, en algunos contratos informáticos ya se prevé una cláusula especial sobre dicha asistencia técnica, la cual debe ser periódica y oportuna.

Este servicio lo puede ofrecer el proveedor o bien una empresa que se encargue de ello, quedando al usuario la elección según las circunstancias. En este sentido, la formación se refiere a la capacitación que el proveedor dé al personal de la empresa del usuario, especialmente a quienes se vayan a encargar de manejar el sistema.

Es indudable que el éxito que pueda tener la informatización de una empresa radica fundamentalmente en que tenga un buen equipo, eficientes programas de cómputo y personal debidamente capacitado.

Esto consiste en el carácter confidencial que el proveedor debe dar a la información de su cliente; si por el contrario, realiza o permite su divulgación a un tercero, eventualmente o no competidor, el usuario estará en todo su derecho de demandarlo por la vía civil o aún por abuso de confianza. Es esencial que en una empresa informática se sigan estos principios de secrecía y confidencialidad para su buen funcionamiento, seguridad y reputación.

Son cláusulas que se refieren a un concepto en especial y que las partes convienen en insertarlas en los contratos informáticos. Por citar algunas tenemos: la cláusula de no solicitud de personal, en la que el cliente se compromete a no contratar al personal del proveedor parta que trabaje con él. Esta cláusula se interpreta como una obligación de no hacer.

Existe otra cláusula que se refiere a la restricción de acceso al equipo y que se utiliza frecuentemente en los contratos de mantenimiento para liberar al proveedor de toda garantía en caso de intervención del usuario o de una tercera persona sobre el equipo informático. Esta cláusula es limitativa de responsabilidad.

Las partes que conforman la relación contractual de índole informática como lo son los proveedores; que son los fabricantes, distribuidores y vendedores de bienes informáticos y son aquellos obligados a salvaguardar los intereses del cliente y darle consejo e información, cumplir con la entrega de los bienes o con la prestación de sus servicios en los plazos estipulados, realizar la prestación conforme a las especificaciones del contrato, garantizar los vicios ocultos que pudiera llegar a tener la prestación realizada, y el estudio de viabilidad para el usuario, actuando en todo momento con probidad y honestidad, así como con una asesoría y apoyo adecuados.

Los usuarios son aquellas entidades (públicas o privadas) o individuos que requieren satisfacer determinadas necesidades a través de los bienes informáticos, y entre sus principales obligaciones están; informarse, documentarse, visitar exposiciones y demostraciones de equipo de servicios informáticos en general, solicitar folletos explicativos sobre las características y funcionamiento de los centros de cómputo, así como de los programas ya existentes, determinar de manera precisa sus necesidades de automatización

fijando y comunicando sus objetivos precisos, suministrar al proveedor de informaciones exactas de su empresa, acompañadas de documentos, gráficas, proyectos y demás; capacitar adecuadamente a su personal para el manejo del centro de cómputo (funcionamiento, seguridad, programación), obtener una mejor adaptación de su empresa a los imperativos de funcionamiento del material instalado, realizar la elección final de entre las ofertas que le presenten los proveedores, considerando los elementos de apreciación de orden financiero y técnico, aceptar y recibir el material o los servicios que ha solicitado, acordar un periodo de prueba a efecto de verificar el funcionamiento del equipo, respetar las directrices propuestas y formuladas por el proveedor sobre el modo de empleo del material o de los programas, pagar el precio convenido según las modalidades fijadas entre las partes.

Los principales contratos informáticos asimilables dentro de las categorías jurídico-contractuales son: la compraventa, arrendamiento, arrendamiento con opción a compra de bienes informáticos, así como la prestación de servicios informáticos.

- *Compraventa*

Se refiere a los equipos y suministros (componentes, accesorios, etc). Su esencia es similar a la de cualquier contrato de compraventa referido a otros

bienes, sin embargo, reviste una seria de elementos peculiares que los tornan aún más complejos.

En este contrato informático se debe establecer en primer término que el proveedor venderá al usuario el material de acuerdo con los planes de contratación ofrecidos, debiendo incluirse una relación de las máquinas que integren el centro de cómputo materia de la compraventa, indicando asimismo, el modelo, descripción, cantidad, precio de compra, y cargo mensual de mantenimiento.

Se deberá asentar en el contrato la fecha de entrega del equipo de cómputo, así como el sitio y las condiciones. Los pagos deberán hacerse de conformidad con el plan de contratación específico establecido en el contrato y ningún cargo comenzará a "surtir efecto" hasta que haya sido aceptado el sistema de cómputo y demás productos amparados por el contrato.

