UNIVERSIDAD DEL INSTITUTO TEPEYAC DE CUAUTITLÁN, S.C.

LICENCIATURA EN DERECHO

CLAVE INC. UNAM 8851-09

LA INCLUSIÓN DEL DELITO INFORMÁTICO EN EL CÓDIGO PENAL PARA EL ESTADO DE MÉXICO.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D A EN D E R E C H O

P R E S E N T A

ROSALBA ROMERO MIRANDA

ASESOR: LIC. URBANO CANIZALES BRIONES

CUAUTITLÁN IZCALLI, EDO. DE MÉXICO. 2006.

AGRADECIMIENTOS

A mis padres:

Don Raúl Fernando Romero Urban.
Doña Delfina Miranda Viquez.

A mis hermanos:

Doña Maria Eugenia Olimpia Romero Miranda.
Doña Maria del Roció Romero Miranda.
Doña Maria Eugenia Olimpia Romero Miranda.
Don Fernando Raúl Romero Miranda.

A mis amigos:

Doña Raquel López Schiavon.
Doña Areli Romero Hernández.
Don José Silva Cedillo.

A mis compañeros:

Doña Leonila Cruz Cortes.
Doña Flor Alicia Álvarez Hernández.
Doña Maria del Sagrario Gomes Soto.
Don David Cortes Herrera.

ÍNDICE

INTRODUCCIÓN

La era de la información trae consigo nuevas manifestaciones en la vida cotidiana de las personas y organizaciones tanto públicas como privadas, y de como el avance tecnológico a traído consecuencias en los distintos sectores sociales, económicos, culturales y sobre todo jurídicos.

La difusión de la informática en todos los ámbitos de la vida social ha determinado que se utilice como instrumento para la comisión de actividades que lesionan bienes jurídicos a través de conductas criminales que se realizan por medio de una computadora, o que afectan el funcionamiento de los sistemas informáticos.

Dentro de la Ley Penal Mexicana aun hay un atraso en relación al vertiginoso avance que cada año tiene la informática y sus herramientas más utilizadas que es el *Internet*, el cual consiste en un escenario virtual mediante el cual, cualquier persona puede utilizar para obtener infinidad de información (datos, imágenes y sonidos) para satisfacer su necesidad o simplemente para aclarar sus dudas sobre algún tema en específico.

Estas herramientas que nos brinda la tecnología constituyen un medio para obtener ilegalmente beneficios o ventajas que han inundado la vida cotidiana y económica de las personas físicas dentro del territorio mexicano. Desafortunadamente estos avances tecnológicos son utilizados para cometer delitos o ejecutar comportamientos ilícitos que afectan derechos ajenos y permanecen impunes por no existir norma penal que los sancionen en específico.

Actualmente en el Código Penal Federal mediante reformas de fecha 17 de Mayo del 2000 publicadas en el Diario Oficial de la Federación se crearon los artículos 211-Bis al 211-Bis7 al Código Penal Federal, que tipifican comportamientos que atentan contra sistemas de computo que son parte del sector financiero mexicano y equipos de informática pertenecientes al Estado, pero este ordenamiento penal no define como tal el delito Informático.

Sin embargo dada la influencia que ha tenido la informática en todas las actividades humanas los delitos informáticos podrían ser también competencia del Código Penal para el Estado de México, protegiendo así a todo usuario que utilice dichas herramientas y se vea afectado en sus bienes jurídicamente tutelados.

La autoridad debe tener presente que la información es un bien jurídico que debe ser especialmente protegido por el Estado puesto que de el y de su administración depende el giro normal de las relaciones comerciales y civiles en la sociedad y aun faltan aspectos importantes en los cuales no se ha previsto dentro del delito Informático el detrimento en el patrimonio de las personas o el que estas conductas son realizadas dolosamente en perjuicio de una o varias personas.

El avance de la informática trae problemas referidos a la propiedad intelectual, la protección del consumidor, el comercio electrónico, la seguridad y la privacidad de la información para ejecutar los que van a requerir nuevas estructuras legales que deberán ser legisladas oportunamente.

Es importante destacar que estos delitos son cometidos por personas con conocimiento y experiencia en una profesión o técnica en la rama de la informática y con una preparación académica que les permite beneficiarse ilícitamente a costa de terceros a través de un instrumento informático.

Ya que el avance de la informática es desmesurada y preocupante por lo que desde hace casi dos décadas no se contemplo que hoy contáramos con conductas en donde se pueda perjudicar el patrimonio de una persona con el solo hecho de utilizar una herramienta tecnológica como lo es la computadora, ya que no es necesario hacer uso de un arma para cometer un delito. Actualmente en nuestra sociedad, la informática esta vinculada con casi todos los actos que llevamos acabo y es importante señalar que hoy en día se ha creado una nueva rama de la ciencia jurídica que la considera como instrumento y objeto de estudio del Derecho, la cual se denomina Derecho Informático.

Los efectos que ha traído el aumento de las transacciones realizadas a través de un sistema informático conectado a una red de ordenadores, conocido como *Internet*, o cualquier otro medio de comunicación trae como consecuencia diferentes problemas como el robo o el fraude a cuentas bancarias con la finalidad de causar un perjuicio en el patrimonio de las personas.

El propósito que tiene esta tesis es establecer las bases bajo las cuales debe estimarse la tipificación del Delito Informático en el Código Penal para el Estado de México, así como comprender igualmente algunos Objetivos Específicos los cuales buscan conocer los antecedentes del Delito Informático, así como conocer los presupuestos del Delito Informático, Analizar la regulación que se le ha dado al Delito Informático en el ámbito nacional e internacional resaltando la falta de regulación del Delito Informático en el Código Penal para el Estado de México y así como establecer la conveniencia de regular el Delito Informático.

Por eso es conveniente que dichas conductas den los lineamientos para que el Código Penal del Estado de México frene y castigue el aumento de estos delitos, proponiendo así las condiciones para su adecuada regulación.

Bajo estas consideraciones, me he propuesto incursionar en el tema como se origina la Informática y la importancia que actualmente tiene esta en la vida diaria originando nuevos estudios dentro del ámbito de Derecho dando así paso al Derecho Informático.

Dentro de este desarrollo del tema expondré algunas definiciones hechas por diferentes autores señalando los elementos que integran el Delito Informático así como los sujetos que cometen este tipos de ilícitos, mencionando las características de este delito y como se clasifican.

Se expondrá el marco legal del Delito Informático tanto en el ámbito Internacional como en el Nacional señalando algunos ordenamientos penales y administrativos que mencionan la problemática de los Delitos Informáticos.

Finalizando con algunas consideraciones sustentadas en el estudio expuesto antes mencionado, ya que la finalidad primordial es la inclusión de un tipo penal que contemple el mal uso de los sistemas informáticos adecuándolo a la realidad que existe hoy en México para proteger a todo usuario de la informática y su patrimonio.