Es importante que se establezca en el contrato el momento en que el usuario adquiere la propiedad; por otra parte, podrá haber un periodo de prueba del equipo que comience desde la fecha de entrega del sistema y termine después de treinta días. Si después de sesenta días no se ha alcanzado un nivel de eficacia, el usuario podrá solicitar el reemplazo total del equipo o de la unidad que no funciona.

El proveedor deberá responder por los daños y perjuicios que le cause al usuario en caso de incumplimiento; asimismo, asumirá cualquier responsabilidad para el saneamiento en caso de evicción. Es por ello que deberá establecer el contrato informático que el proveedor garantizará que el equipo y sus dispositivos no tendrán algún defecto.

El proveedor deberá garantizar también el tiempo que se obligue a suministrar al usuario las partes y refacciones necesarias para mantener los equipos en las condiciones adecuadas de funcionamiento. Por otro lado, el proveedor proporcionará por escrito al usuario toda la información técnica necesaria para que éste haga el uso adecuado del equipo.

Durante el tiempo que dure el contrato y aún después, ambas partes deberán convenir en mantener con discreción cualquier información recibida de la otra parte que haya sido clasificada como confidencial. El proveedor será responsable de las violaciones que se causen en materia de patentes o derechos de autor respecto de los objetos materia del contrato proporcionados al usuario. A este respecto, debe comprometerse al pago de daños y perjuicios.

Las partes deben establecer el plazo durante el cual el usuario puede cancelar temporal o definitivamente el equipo solicitado mediante aviso por escrito. En caso de que el usuario, por así convenir sus intereses, adquiera equipos de compañías extranjeras, teniendo la obligación de pagar el impuesto sobre la renta.

Este contrato constituye un acuerdo entre las partes y deja sin efecto cualquier negociación, obligación o comunicación ya sea oral o escrita, hecha con anterioridad a la firma del mismo.

- *Arrendamiento*

Aplicándolo en materia informática, existen diversas cláusulas específicas para el arrendamiento de sistemas de cómputo, debiéndose insertar en el contrato una relación de las máquinas y sistemas operativos indicando su modelo, descripción, cantidad, precio de compra, renta mensual y cargo mensual de mantenimiento.

Se deberá estipular la duración del contrato en los términos y condiciones acordados respetando los mecanismos de prórroga que se presenten; asimismo, se deberán definir claramente la fecha, el sitio y las condiciones de entrega del sistema de cómputo.

Una vez que las partes han fijado los precios que regirán las operaciones del contrato, se estipulará el compromiso de no alterar los precios pactados originalmente durante la vigencia del mismo; el pago del precio le da derecho al arrendatario de usar en forma ilimitada el sistema de cómputo con sus fases operativas y de programación. El usuario tiene derecho de solicitar que se estipule en el contrato que el equipo de cómputo se pruebe en las instalaciones del proveedor de acuerdo con ciertos estándares establecidos, debiendo proporcionar

el arrendador documentos, formularios y publicaciones referentes a ese equipo de cómputo.

El arrendatario podrá cancelar cualquier unidad de equipo dando aviso al arrendador con treinta días de anticipación y podrá dar por terminado el contrato si el proveedor incurre en violación de cualquiera de las cláusulas del mismo.

Se deberá estipular en el contrato que el arrendador notificará al usuario con uno o dos años de anticipación según sea pactado, su retiro del mercado nacional y mientras esté en el mercado deberá comprometerse a prestar los servicios amparados por el contrato.

En el contrato informático de arrendamiento existen varias cláusulas similares a las que se pactan en un contrato de compraventa, entre ellas que el arrendador deberá mantener en forma confidencial toda documentación que le haya sido facilitada por el arrendatario a fin de realizar el estudio de viabilidad.

El proveedor o arrendador será responsable de las violaciones que se causen en materia de patentes o derechos de autor y se comprometerá a indemnizar por daños y perjuicios a un tercero afectado.

Por otro lado, el arrendador deberá garantizar que el equipo y sus dispositivos estarán libres de cualquier defecto de materiales o mano de obra y

comprometerse a mantener el objeto de materia del contrato en condiciones satisfactorias de operación ajustando, reparando o reemplazando las piezas o artículos defectuosos que causen una operación anormal, así como hacerse cargo de la instalación del sistema de cómputo.

El proveedor también debe hacerse responsable de los empleados que envía a las instalaciones del usuario y asumir cualquier responsabilidad para el saneamiento en caso de evicción, así como indemnizar al usuario en caso de actuar dolosamente.

- *Arrendamiento con opción a compra*

Esta figura es una modalidad del contrato de arrendamiento muy empleado en materia informática y generalmente conocido bajo el anglicismo de *leasing*. Este contrato establece que la opción de compra se podrá ejercer en cualquier momento después de la fecha de aceptación del sistema de cómputo respecto a todo o parte del mismo, considerando los porcentajes pactados de las rentas pagadas que abonarán al precio de compra.