CAPÍTULO PRIMERO
MARCO TEÓRICO DE LA INFORMÁTICA

I. Informática

Sus orígenes los encontramos en 1965 en Francia donde se comenzó a utilizar el término informática (*Informatique*) refiriéndose a las ciencias y a las técnicas para recoger datos y para su procesamiento con el fin de facilitar y desarrollar complejas operaciones a gran velocidad. Para Julio Téllez Valdez, en quien nos apoyaremos en su obra DERECHO INFORMATICO para la elaboración de este trabajo, los orígenes de la informática "surge de la misma inquietud racional del hombre, el cual, ante la continua y creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formar nuevos postulados y desarrollar nuevas técnicas que satisfagan dichos propósitos."[1]

Lamentablemente en varias referencias bibliográficas se encuentran los antecedentes de la informática y la computación como los mismos, los cuales posteriormente los expondremos.

1. Nociones y Concepto de Informática

Para explicar la informática en primer lugar hay que entender ¿Qué es información? Y después, ¿Qué debemos entender por procesamiento de información?

En su definición más amplia la información es todo lo que reduce la incertidumbre entre varias alternativas posibles, es decir, se consideraría que son los datos que necesitamos conocer para tomar decisiones de manera más efectiva.

[1] TÉLLEZ VALDÉZ, Julio. *Derecho Informático*, 3ª. ed., McGraw-Hill, México, 2004, p.3.

El concepto de información se refiere a todo aquello que esta presente en el mensaje o señas cuando se establece un proceso de comunicación entre un emisor y un receptor. Así, cuando dos personas hablan, intercambian información. La información puede encontrarse y enviarse en muchas formas, a condición de que quien la reciba pueda interpretarla.

Es necesario no confundir a la información con los datos[2] por que suelen utilizarse como sinónimos. Se dice entonces "que la información es el significado que tiene una comunicación para un receptor en una situación dada, en relación con un problema especifico."[3]

Para lograr interpretar la información se necesita procesarla y esto implica el almacenamiento, la organización y, la transmisión de la misma. Para ello, en la informática intervienen varias tecnologías, podríamos decir que son dos sus pilares: como son la comunicación y la computación; es decir, en lo que actualmente conocemos como informática concurren muchas de las técnicas y de las maquinas que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar sus capacidades de memoria, de pensamiento y de comunicación.

Cuando un naufrago marca en el tronco de un árbol una raya por cada día que pasa, lo hace para no perder la cuenta, es decir, para apoyar su memoria; cuando se utiliza una calculadora para sumar dos cantidades, se auxilia el pensamiento; cuando una persona en un centro comercial anuncia una oferta en el altavoz, esta potenciando su capacidad de comunicarse con palabras; y actualmente, cuando una persona se comunica con otra a miles de kilómetros de distancia, esta empleando una tecnología informática por excelencia que es *Internet*[4], en la que

[2] "La diferencia básica entre datos e información consiste en que los datos no son útiles o significativos como tales, si no hasta que son procesados y convertidos en una forma útil llamada información." MORA, José Luís y ENZO MOLINO. *Introducción a la Informática*, 4ª. ed., Trillas, México, 1991, p.33.
[3] *Ibidem*, p.33.
[4] *abrev.* de *Internacional Network*, red telemática internacional, "*Internet* no es un cuerpo físico o tangible si no una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. Es la red de redes: enlaza pequeñas redes de área local (LAN, *Local Area*

interviene no solo el lenguaje escrito, si no también el teléfono (una maquina de comunicar) y la computadora (maquina electrónica diseñada para la manipulación y procesamiento de datos), por lo tanto al estar enviando información la cual esta siendo procesada por una computadora para que quien la reciba pueda comprenderla, se entiende que se esta procesando la información.

Ya que se ha explicado la importancia de la información y del procesamiento de la misma continuaremos definiendo a la informática como la ciencia que se encarga de la automatización del manejo de la información.

"El termino es acrónimo de INFORmación autoMATICA, que significa: todo lo que tiene relación con el procesamiento de datos, utilizando las computadoras."[5] Es así que para Julio Téllez Valdez la informática se defina como: "La palabra informática es un neologismo derivado de los vocablos, información y automatización, sugerido por Phillipe Dreyfus en el año de 1962. En sentido general, la informática se define como un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones. Cabe aclarar a nuestro parecer, que es mas una técnica que una ciencia, debido a su carácter eminentemente pragmático."[6]

Se entiende entonces que la informática combina aspectos teóricos y prácticos de la ingeniería, eléctrica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica. Así podemos entender el concepto de informática como el conjunto de conocimientos que permiten el tratamiento automático de la información y se

---

Network), redes de área metropolitana (MAN, *Metropolitan Area Network*) y grandes redes de área amplia (WAN, *Wide Area Network*) que conectan a los sistemas informáticos de múltiples organizaciones en el mundo. Hay varios métodos para interconectar esas redes: a través de líneas telefónicas, de líneas de alta velocidad, fibra óptica, satélites y microondas. BARRIOS GARRIDO, Gabriela. *et al., Internet y Derecho en México*, 1ª. ed., McGraw-Hill, México, 1998, p.5.

[5] FERREYRA CORTES, Gonzalo. *Virus en las computadoras*, Macrobit, México, 1990, p. 1.

[6] TÉLLEZ VALDEZ, Julio. *op. cit*., p.p. 3-4.

utiliza para abarcar a todo lo relacionado con el manejo de datos mediante equipos de procesamiento automático como las computadoras.

Por ultimo es importante destacar que la informática se aplica a diversos sectores de la actividad diaria como son la medicina, ingeniería, industria, en la investigación científica, el arte, a nivel empresarial y a nivel profesional, en donde su principal función es facilitar información oportuna y veraz, los cual facilita y automatiza procesos, lo que a su vez trae como ventaja una disminución en los costos. Dentro de las ventajas principales de la informática son las siguientes: la creación de nuevas computadoras, la creación de nuevas especificaciones de trabajo, el desarrollo e implementación de sistemas informáticos existentes. La necesidad de la informática de optimizar tiempo y costos da lugar al surgimiento de la computación.

II. Generalidades de la Computación

1. Orígenes de la Computación

Desde épocas remotas el hombre ha tenido la necesidad de encontrar métodos rápidos y efectivos para resolver sus cálculos, a principio utilizaba sus manos y almacenaba toda información que le era posible en su memoria. Una vez que el hombre invento una forma de contar, es decir, que determino un sistema numérico para realizar cálculos, comenzó a utilizar mecanismos que lo auxiliaban para realizar dichas operaciones. Desde el ábaco hasta las computadoras personales o *lap-toc* estas han tenido una gran influencia en diferentes aspectos de nuestro diario vivir, mejorando nuestra calidad de vida y abriendo puertas que antes eran desconocidas para la humanidad.