Al ser la compra de equipo informático un gasto muy fuerte para las empresas, es frecuente que en un principio tomen en arrendamiento el centro de cómputo y lo paguen a plazos hasta adquirir la propiedad del mismo.

A este tipo de contrato informático se aplican las cláusulas del contrato de arrendamiento y las del contrato de compraventa en cuanto a adquisición del equipo.

- *Prestación de Servicios*

Este tipo de contratos se refiere a todos aquellos trabajos que sobre determinadas materias se realicen. El contrato que más se asemeja en nuestro derecho civil a este tipo de contrato informático es el de prestación de servicios profesionales que se refiere a los servicios que presta el profesional a una persona llamada cliente, quien se obliga a pagarle una determinada retribución llamada honorarios.

En esta figura se requiere que el prestador de servicios tenga una adecuada preparación técnica además de un título profesional, así como capacidad general para contratar. A este respecto, cabe mencionar que se entiende por ejercicio profesional "La realización habitual de todo acto o la prestación de cualquier servicio propio de cada profesión".

Entre las principales características de este contrato tenemos que son: bilaterales, onerosos, conmutativos y formales o consensuales según acuerden las partes. Los elementos reales son: el servicio profesional y los honorarios. En el llamado contrato de prestación de servicios informáticos hay una categoría que se

refiere a la utilidad o provecho que se obtiene de la realización de acciones o actos concretos de personas físicas o morales que coadyuven de manera directa o indirecta al manejo de la información estando su aplicación relacionada con la estructuración y composición de datos.

Las partes en este contrato informático se denominan "proveedor", siendo aquel que presta el servicio de (prestador) y que la mayoría de las veces son empresas de computación, así como el "cliente" o "usuario" (prestatario) siendo aquel que recibe el servicio y lo retribuye.

Entre dichos contratos de servicios informáticos podemos manifestar que existen el de explotación de programas, de consulta de archivos y banco de datos, el de estudio de mercados en informática, el de documentación técnica, el de mantenimiento correctivo y preventivo de equipo o de sistemas, el manejo de datos, el de desarrollo de estudios de viabilidad para la selección de bienes y servicios, el de consultoría, el de diseño de sistemas, asistencia técnica, formación, etc. La importancia que han ido adquiriendo este tipo de contratos es el resultado de la necesidad cada vez mayor de asesoramiento y servicios informáticos varios que requieren los usuarios.

La problemática fundamental de este tipo de contratos consiste en el desequilibrio notorio existente entre las partes en razón de que comúnmente el proveedor de bienes o servicios se vale de sus conocimientos técnicos sobre la

materia y el correlativo desconocimiento por parte del usuario para imponer sus condiciones mediante una redacción contractual con términos pronunciadamente técnicos en detrimento de los elementos jurídicos, los cuales, en la mayoría de las ocasiones, son aceptados por los usuarios en razón de sus necesidades informáticas y su falta de adecuada asesoría técnica, convirtiendo a éstos en verdaderos contratos de adhesión.

Este tipo de contratos manifiestan una gran cantidad de lagunas jurídicas, las cuales, a su vez, son eventualmente fuente de controversias y conflictos en cuanto a la falta de precisión en caracteres tan importantes como las garantías, responsabilidades, reparación del sistema, pago de daños y perjuicios, etc.

De esta forma nos percatamos que los contratos informáticos ameritan un tratamiento pormenorizado, especialmente en cuanto a las diversas implicaciones hasta hoy desconocidas por el derecho tradicional a efecto de contemplar un régimen jurídico regulador efectivamente aplicable.

CAPITULO III

CLASIFICACIÓN DEL DELITO INFORMATICO EN LA LEGISLACIÓN MEXICANA

3.1. DELITOS INFORMÁTICOS

Los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos.

También se puede definir al delito informático como la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.

Delito informático se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

El Código Penal de 1995 ha introducido nuevas figuras y modalidades delictivas que a continuación se enumeran: Descubrimiento y revelación de secretos, se trata de un delito contra la intimidad, por ello la interceptación del correo electrónico se asimila a la violación de la correspondencia.

En el Código Penal anterior sólo se preveía la destrucción de bienes materiales, por lo que los daños causados a bienes inmateriales no estaban incluidos en este delito.

En el Código Penal Federal vigente establece en su Capitulo de Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática

El Código Penal no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de las personas o para violar, acceder o descubrir sus secretos.

Mero acceso no consentido: Conocido como hacking directo: acceso indebido o no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional.