Durante el transcurso de la historia el hombre comienza a crear sistemas numéricos que le ayudan a realizar operaciones con mayor rapidez y fluidez, desarrollo herramientas que le ayudarían a cuantificar. Uno de los primeros

dispositivos mecánicos para contar fue el Ábaco el cual fue ideado en China al rededor de 2,500 a.C. este calculador mecánico consistía en un sistema de barras y poleas con lo cual se podían efectuar diferentes tipos de cálculos aritméticos. La Regla de Calculo es creada en 1622 por el matemático ingles William Oughtred, utilizo logaritmos para fabricar un dispositivo que simplificaba la multiplicación y la división, el cual consistía en dos reglas graduadas unidas que se deslizaban una sobre otra. La Pascalina es la primera maquina de sumar construida por el matemático y filosofo francés Blaise Pascal en 1642, funcionaba como maquinaria a base de engranes y ruedas. La Tarjeta Perforada inventada en 1801 por el francés Joseph Marie Jackard, era una maquina para tejer complicados diseños de telas, esta maquina funcionaba con tarjetas perforadas, que contenían información del camino que debían seguir los hilos de la tela para lograr un diseño determinado. La Maquina de Babbage creada en 1834 por Charles Babbage el cual concibió la idea de una maquina analítica la cual podía sumar, substraer, multiplicar y dividir en secuencia automática a una velocidad de 60 sumas por minuto. Y el Código Hollerit creado en 1890 en Estados Unidos mediante la utilización de un sistema que hacia pasar tarjetas perforadas sobre contactos eléctricos, esperando lograr una maquina que hiciera el proceso estadístico de datos rápidamente.

No es hasta el primer tercio del siglo XX, con el desarrollo de la electrónica que se empiezan a solucionar los problemas técnicos que acarreaban estas maquinas, remplazándose los sistemas de engranaje y varillas por impulsos eléctricos, creándose así las primeras computadoras electrónicas en el periodo de 1930-1950, no almacenaban el programa en la memoria, todas se programaban externamente. Durante estos años destacaron cinco computadoras: en 1944 se crea la MARK I, esta computadora usaba componentes eléctricos y mecánicos; en 1945 se construye la ENIAC (*Electronic Numerical Integrator and Calculator*) constituida de tubos de vació; en 1950 se crea la EDVAC (*Electrones Discrete Variable Automatic Computer*) contenía cuatro mil bulbos y usaba un tipo de memoria basado en tubos llenos de mercurio por donde circulaban señales

eléctricas sujetas a retardos; en 1951 se desarrolla la UNIVAC (*Universal Automatique Computer*) que fue la primera computadora digital producida comercialmente, la UNIVAC I era capaz de alcanzar un alta velocidad debido a que utilizaba diodos de cristal en vez de tubos de vació.

Todo el desarrollo de las computadoras suele dividirse en generaciones las cuales mencionan la forma en que han evolucionado al ser más rápidas, más pequeñas y más baratas, presenciando un cambio importante en el *Hardware*[7] y el *Software*.[8]

Las maquinas que forman la llamada primera generación (aproximadamente de 1950 a 1959) se caracterizan por la aparición de computadoras comerciales las cuales estas aun eran voluminosas y usaban tubos de vació como interruptores eléctricos; posteriormente aparecen las maquinas de la segunda generación (aproximadamente de 1959 a 1965) estas computadora utilizaban transistores y disponen de lenguajes que facilitan su uso, esto redujo su tamaño así como su costo; en la tercera generación (aproximadamente de 1965 a 1975) surge el circuito integrado, que eran transistores, cableado y otros componentes en un solo *chip*[9], en esta generación aparecen las mini computadoras en el mercado; durante la cuarta generación (aproximadamente de 1975 a 1985) la industria de la electrónica permite que subsistemas de computadoras completas cupieran en una sola tarjeta de circuito, a la vez que en esta generación aparecen las redes de computadoras; y por ultimo en la quinta generación (comienza en 1985) dado el gran desarrollo de las computadoras con el objetivo de producir maquinas con

---

[7] "Conjunto de los componentes que integran la parte material de una computadora." Real Academia de la Lengua. *Diccionario de la Lengua Española*, Espasa-Calpe, España, 2001, p. 1189.

[8] "Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora." *Ibidem*, p. 2083.

[9] "es una pastilla o *chip* muy delgado en el que se encuentran miles o millones de dispositivos electrónicos interconectados, principalmente diodos y transistores, y también componentes pasivos como resistencia o capacitores. Su área puede ser de un cm2 o incluso inferior. Algunos de los circuitos integrados más avanzados son los microprocesadores que controlan múltiples artefactos: desde computadoras hasta electrodomésticos, pasando por los teléfonos móviles." http://es.wikipedia.org/wiki/Chip

innovaciones reales en los últimos años se creo una singular batalla entre varios países fundamentalmente entre Estados Unidos y Japón, esta lucha sirvió para colocarse a la vanguardia en los nuevos adelantos en materia de computación, con el proyecto de producir computadoras realmente inteligentes, sistemas que se puedan programar con lenguajes naturales mediante los cuales sea posible conversar.

2. Concepto de Computadora

Ya que se entiende a la computación como el conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras, es decir, como una disciplina que se basa en la electrónica, las matemáticas y en la física y que permite llevar acabo todo tipo de cálculos numéricos a través de un procesador de datos programable llamado computadora, comprenderemos mejor el concepto de computadora. Actualmente vivimos en la era de las computadoras donde es difícil pensar en una profesión en la que no haya influido el desarrollo de estas, el aumento desmesurado de la demanda de computadoras personales y de todo tipo de dispositivo dirigido por computadora han colocado a esta en prácticamente cualquier lugar: el trabajo, la empresa, el laboratorio, el hogar, las universidades, etcétera.

La computadora es una maquina capaz de efectuar una secuencia de operaciones mediante un programa, de tal manera, que se realice un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida.

“En México el termino computadora es mas utilizado para designar a aquellos dispositivos electrónicos que tienen capacidad para procesar datos, mediante mecanismos sumamente avanzados que permiten el almacenamiento de datos e

instrucciones, y su manipulación automática mediante el concepto de “programa almacenado”.”[10]

Así mismo una computadora es cualquier dispositivo usado para procesar de acuerdo con un procesamiento bien definido, al principio la palabra era usada para describir a las personas que hacían cálculos aritméticos, con o sin ayuda mecánica, pero luego se traslado solamente a las maquinas, sin embargo también se podría entender que “las computadoras, por su parte, son herramientas de procesamiento de datos que han permitido al hombre desarrollar su capacidad mental, de la misma manera como las maquinas multiplicaran su capacidad física desde su invención.”[11]

3. Estructura de una computadora.

Después de un breve recorrido por la historia de la computación se analizara la parte lógica y técnica de la computadora, es decir los programas y la maquinaria con que opera esta maquina.

A. Nivel Operacional

La computadora a nivel operacional podemos decir que es un dispositivo electrónico que interpreta y ejecuta órdenes programadas, la cual se integra por unidades de entrada y de salida (o también llamados periféricos), unidad central de proceso (o CPU) y un dispositivo de almacenamiento.

a. Unidades de Entrada

Las unidades de entrada son aquellas que permiten al usuario dar instrucciones o datos en la computadora, es decir, convierte las señales externas en un código

[10] ARECHIGA G, Rafael. *Introducción a la Informática*, 1ª. ed., Limusa, México, 1994, p. 20.

[11] GRATTON, Pierre. *Protección Informática*, 1ª. ed., Trillas, México, 1998, p. 23.

especial que puede procesar la computadora. Los dispositivos de entrada mas comunes son el teclado y el *mause* o ratón[12] pero actualmente gracias a la innovación tecnológica existen mas dispositivos de entrada como son el micrófono, el lápiz óptico, las pantallas sensibles al tacto (*Touch Screen*), el lector de código de barras, la cámara digital y el *scanner*[13].

b. Unidad Central de Proceso

La unidad central de proceso CPU (*Central Process Unit*) se considera la parte mas importante de una computadora, por que en ella se realizan las operaciones del sistema informático, ya que esta es la responsable de controlar el flujo de datos (actividades de entrada y de salida) y de la ejecución de las instrucciones de los programas sobre los datos, es decir, realiza todos los cálculos.

c. Dispositivo de Almacenamiento

El dispositivo de almacenamiento o unidad de memoria tiene como función almacenar datos antes de ser procesados, durante su proceso y después de que este haya terminado mientras la información es dirigida a las unidades de salida.

d. Unidades de Salida

[12] "Pequeño aparato manual conectado a un ordenador o a un terminal, cuya función es mover el cursor por la pantalla para dar órdenes." Biblioteca de Consulta *Microsoft*® *Encarta*® 2004. © 1993-2003 *Microsoft Corporation*.

[13] "Escáner de ordenador en un escáner (del idioma inglés: scanner) es un periférico que se utiliza para convertir, mediante el uso de la luz, imágenes impresas a formato digital." http://es.wikipedia.org/wiki/Esc%C3%A1ner_de_ordenador

Las unidades de salida son los medios en los que se reciben los resultados de los cálculos o de las manipulaciones de datos de la computadora, es decir, se encargan de mandar una respuesta hacia el exterior por medio del monitor o pantalla, la impresora, el altavoz, los auriculares, las bocinas, el *fax*[14] y el *plotter*[15].

B. Nivel Estructural.

La estructura de una computadora se compone por los elementos que la integra como son un soporte lógico "*Software*" y por un equipo físico "*Hardware*".

a. *Hardware*

Se denomina *hardware* a los elementos físicos de las computadoras que comprenden todos aquellos elementos mecánicos, electrónicos y eléctricos de las computadoras, el *hardware* se refiere al conjunto de piezas físicas que integran una computadora, es decir, es todo lo que se puede tocar como los cables, circuitos, tarjetas, el teclado, el monitor, etcétera.

b. *Software*

El *Software* es la parte intangible de la computadora, es el conjunto de instrucciones elaboradas en base en una secuencia lógica, por lo tanto son todas

[14] "Se denomina *fax*, por abreviación de *facsímil*, a un sistema que permite transmitir a distancia por la línea telefónica escritos o gráficos (telecopia)." http://es.wikipedia.org/wiki/Fax

[15] "Un *plotter* o trazador gráfico es un dispositivo de impresión conectado a una computadora, y diseñado específicamente para trazar gráficos vectoriales ó dibujos lineales: planos, dibujos de piezas, etc. Efectúa con gran precisión impresiones gráficas que una impresora no podría obtener. Los primeros usaban plumillas de diferentes trazos ó colores. Actualmente son frecuentes los de inyección, que tienen mayor facilidad para realizar dibujos no lineales y en múltiples colores, son silenciosos y más rápidos y precisos." http://es.wikipedia.org/wiki/Plotter

las instrucciones que le permiten al equipo físico realizar una tarea específica y generar los resultados esperados.

C. Lenguajes de Programación

Ya que las computadoras no saben razonar por si solas ni tomar decisiones por cuenta propia es necesario introducirles instrucciones para indicarle no solamente lo que tiene que hacer, si no también el momento en que tiene que lo debe hacer, el lenguaje de programación es un conjunto de palabras y de reglas de sintaxis para facilitar la comunicación con la compradora, el lenguaje a utilizar debe ser elegido de acuerdo con las necesidades particulares de los usuarios y con la capacidad del equipo en uso, se entiende entonces que el lenguaje de programación es utilizado para definir una serie de instrucciones que representan las tareas que procesara una computadora; al conjunto de instrucciones agrupadas se le conoce como programa.[16]

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

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

[16] "Un programa es simplemente una secuencia de instrucciones que orienta a la CPU en el desarrollo de los cálculos. Por ultimo, este programa debe expresarse de forma que pueda ser entendido por la CPU." TREMBLAY, Jean Paul y BUNT, Richard B. *Introducción a la Ciencia de las Computadoras*, 1ª. ed., McGraw-Hill, México, 1986, p. 47.

El progreso en los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza la cual esta al alcance de millones de usuarios. Las mas diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que en la practica cotidiana, de hecho sin limitaciones entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años solo podían ubicarse luego de largas búsquedas. En la actualidad esa enorme cantidad de conocimiento puede obtenerse en segundos o minutos, transmitiéndose incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder inmediatamente.

El espectacular desarrollo de la tecnología informática habré las puertas a nuevas posibilidades de delincuencia antes impensable. La manipulación fraudulenta de las computadoras con animo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad[17], son algunos se los procedimientos relacionados en el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer delitos. La informática reúne unas características que la convierte en el medio idóneo para la comisión de distintas modalidades delictivas, en especial de carácter patrimonial (apropiaciones indebidas, fraudes, sabotajes, etcétera).

La facilidad de obtener una gran cantidad de datos acumulados facilita el acceso a estos y la relativamente fácil manipulación de estos datos trae como consecuencia el uso indebido de la información.

[17] *v* “del *lat*. Privare, apartar.” COROMINAS, Joan. *Breve Diccionario Etimológico de la Lengua Castellana*, Gredos, España, 1983, p. 476.

CAPÍTULO SEGUNDO
MARCO TEÓRICO DEL DELITO INFORMÁTICO

I. Relaciones entre la Informática y el Derecho.

Las relaciones entre la informática y el derecho tienen dos facetas: la primera es la aplicación de la informática a los procesos de creación, conocimiento y aplicación del derecho (Informática Jurídica), y la segunda es la informática como objeto de regulación jurídica, que ha dado origen al llamado derecho de la informática. Ambos campos son producto y consecuencia del desarrollo y difusión de la tecnología de las computadoras.