3.1.1. ASPECTOS LABORALES DE LA INFORMÁTICA

Las restricciones al uso de e-mail por parte de los empleados podrá a su exclusiva discreción, determinar: (a) el número máximo de días en que los mensajes pueden conservarse en el servidor respectivo antes de ser borrados definitivamente sin aviso previo al Usuario; (b) que los mensajes publicados en el tablero de mensajes u otro Contenido que sea cargado será retenido por los Servicios; (c) el número máximo de mensajes de correo electrónico que pueden ser enviados o recibidos por una cuenta en los Servicios; (d) el tamaño máximo de cualquier mensaje de correo electrónico que puede ser enviado o recibido por una cuenta en los Servicios; (e) el máximo espacio del disco que será asignado en los servidores a nombre de cada uno de los Usuarios; y (f) el número máximo de veces y la duración máxima para la cual el Usuario podrá acceder a los Servicios en un determinado periodo de tiempo.

El uso ilícito del servidor El Usuario se obliga a:

- No transmitir información ilegal, obscena o pornográfica de cualquier tipo que constituya delito o violación a las leyes vigentes.

- No transmitir intencionalmente información o adicionar información o software que se encuentren afectados por algún virus o componentes dañinos que pudieran de alguna manera afectar el Servicio.

- Usar fraudulentamente el Servicio en cualquier forma que contravenga el presente Contrato.

- Copiar, pegar, publicar, transmitir, reproducir o distribuir en cualquier forma, información, software o cualquier otro material obtenido a través de Internet, el cual esté protegido por derechos de propiedad industrial e intelectual o cualquier otro derecho, sin obtener permiso previo del propietario o titular del derecho, en términos de la legislación vigente.

- Utilizar el Servicio para ofertas de llamada revertida internacional, que usen la señalización de la llamada incompleta a país alguno en el que este prohibido legalmente hacer este tipo de llamadas.

- Utilizar el Servicio para la transportación de tráfico conmutado de voz hacia o proveniente de cualquier parte del mundo, toda vez que esto constituye una violación a la legislación mexicana.

En caso de que el Usuario se involucre en una o varias de las prácticas aquí prohibidas, puede resultar en la suspensión temporal del Servicio o

terminación del Servicio sin necesidad de declaración judicial y sin responsabilidad alguna para.

3.1.2. VALOR PROBATORIO DE INFORMÁTICOS

El derecho a la prueba va unido al derecho fundamental a la defensa; esto es, aquél que dice que tiene un derecho, necesariamente tiene el deber de probarlo ante un juez y mediante un procedimiento determinado. Si no se puede probar un derecho, consecuentemente no existirá tal.

Las relaciones legales actuales de medios probatorios, no recogen expresamente las técnicas electrónicas, ello no obsta poder invocar y aportar estos elementos probatorios en los juicios en base a los fundamentos jurídicos de pertenencia, indefensión, adecuación real y social, principio de contradicción, etcétera; ya que nada lo impide, pero recomendando disponer en ellos de señas de identidad y autoría y no violar ningún precepto en su obtención.

La actual tecnología ofrece la posibilidad de poder individualizar los registros y dotarles de señas de identidad, nada impedirá pues, dotar a los dispositivos que producen registros, eléctricos, ópticos, magnéticos y físicos de un carácter, logotipo, numero, clave, o cualquiera que sea exclusivo, y con más dificultades de violación que la firma autógrafa, como por ejemplo la denominada

identificación "Biométrica" que partiendo de la huella digital permite el acceso o registro en el sistema, pero impide reconstruir la huella desde ningún sistema, con lo que se preserva la intimidad y se impide la falsificación y manipulación.

En la actualidad la problemática de la prueba reside en el hecho de que generalmente es asimilada a una prueba escrita (aunque es necesario determinar bajo que procedimiento se puede encontrar). Ante eso, es preciso distinguir el concepto de documento, que no debemos restringirlo a la naturaleza del soporte informático ni al escrito como único elemento material, lo que viene a caracterizar al documento informático es su propia desmaterialización o inmaterialización, aunque con ello no deja de ser concreto, visible y perceptible, pues siempre existirá un soporte material (llámese disco magnético, disco óptico numérico o listado de impresor).

De lo anterior se infiere que los registros o documentos informáticos no constituyen una información escrita en sentido jurídico, pues estos contienen llaves de acceso, pueden modificarse con facilidad y no permiten diferenciar entre una copia y su original, lo que si permiten los documentos escritos en papel, aunque a veces se entiende que los documentos informáticos solo constituyen una manera electrónica de escribir.

Frente a las nuevas tecnologías de la información que ofrecen un lenguaje técnico no comprensible, además de la mediación de una máquina que impide la

aprehensión directa de la información, existe una desmaterialización de la propia información, lo que trae aparejada la imposibilidad práctica y física de preconstituir una prueba.