1. Derecho Informático

En la opinión del jurista Julio Téllez el derecho informático se deriva de la interrelación informática-derecho ya que por su importancia debe ser considerado como una obligación para el jurista, en virtud de la necesaria regulación jurídica del fenómeno informático en la sociedad.

La relación de la informática y el derecho nos lleva a considerar a la informática como sujeto del derecho, en cuyo caso hablamos de la informática jurídica; o bien, como objeto del derecho, encontrándonos entonces con el derecho de la informática o derecho informático.

El derecho informático debe constituir una reglamentación jurídica que prevea, atenúe o castigue los efectos que se derivan del abuso y el uso de la informática.

Este cuerpo normativo deberá tener una cobertura en dos niveles fundamentales: nacional e internacional, con la finalidad de que se evite la permanencia de determinados ilícitos informáticos en caso de ser realizados en un país que no esta reglamentado a otro que si lo esta.

Una cuestión importante a destacar del llamado derecho informático es si este constituye una disciplina autónoma, con principios y sistemas propios o si

eventualmente se puede encuadrar en el derecho público o privado. Este punto es objeto de innumerables controversias, sin lograr todavía unificar criterios al respecto. Cabe señalar que aunque esta posible discusión, no es tema central del presente trabajo, nosotros nos inclinamos por la postura que niega autonomía al derecho de la informática ya que no cuenta con instituciones, figuras precisas y conceptos propios; elementos indispensables para la constitución de una disciplina autónoma: si no que esta constituido simplemente por las soluciones jurídicas que se han dado a los problemas originados por la informática, pero que todavía se hallan encuadrado dentro de las ramas tradicionales, por ejemplo: del derecho civil, penal, mercantil, etcétera.

Como ya se ha explicado anteriormente la interrelación de la informática y el derecho se podría definir al derecho informático según Julio Téllez como "una rama de la ciencias Jurídicas que considera a la informática como instrumento y objeto de estudio del derecho"[1]

La interrelación de la informática y el derecho, o la influencia de la informática en el campo de las relaciones jurídicas, se manifiesta en muy diversos campos, entre los que podemos citar de manera enunciativa, los siguientes:

A. Contratos electrónicos y firma electrónica,
B. Protección de la privacidad[2] y de la información,
C. Propiedad intelectual,
D. Contenido de Internet y
E. Delitos informáticos[3].

---

[1] TÉLLEZ VALDEZ, Julio, *op. cit*. p. 17.

[2] "La privacidad puede ser definida como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial. Aunque *privacy* deriva del latín *privatus*, privacidad se ha incorporado a nuestra lengua en los últimos años a través del inglés, por lo cual el término es rechazado por algunos como un anglicismo, aduciendo que el término correcto es intimidad, y en cambio es aceptado por otros como un préstamo lingüístico válido." http://es.wikipedia.org/wiki/Privacidad

[3] BEEKMAN, George. *Introducción a la Informática*, 6ª. ed. Pearson Prentice Hall, Madrid, 2005, p. 356. "LA MARAVILLOSA MÁQUINA PARA JUGAR AL AJEDREZ DE KEMPELEN.
En 1760 Wolfgang Kempelen, un inventor húngaro de 49 años además de ingeniero y consejero en la corte de la emperatriz austriaca Maria Teresa, construyo un jugador de ajedrez mecánico. Este sorprendente artilugio derrotó a los más renombrados jugadores internacionales de la época e hizo ganar a su inventor fama mundial.

En síntesis la informática presta ayuda al derecho, lo que se conoce con el nombre de informática jurídica. Por otra parte el derecho, como regulador de la vida social, tiende a regular los problemas que va creando la revolución tecnológica: he aquí el llamado derecho informático. Dentro de este ultimo, existe un capitulo relacionado con el derecho penal y que consiste en el estudio de aquellos delitos donde la informática juega un papel preponderante ya sea por que se utiliza como medio para delinquir o por que ella es el objeto del delito en si.

2. Antecedentes del Derecho Informático

El primer antecedente al que debemos referirnos lo encontramos en el año 1949, apenas un año después de que en los Estados Unidos, se da a conocer la obra "cibernética"[4] de Norbert Wienner, obra la cual motiva al juez norteamericano Lee

---

Un autómata con aspecto de turco se sentaba tras la enorme caja que soportaba el tablero y las piezas. El operador de la maquina podía abrir la caja para demostrar que no había nada dentro de ella excepto una red de ruedas dentadas, engranajes y cilindros giratorios cada doce movimientos, Kempelen debía <<dar cuerda>> al aparato con una enorme llave. Desde luego, ahora se sabe que esta maquina era realmente una gran broma. El autentico jugador era un enano que controlaba el mecanismo desde dentro y que estaba oculto por espejos cuando la caja se habría. El pequeño jugador no podía ver el tablero, pero podía determinar las piezas a mover vigilando una serie de imanes que se encontraban bajo el mismo.
Kempelen no tenia intención de llevar el engaño mucho mas allá; lo concibió como una broma y lo desmantelo tras su primera gira. Pero se convirtió en esclavo de su propio fraude cuando el publico y la comunidad científica le llenaron de alabanzas al considerarlo como el creador de la primera <<maquina-hombre>>.En 1780, el emperador José II ordeno la realización de otra demostración del jugador de ajedrez mecánico, y Kempelen tubo que reconstruir la maquina. El dispositivo visito todas las cortes europeas de entonces, y el público se mostró incluso más fascinado y curioso que antes.
Tras la muerte de Kempelen en 1804, la maquina fue adquirida por el empresario Maelzel, que la enseño por dentro y por fuera. En 1809, desafió a Napoleón Bonaparte a jugar una partida. Cuando este realizo repetidamente varios movimientos ilegales, la maquina-hombre quito varias piezas del tablero. Napoleón estaba encantado por haber hecho perder los nervios a la maquina. Cuando se jugo la siguiente partida, Napoleón fue ampliamente vencido.
La maquina llego a América en 1826, donde atrajo a una enorme cantidad de gente que pagaba por verla. En 1834, dos artículos distintos (uno de ellos de Edgar Allan Poe) revelaron sus secretos. El articulo de Poe era perspicaz aunque no del todo correcto; uno de sus 17 argumentos era que un autentico jugador automático debería ganar siempre.
Una vez que Maelzel murió en 1837, la maquina paso de mano en mano hasta ser destruida por el fuego en Filadelfia en 1854. durante los 70 años que el autómata fue exhibido públicamente, su <<cerebro>> fue alimentado por 15 jugadores diferentes, los cuales ganaron 294 de 300 partidas.

[4] *v* "La cibernética es la ciencia que se ocupa de los sistemas de control de comunicación en las personas y en la maquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. El nacimiento de la cibernética se estableció en el año 1942, en la época de un Congreso sobre la inhibición cerebral celebrado en Nueva York, del cual surgió la idea de la fecundidad de un intercambio de conocimiento entre fisiólogos y técnicos en mecanismos de control. cinco años mas tarde, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de un palabra griega que puede traducirse como piloto, timonel o regulador. Por tanto la palabra cibernética podría significar ciencia de los mandos. Estos mandos son estructuras con elementos especialmente electrónicos y en correlación con los

Loeverger a escribir un articulo titulado, El Próximo Paso, y en el cual por primera vez se utiliza el termino "Jurimetría"[5] primer antecedente del derecho informático y con el cual se vislumbraba el surgimiento de una nueva rama del derecho, encargadas de las aplicaciones cibernéticas a la información jurídica. El juez Loeverger circunscribió la utilidad y fin de la Jurimetría al estudio de la racionalización del derecho a través de la aplicación de la automatización elevando inclusive una propuesta de aplicación limitada únicamente al derecho fiscal.

En 1958 en Francia el jurista, Lucien Mehi, desarrolla el trabajo titulado automatización en el mundo legal, exponiendo puntos de vista relativos a lo que se dio en nombrar las *maquinas leyes*, calificando las mismas en dos categorías distintas; maquinas documentales y maquinas de consulta.

Para 1963 se publica un articulo, en el que se dan a conocer ideas de gran interés sobre la aplicabilidad de la cibernética al derecho, este articulado conocido como el Knapp (nombre de su autor) no tuvo mayor relevancia ya que fue escrito en Checoslovaco, sin embargo este inconveniente fue superado posteriormente al publicar el mismo autor un estudio titulado "*Stadd an Reich*" publicado en Alemán.

Estos antecedentes continúan en Italia, donde encontramos el trabajo de dos juristas de nombres Frosini, escritor del libro titulado *Cibernetica Diritto e Societá* publicado en 1968 y Mario Lozano, quien se encargo de recopilar y publicar todas las notas de la cátedra que impartía denominada Introducción a la Informática Jurídica.

---

mecanismos que regulan la psicología de los seres vivientes los sistemas sociales humanos , y a la vez que permiten la organización de las maquinas capaces de reaccionar y operar con mas precisión y rapidez que los seres vivos, ofrecen posibilidades nuevas para penetrar mas exactamente las leyes que regulan la vida general y especialmente la del hombre en sus aspectos psicológicos, económicos, sociales, etc." http://www.monografias.com/trabajos/cibernetica/cibernetica.shml

5 *v* "La jurimetría es la disciplina que tiene como propósito o razón la posibilidad de la sustitución del Juez por la computadora, finalidad que por los momentos es inaceptada, simplemente porque a través de la jurisdicción se emana una sentencia, y para ello, que mejor candidato que un ser humano que por supuesto tiene el sentido racional, con lo pueda acudir al sistema de integración y poder a través de las interpretaciones y lógica jurídica dar una sentencia llena de la interrelación de la paz y la justicia, para lograr verdaderas sociedades, verdaderas democracias y libertades." http://www.monografias.com/trabajos22/iuscibernetica/iuscibernetica.shtml

Este proceso continuo en los sesentas hasta establecer que los bancos de datos que se utilizaban en ese entonces se podía utilizar no solo para almacenar y obtener información de una manera sencilla, si no que algunas actividades jurídicas tales como certificaciones, atribuciones de juez competente, elaboración de sentencias, podían ser realizadas fácilmente auxiliándose de la informática, originándose en consecuencia la informática jurídica desicional.

Ya con la aparición de las primeras computadoras se introduce la automatización en los estudios de operadores jurídicos (jueces, abogados fiscales, asesores jurídicos) y las redes de información penetran tempestuosamente en las administraciones públicas.

Este desarrollo continua a pasos agigantados hasta que alrededor del año 1991, cuando nace la *World Wide Web.*[6]

El *Internet* también conocido como la "red de redes", es un medio masivo de comunicación constituido por dos aspectos pocos regulados jurídicamente y en constante cambio. El primero es una red computacional global interconectada principalmente por fibra óptica; y el segundo, la participación de un grupo de personas físicas o morales que conforman una comunidad virtual a la cual se le conoce como "ciberespacio"[7]. Sus características generales son la carencia de una autoridad reguladora y su carencia de dueño, por lo que *Internet* es un ente descentralizado autónomo que carece de nacionalidad tiende a crecer velozmente[8].

---

[6] "La *World Wide Web*, la *Web* o *WWW,* es un sistema de navegador *web* para extraer elementos de información llamados "documentos" o "páginas *web*". Puede referirse a "una *web*" como una página, sitio o conjunto de sitios que proveen información por los medios descritos, o a "*la Web*", que es la enorme e interconectada red disponible prácticamente en todos los sitios de Internet." http://es.wikipedia.org/wiki/Web

[7] "Palabra acuñada por William Gibson en su popular novela de ficción científica Neuroromancer, para describir la esfera dinámica cultural de la gente y las maquinas trabajando dentro de los confines de las redes computacionales." ALLISON, G. Burguess. *The Lawyer´s Guide to the Internet*, ABA, USA, 1995, p. 331.

[8] PADRÉS JIMÉNEZ, Manuel Alexandro. *La Regulación Jurídica de la Libertad de Expresión en el Internet,* ITAM, México, 1998, pp. 5-20.

Ya que el nacimiento del comercio electrónico se sitúa en 1995, principalmente al utilizar la *Internet* para los negocios y con ello la mayoría de los países del mundo en mayor o menor medida comienzan a legislar respecto al tema.

En contraparte a los beneficios que el desarrollo de la informática aparta a la humanidad, nos encontramos con la inconveniencia que casi siempre acompaña a la solución de las conductas delictivas y punibles que el gran avance tecnológico ha generado, y que han encontrado un espacio tan prolífico en el campo de la informática.

En los inicios del desarrollo de la informática y al detectarse las primeras violaciones al derecho intrínseco a ella, se pretendió desarrollar sistemas de seguridad que proporcionan la inviolabilidad de los mismos sin embargo el desarrollo de estos sistema de seguridad únicamente han presentado un reto, para los delincuentes dedicados a la violación de los mismos por que lo que diversos países se dieron a la tarea de desarrollar el derecho informático, pero en el caso de nuestro país estos esfuerzos han sido limitados ya sea por la creación de leyes demasiado particularizadas hacia un solo tipo de delito o por que los congresos estatales se han encargado de regular su ámbito de competencia sin que exista la comunión necesaria para que se le de el carácter de federal a las leyes necesarias.

El tema de derecho informático ya que es innovador dentro de las ciencias jurídicas pretende tratar de regular a los delitos informáticos se requiere que los encargados de establecer las conductas delictivas y sus correspondientes castigos y medidas de prevención estén aun paso adelante del posible delincuente, lo cual resulta un tanto difícil ya que se ha abierto la puerta a conductas antisociales y delictivos que se manifiestan de formas variadas.