Por otro lado, se considera que surge otro problema en razón de la identificación de las partes que intervienen en una comunicación. Para lo anterior existen mecanismos o servicios que permiten confirmar a partir de la apertura de una conexión o en curso de transmisión, la identidad de las partes en una comunicación, de modo que sea imposible a un tercero hacerse pasar por una de tales partes; esto se refiere al llamado Código Secreto, el cual consiste en la combinación de cifras y/o letras que el sujeto digita sobre el teclado del sistema que utiliza; por ejemplo, los números de identificación personal; la criptografía

CAPITULO IV

DETERMINACIÓN DE APLICACIÓN DE SANCIONES

4.1. SANCIONES EN EL DERECHO ESPAÑOL

Los artículos constitucionales 18.4 y 105 apartado `b' diseñan el perímetro protector, genérico del problema que tratamos, y defieren en una Ley Orgánica su tratamiento pormenorizado. El artículo 18.4 (de la Constitución de 1978) reza: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[13]

Por su parte, el 105 apartado `b' dispone: "[La ley regulará] b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas". Para dar cumplimiento a la preceptiva constitucional, se dictó la Ley

---

13 *Constitución de España de 1978*, art. 18.4. "La ley limitará el uso de la informática.....".

Orgánica número 5/1992 (de 29 de octubre) sobre "regulación del tratamiento automatizado de los datos de carácter personal" (" *BOE*" número 262, de 31 de octubre de 1992). Tal normativa (conocida como LORTAD) constituye un instrumento para impedir que, a través de la tecnología informática, las personas sean blanco de perjuicios en sus derechos.[14]

Su ámbito de aplicación se circunscribe a aquellos datos de carácter personal (entendidos, según el artículo 3.a, como cualquier información concerniente a personas físicas identificadas o identificables) que figuren en ficheros automatizados de los sectores público y privado; incluye, además, toda modalidad de uso posterior aun cuando no automatizado, de datos personales registrados en "soporte físico susceptible de tratamiento automatizado".[15]

Se excluye del espectro aplicativo de la LORTAD: a los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general (artículo 2.2.a); a los ficheros mantenidos por personas físicas para fines exclusivamente personales (artículo 2.2.b); a los de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales (artículo 2.2.c); a los de informática jurídica a los que el público tenga acceso, siempre que aquellos se limiten a reproducir disposiciones o resoluciones judiciales ya publicadas en periódicos o repertorios oficiales (artículo 2.2.d); y a los mantenidos por los partidos políticos, sindicatos e iglesias en la medida que tales datos se refieran a sus asociados, miembros o exmiembros (artículo 2.2.e).

---

14 *Ley Orgánica sobre Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*, no. 5/1992 de 29 de octubre; " BOE" número 262, de 31 de octubre de 1992.
15 Ibidem

Algunos de los principios de la protección de datos de carácter personal que la normativa estableció, disponen que:

Sólo podrán ser recogidos y tratados automatizadamente aquellos datos adecuados, pertinentes y no excesivos con relación al ámbito y finalidades para los que fueron obtenidos (artículo 4.1), no pudiendo ser utilizados para fines distintos de aquellos para los que se recolectaron (artículo 4.2); deberán ser exactos y actualizados, de modo que respondan verazmente a la situación real del afectado (artículo 4.3); serán cancelados cuando hubiesen dejado de ser necesarios o pertinentes para el objetivo en persecución del cual fueron recabados y registrados (artículo 4.5); deberán ser almacenados de forma que permitan al afectado ejercer el derecho de acceso a los datos (artículo 4.6); se proscribe la recolección de datos por medios fraudulentos, desleales o ilícitos (artículo 4.7).

El tratamiento de datos personales requerirá el consentimiento del concernido, salvo alguna disposición legal en contrario (artículo 6.1). Tal consentimiento no será necesario entre otros casos cuando los datos se recojan de fuentes accesibles al público o cuando se recolecten para el ejercicio de funciones propias de las administraciones públicas en el marco de sus competencias (artículo 6.2).

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos personales que revelen ideología, religión y creencias (artículo 7.2). Los datos que refieran al origen racial, a la salud

y a la vida sexual solamente podrán ser recabados, tratados y cedidos cuando existan razones de interés general dispuestas por ley, o bien, cuando medie el consentimiento expreso del sujeto concernido (artículo 7.3). Quedan, asimismo, proscriptos los ficheros creados con el exclusivo propósito de almacenar datos personales reveladores de la ideología, religión, creencias, origen racial o vida sexual (artículo 7.4).

El responsable del fichero automatizado y quienes participen en cualquiera de las etapas del proceso de tratamiento de datos personales están obligados al secreto profesional (artículo 10).

La LORTAD ha establecido los siguientes derechos de las personas:

El afectado podrá impugnar los actos administrativos o decisiones privadas que entrañen una valoración de su conducta, cuyo exclusivo fundamento sea un tratamiento automatizado de datos personales que proporcione una definición de sus características o personalidad (artículo 12).

Cualquier persona podrá conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero; debiendo recabar tal información del Registro General de Protección de Datos, el que será de consulta pública y gratuita (artículo 13).

Se acuerda al afectado el derecho de acceso a los ficheros automatizados para solicitar y obtener información de sus datos de carácter personal (artículo

14.1), derecho que podrá ser ejercitado a intervalos no inferiores a doce meses salvo que acredite un interés legítimo, hipótesis en la cual podrá hacerlo dentro de un plazo menor (artículo 14.3). La información podrá consistir en la mera consulta por visualización de los ficheros o en la comunicación de los datos por escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible (artículo 14.2).

También se establece el derecho de rectificación y cancelación, para el supuesto de que los datos personales resulten inexactos o incompletos (artículo 15.2). La cancelación no será procedente cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros, o cuando mediase obligación de conservar los datos (artículo 15.4). No se exigirá contraprestación alguna para la rectificación o cancelación de los datos personales inexactos (artículo 16.2).

Los afectados que, como consecuencia del incumplimiento de la LORTAD por parte del responsable del fichero, sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados (artículo 17.3).

Ejemplificativamente, y para concluir este breve repaso, recordamos que la LORTAD fue complementada con posterioridad entre otros instrumentos normativos por los Reales Decretos:

a) Número 428/1993 (26 de marzo), por el que se aprueba el Estatuto de la Agencia de Protección de Datos (que, conforme el artículo 1.1 de dicho Real Decreto, es un ente de derecho público que tiene por objeto la garantía del

cumplimiento y aplicación de las previsiones de la LORTAD, actuando con plena independencia de las administraciones públicas y relacionándose con el gobierno a través del Ministerio de Justicia artículo 1.2), y

b) Número 1.332/1994 (20 de junio), por el que se desarrollan determinados aspectos de aquella Ley Orgánica, la transferencia internacional de datos (capitulo II), la notificación e inscripción de ficheros (capitulo III), el procedimiento sancionador (capitulo V), etcétera.

4.2. SANCIONES EN EL DERECHO MEXICANO

Las sanciones en la legislación penal mexicana establece que el delito informático se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.[16]

La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.[17]

---

16 *Codigo Penal Federal;* art. 210., publicado en el Diario Oficial de la Federación el 26 de mayo de 2004
17 Ibidem art. 211.

A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.[18]

El acceso ilícito a sistemas y equipos de informática se sanciona al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.[19]

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.[20]

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.[21]

18 *Código Penal Federal;* art. 211 bis., publicado en el Diario Oficial de la Federación el 26 de mayo de 2004
19 Ibidem art. 211 bis 1
20 Ibidem art. 211 bis 1 párrafo II
21 Ibidem art. 211 bis 2

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.[22]

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.[23]

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.[24]

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.[25]

22 *Código Penal Federal;* art. 211 bis 2 párrafo II., publicado en el Diario Oficial de la Federación el 26 de mayo de 2004
23 Ibidem art. 211 bis 3
24 Ibidem art. 211 bis 3 párrafo II
25 Ibidem art. 211 bis 4

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.[26]

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.[27]

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.[28]

4.2.1. TIPOS DE CONDUCTAS INVOLUCRADAS

El 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.

---

26 *Código Penal Federal;* art. 211 bis 4 párrafo II., publicado en el Diario Oficial de la Federación el 26 de mayo de 2004
27 Ibidem art. 211 bis 5
28 Ibidem art. 211 bis 5 párrafo II

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, 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 por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

La palabra información del latín in-formare (poner en forma), es una noción abstracta, no obstante que posee una connotación vinculada a una de nuestras mas grandes libertades: la de opinión y expresión de informaciones e ideas por cualquier medio que sea, de aquí que la información se haya considerado como un elemento susceptible de ser transmitido por un signo o combinación de signos,

o como un proceso físico-mecánico de transmisión de datos, tendiendo como dato el elemento referencial acerca de un hecho. En sentido general, un conjunto de datos constituye una información.