Del análisis anterior podemos ver que cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. Es entonces como de este análisis

podemos decir que si bien aun no existe el derecho informático como una rama mas del derecho, si existen conductas delictivas que tienen a la informática como un conducto o herramienta para delinquir la cual trae como consecuencia el llamado delito informático el cual enseguida analizaremos.

3. Concepto de Delito Informático.

Antes de entrar directamente en materia y mostrar las distintas definiciones del delito informático, es necesario definir al delito según el Código Penal para el Estado de México, para tener una ubicación de lo que es el delito según la ley.

“Artículo 6º. El delito es la conducta típica, antijurídica, culpable y punible”.

Definir al delito informático resulta difícil ya que los conceptos básicos así como las definiciones varían de una manera importante de un país a otro, derivado esto desde el idioma utilizado, las frases y expresiones que combinan y se utilizan inclusive por cada país, esto es notorio al analizar el delito informático ya que tiene diferentes acepciones en cualquier parte del mundo.

Ya que a nivel internacional no existe una definición concreta de lo que es el delito informático la OCDE define al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.

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

Para el autor Davara Rodríguez no parece adecuado hablar de delito informático ya que, como tal, no existe si atendemos a la necesidad de una tipificación en la

legislación penal para que pueda existir un delito. Definiendo de esta manera al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada acabo utilizando un elemento informático y/o telemático o vulnerando los derechos del titular de un elemento informático, ya sea *hardware* o *software*".[9]

Determinados enfoques doctrinales subrayan que el delito informático, más que una forma especifica de delitos, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

Para el jurista Julio Téllez define a los delitos informáticos como "actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin".

Para el autor Pablo Andrés Palazzi no hay concepto formal de delito informático sino solamente hace una aproximación a una definición sobre el delito informático mencionado que "la cuestión consiste en determinar que papel juega los ordenadores es en estos hechos ilícitos. Prácticamente cualquier delito del código penal, desde el homicidio hasta el delito de fraude pueden presentar alguna relación con la informática. Sin establecer una regla genérica, podemos afirmar que una computadora puede constituir un medio para cometer un delito o el objeto sobre el cual recaiga el mimo".[10]

Por otra parte, cabe mencionar que se han formulado diferentes denominaciones además de delitos informáticos, para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos electrónicos, delincuencia informática, delincuencia de cuello blanco, abuso informático, delitos relacionados con las computadoras, crímenes por computadoras, delincuencia relacionada con el ordenador, etcétera.

---

9 DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Informático*, 4ª. ed. ARANZADI, Madrid, 2002, p. 338.

10 PALAZZI, Pablo Andrés. *Delitos Informáticos*, 1ª. ed., AD-HOC SRL, Argentina, 2000, p.33.

A grandes rasgos es lo que significa el delito informático, una conducta delictiva que esta relacionada con sistemas informáticos, y para ayudar a comprender que es un delito informático, únicamente es necesario recordar que es un delito como cualquier otro, y que únicamente para su comisión el sujeto que lo lleva acabo utiliza herramientas informáticas o de computo.

II. Elementos Jurídicos del Delito Informático

Como anteriormente mencionamos, por delito informático entendemos a cualquier actividad o conducta ilícita, susceptibles de ser sancionadas por el derecho penal, que en su realización involucre el uso indebido de los medios informáticos y para comprender la importancia de reglamentar lo concerniente a esta figura delictiva es preciso entender lo que son los elementos que conforman el delito informático llegando a desentrañar una mejor comprensión de esta figura delictiva.

Ya que el concepto de delito en general esta señalado como la violación a la ley o al mismo abandono que se tiene de esta, provocando un daño en la seguridad de los ciudadanos, y que necesariamente debe estar estipulado como tal dentro del ordenamiento jurídico aplicable.

Una vez entendido el concepto jurídico de delito anteriormente definido en el articulo 6º. del Código Penal para el Estado de México es necesario llegar al análisis de los elementos que conforman el delito informático.

Ya que se ha señalado lo que entendemos por delito, es necesario destacar que son cinco elementos jurídicos que se considera conforma al delito, y para lograr un mejor entendimiento y comprensión de este, es importante comprender cada uno de los elementos que lo conforman como son los siguientes:

1. Conducta

Debemos entender primeramente a la definición de conducta según Eduardo López Betancourt como: “La conducta es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito”[11]

Recordando que el articulo 6º. del Código Penal para el Estado de México precisa que como conducta se tomara a aquella expresión de la conducta humana que puede consistir en una acción u omisión, las cuales producirán un resultado y que un elemento particular, es que tal conducta este sancionada como elemento del delito.

Entendiendo a la acción como un hacer corporal y voluntario y como omisión, un no hacer, cuando ese hacer es esperado y se tiene el deber de no omitirlo.

También es importante mencionar la clasificación de la omisión ya que depende que tengamos una mayor comprensión, y es:

Omisión simple: consisten en omitir la ley dispositiva, es decir, se sanciona la omisión o la inactividad de sujeto al cual no produce un resultado material.

Comisión por omisión: a diferencia de la anterior clasificación, esta consiste en realizar la omisión con un resultado prohibido por la ley, es decir, la inactividad voluntaria que al infringir un mandato de hacer acarrea la violación de una norma prohibitiva causando un cambio material en el exterior.

Para el estudio correcto de este tema en particular es importante destacar que el delito informático solamente puede ser cometido por acción y no por omisión, ya que, si se considera que la capacidad del individuo se aplica a la comisión de un hecho delictivo se logra observar que dicho sujeto debe tener el objetivo determinado y específicamente de cometer tal falta, por lo que no es posible que

---

[11] LOPEZ BETANCOURT, Eduardo. *Teoría del Delito*, 7ª. ed., Porrúa, México, 1999, p. 83.

un sujeto al omitir la ejecución de una actividad, produzca como resultado la comisión del delito informático ya que este delito requiere que el individuo este plenamente seguro de lo que realiza y los medios utilizados para alcanzar su cometido.