A) Características

En cualquier proceso en que intervenga la información, se encuentran las siguientes características:

- Clara e Inteligible; es decir, que su contenido y vehículo de significación debe estar dentro de las normas y lógica de comunicación, acordadas individual o socialmente.
- Relevante; significa que debe revestir un carácter efectivo en el proceso de decisión en el que intervenga.
- Completa; quiere decir que cubra el mayor rango de posibilidades existentes en el momento en que se le requiera.
- Oportuna; es decir, que intervenga y se pondere en el momento en que sea menester.
- Confiable; cuando cumpla satisfactoriamente con los elementos anteriormente enunciados.

B) Clasificación

La información, por otra parte, ha sido objeto de variadas clasificaciones, de entre las que podemos destacar la siguiente:

- Según su contenido; dependiendo del área a que se refiera: jurídica, científica, histórica, política, etc.
- Según su carácter cronológico; pasada, presente o futura.
- Según sus fuentes: oficial, privada, clandestina, confidencial.
- Según sus fines; persuasiva, recreativa, represiva, formativa, alienante.
- Según su procesamiento; manual, semiautomática y automática.

C) Aspectos cualitativo y cuantitativo

Cualitativamente se ha concebido a la información como el contenido de lo que es objeto de intercambio entre el sujeto y el mundo externo, presentándose un conjunto de datos como elementos de las relaciones del hombre y tendente a una ordenación. Es decir, que visto desde este punto de vista, la información constituye un factor de organización.

Por otra parte, cuantitativamente, la información es la medida de disminución de incertidumbre del sujeto respecto a los objetos, de aquí que se hable de una entropía en cuanto al nivel de desorganización y desconocimiento del hombre sobre las cosas en un momento dado.

4.2.2. TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ONU

Actualmente en nuestro país es posible codificar la información a través de programas especiales, tarjetas electrónicas con claves de acceso o sistemas que después de cada operación generan una nueva clave para que la información pueda ser conocida por el destinatario final, lo cual permite realizar transacciones comerciales con mayor seguridad. Sin embargo, es necesario que se inicie una actividad legislativa que actualice, en materia penal, a los diversos elementos de la tecnología de la información.

Es un hecho que el Internet puede ser usado como un medio para la realización de toda una serie de delitos que se encuentran tipificados en el Código Penal Mexicano y en la mayoría de las leyes criminales alrededor del mundo. La información que viaja por Internet puede ser usada por hackers o "piratas", o puede usarse como medio para la transmisión de pornografía, o para la transmisión de información entre bandas internacionales de narcotráfico.

Los delitos informáticos constituyen una gran laguna en nuestra legislación penal. El derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren de un análisis urgente por parte de nuestros académicos penalistas y de legisladores.

En un país con importante tradición criminalista como lo es Italia, nos encontramos delitos como:

a) Acceso abusivo, el cual se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad ("passwords" o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso al sistema solamente a las personas por él autorizadas. Este delito es castigado con reclusión de hasta tres años previendo agravantes.

b) Abuso de la calidad de operador de sistema. Este delito es un agravante al delito de acceso abusivo y lo comete aquel que tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.

c) Fraude informático. Cuando por medio de artificios o engaños, procura para sí o para otros un injusto beneficio, ocasionando daño a terceras personas. También se entiende como tal a la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones y programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La sanción para este tipo de delito es de meses hasta tres años de prisión, más una multa considerable.

d) Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tienen la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.

e) Intercepción abusiva. Es un delito que se comete realizando el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, la intercepción fraudulenta es el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación, mediante cualquier medio, de información al público del contenido de esas comunicaciones, teniendo una sanción de entre 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el mismo fin.

f) Falsificación informática. Es la alteración, modificación o eliminación del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales se equiparan a los escritos).

En este sentido, la doctrina italiana tiene muy clara la noción de "documento informático", al cual definen como cualquier soporte informático que contiene datos, informaciones o programas específicamente destinados a elaborarlos.

g) Espionaje informático. Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionando daño a otro.

h) Violencia sobre bienes informáticos. Es el ejercicio arbitrario a través de la violencia sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

i) Abuso de la detentación y difusión de códigos de acceso ("passwords"), que es la publicación o mal uso de claves de acceso sin la autorización de quien tiene el derecho legítimo.

j) Violación de correspondencia electrónica, la cual tiene agravantes en caso de causar daños.

Los tipos de delitos informáticos reconocidos por la organización de las naciones unidas (ONU) que en su legislación internacional se encuentran establecidos son:

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:

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

- Gusanos: se fabrica 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.

- 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.

- 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 ilegitimo 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.

4.3. LEGISLACIONES INTERNACIONALES

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.

b) Estafa informática.

c) Falsificación de datos probatorios 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.

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

e) Sabotaje informático: 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.

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: se regulan no sólo los datos personales sino también los no personales y los programas.

b) Estafa informática: 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: 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: se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

c) Destrucción de datos: 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: se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

e) Uso de documentos informatizados falsos: se sanciona a quien conscientemente haga uso de documentos falsos.

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 específica 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 prehacking (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, señala que se impondrá sanción a quien causare daños en propiedad ajena. 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, 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 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, 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, 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. 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 les 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 intimidad que constituyen el objetivo principal de esta Ley. Sin embargo es importante destacar la 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.

CONCLUSIONES

PRIMERA.- El manejo de la información dentro de las organizaciones es esencial para sus operaciones, esta información es resultado de la labor de la institución para recabarla, clasificarla, almacenarla y procesar mas información, esta situación convierte a la información en un recurso invaluable ya que la pérdida de la misma, la fuga y su caída en manos de la competencia o de enemigos puede ocasionar daños, pérdida de mercado o recursos capitalizables, prestigio y aún llevar a una empresa a la quiebra o pérdida de la credibilidad de las políticas de la administración pública.

SEGUNDA.- Es por eso que se convierte en imprescindible el normar y legislar en las empresas y los organismos públicos sobre la tipificación de delitos informáticos, 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.

TERCERA.- Los fraudes electrónicos, el robo de información, la cada vez mayor participación de individuos sin profesionalismo y ética que no manejan de manera prudente y segura la información y que generan además código nocivo que afecta por igual a ambientes de cómputo y redes de comunicaciones con daño a los datos, también debe ser tipificado como delito.

CUARTA.- 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.

QUINTA.- Se debe hacer alusión a lo que encuentra penado en el código penal como lo son las siguientes conductas:

Hacking indirecto: Supone un acceso inconsentido al ordenador o sistema informático como medio para cometer diferentes conductas delictivas. Se castiga por el delito finalmente cometido. (Ejemplo; daños, interceptación del correo electrónico, etc).

Espionaje informático empresarial, aquí el bien jurídico protegido es el secreto empresarial, la información almacenada informáticamente que supone un valor económico para la empresa porque confiere al titular una posición ventajosa en el mercado.

Daños informáticos o sabotaje, se trata de los daños causados en el sistema informático mediante la introducción de virus y bombas lógicas.

Mismas que se deberían tomar en cuenta para establecer una tipificación mas especifica en lo que respecta a diversas conductas que se pueden llegar a presentar.

BIBLIOGRAFIA

1. Análisis del nuevo Código Penal para el Distrito Federal; García Ramírez, Sergio y Islas de González Mariscal, Olga (Coordinadores); 2003.

2. Instrumentos jurídicos contra el crimen organizado; Andrade Sánchez, Eduardo; 1997

3. Sistema de consecuencias jurídicas del delito: nuevas perspectivas; Jaén Vallejo, Manuel; 2002.

4. Teoría del delito, 2a. reimp.; Plascencia Villanueva, Raúl; 2000

5. Ciencia, Estado y derecho en las primeras revoluciones industriales; Kaplan, Marcos; 2000.

6. Contratos, riesgos y seguros informáticos; Téllez Valdés, Julio; 1988

7. Derecho e informática en México. Informática jurídica y derecho de la informática; Ríos Estavillo, Juan José; 1997

8. Derecho informático; Téllez Valdés, Julio; 1991.

9. Diálogos sobre la informática jurídica; Bilón, Jean Loui et al. (Coordinadores); 1989

10. La protección jurídica de los programas de computación, 2a. ed.; Téllez Valdés, Julio; 1989.

11. 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. Callegari, Lidia. 1985.

12. 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. Fernández Calvo, Rafael.

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

LEGISGRAFÍA

1. Constitución de España de 1978

2. Código Penal Federal para la República Mexicana

3. Código Penal para el Distrito Federal

4. Código Penal para el Estado de Veracruz

5. Código Penal para el Estado de Sonora

6. Ley Orgánica sobre Regulación del Tratamiento Automatizado de los Datos (LORTAD)

OTROS MEDIOS DE INFORMACIÓN

1. http://comunidad.derecho.org/pantin/g37313.html

2. http://delitosinformaticos.com/delitos/delitosinformaticos.shtml

3. http://delitosinformaticos.com/trabajos/criminalista.pdf

4. http://derecho.org/comunidad/ulsaagg/cdi.html

5. http://derecho.org/comunidad/ulsaksb/dedo.html

6. http://edec.iespana.es/edec/derinfor/138.htm

7. http://listas.ecuanex.net.ec/pipermail/politicas-internet-lac/2002-November/000600.html

8. http://mipagina.cantv.net/ccsunderground/legislacion%20-%20Actualizacion.html

9. http://perso.wanadoo.es/aniorte_nic/apunt_etic_legislac4.html

10. http://personales.ciudad.com.ar/roble/delitosinf.html