2. Tipicidad

Para entender este elemento del delito es necesario precisar su concepto entendiendo a la tipicidad como: “la adecuación de la conducta al tipo penal”[12]

Para comprender la diferencia entre lo que es la tipicidad con el tipo penal el autor López Betancourt señala que: “Debemos tener cuidado de no confundir tipicidad con tipo; la primera se refiere a la conducta, y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito; es la formula legal a la que se debe adecuar la conducta para la existencia de un delito”[13]

Cabe señalar que la tipicidad se encuentra fundamentada en la Constitución Política de los Estados Unidos Mexicanos en su párrafo tercero, articulo 14, que a la letra dice: “En los juicios de orden criminal, queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no este decretada por una ley exactamente aplicable al delito de que se trata”

Ya que del anterior análisis es necesario tanto el tipo como la tipicidad, es decir, que permanentemente debe existir el tipo, entendiéndolo como aquella descripción previa realizada por los legisladores y plasmada en las leyes; posteriormente la tipicidad, la cual se considera como la necesaria adecuación de la conducta llevada acabo por un sujeto al tipo, por lo consiguiente dentro del delito informático deben los legisladores abarcar todos los supuestos de esta conducta criminal, no dejando alguna característica especial como lo es la capacidad intelectual que tiene los sujetos con preparación, para llevar acabo el delito informático, entendiendo a la capacidad intelectual como aquella

[12] *Ibidem,* p. 117.
[13] *Ibidem*, p.118.

preparación académica que tiene el sujeto el cual puede facilitarse y apoyarse en un momento dado a la comisión del delito informático, ya que esta característica agrava su conducta dado que el sujeto no se encuentra en las mismas condiciones que un sujeto con educación básica.

3. Antijuridicidad

Se entiende como antijuridicidad a aquello que comúnmente se aceptaría como lo contrario al derecho, pero al contravenir al derecho encontramos que el delito no es lo contrario a la ley, si no mas bien el acto que se ajusta a lo escrito en la ley penal, es decir se considera antijurídico todo actuar de un sujeto y que va en contra de las estipulaciones legales penales, y que por tal transgresión cause un daño o perjuicio social por esta violación.

Es importante para entender el concepto de antijuridicidad quede claro que la conducta o hecho son antijurídicos, cuando no son lícitos, es decir la conducta debe infringir la norma penal o una prohibición de orden jurídico.

Por consiguiente la conducta hecha por un sujeto el cual cuenta con una capacidad intelectual elevada a diferencia de un sujeto con preparación académica normal y que utiliza a la tecnología como medio para cometer un delito es importante ya que esta conducta debe de quedar clara para la adecuación de reglamentar el delito informático.

4. Culpabilidad

Este elemento lo podemos contemplar según Fernando Castellanos como: “el nexo intelectual y emocional que liga al sujeto con su acto”[14]

Ya que entendemos a la culpabilidad como un elemento básico del delito el cual lo entendemos como el nexo intelectual y emocional que une al individuo con el acto delictivo es importante entender que es el nexo el cual es definido como el

[14] CASTELLANOS TENA, Fernando. *Lineamientos Elementales del Derecho Penal*, 4ª. ed., Porrúa, México, 1999, p. 234.

fenómeno que se da entre dos entes, es decir, es la relación que existe entre el sujeto y el delito.

La culpabilidad se presenta dentro del Código Penal para el Estado de México 8º, fracción primera y segunda. En dos formas fundamentales las cuales se presentan como:

"I. Dolosos;

El delito es doloso cuando se obra conociendo los elementos del tipo penal o previendo como posible el resultado típico queriendo o aceptando la realización del hecho descrito por la ley.

II. Culposos;

El delito es culposo cuando se produce un resultado típico que no se previó siendo previsible o confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observarse según las circunstancias y condiciones personales."

Para comprender mejor lo que es la culpabilidad se explicara doctrinalmente el dolo según Fernando Castellanos como: "El dolo consiste en el actuar, conciente y voluntario dirigido a la producción de un resultado típico y antijurídico"[15].

Se entiende entonces al dolo cuando en el sujeto se ha representado en su mente la conducta que va a realizar y el resultado que va a producir, decidiendo en un acto de voluntad llevar acabo lo que en su mente se represento, y por consiguiente la conducta dolosa es intencional y voluntaria.

Para al mismo autor antes mencionado se entiende a la culpa de la siguiente manera: "existe culpa cuando se realiza la conducta sin encaminar la voluntad a la producción de un resultado típico, pero este surge a pesar de ser previsible y

[15] *Ibidem*. p. 239.

evitable, por no ponerse en juego, por negligencia o imprudencia, las cautelas o precauciones legalmente exigidas"[16].

Se entiende entonces que la culpa la encontramos cuando el sujeto no desea realizar una conducta que lleve un resultado delictivo, pero por un actuar imprudente, negligente y carente de atención, cuidados y reflexión produce una conducta que ocasiona un resultado previsiblemente delictuoso a diferencia del dolo, esta conducta es imprudencial, culposa o no intencional.

Por lo tanto y respecto a nuestro tema en particular, podemos llegar a entender que el delito informático es de tipo doloso, ya que se confirma a plenitud la voluntad del sujeto por delinquir, una característica que nos facilita la determinación de esta conducta delictiva, es la búsqueda e implementación de nuevas formas que le faciliten la comisión de tal delito, es decir, el sujeto contempla plenamente el resultado de las acciones ya que es este mismo quien a través de sus conductas pretende lograr la obtención de un beneficio para si o para otra persona, pero siempre con la claridad mental del objetivo o resultado de sus acciones.

A diferencia de los elementos anteriores del delito, dentro de este elemento en particular encontramos que existe la imputabilidad como un presupuesto de la culpabilidad.

A. Imputabilidad.

Para entender mejor lo anterior debemos aludir a lo que se considera como imputabilidad la cual se entiende como la capacidad de entender y querer un resultado establecido dentro del ámbito del derecho penal.

Se considera que un sujeto es imputable cuando este al realizar una conducta descrita en la ley como delito, esta en capacidad de conocer su ilicitud, es decir se entiende a la imputabilidad como la capacidad de querer y entender en el campo

[16] *Ibidem*. p. 248.

del derecho penal, también se podría considerar que la imputabilidad cuenta con un elemento intelectual referido a la comprensión del alcance de los actos que uno realiza y otro que establece en desear el resultado.

Con el análisis anterior de lo que es la imputabilidad queda entendido que el sujeto para que se le pueda atribuir el delito es necesario que cuente con la capacidad para entender y querer un resultado, es decir no debe de padecer algún transtorno mental temporal o permanente al momento de cometer un delito y ya que el tema que nos ocupa para poder llevarlo acabo el sujeto debe de saber y tener conocimiento del dolo que puede provocar al utilizar una herramienta tecnológica como lo es la computadora.

5. Punibilidad

La conducta, típica, antijurídica y culpable debe tener como complemento la amenaza de una pena, es decir, debe ser punible y sancionado con una pena el comportamiento delictuoso. Para Pavón Vasconcelos la punibilidad esta definida como: “la amenaza de pena que el Estado asocia a la violación de los deberes consignados en las normas jurídicas, dictadas para garantizar la permanencia del orden social”.[17]

Ya que se entiende a la punibilidad como el merecimiento de una pena, en función o por razón de la comisión de un delito, tomaremos en consideración que todo delito se aplicara una pena, llegamos entonces a comprender que la punibilidad constituye un elemento más del delito.

En este elemento como lo es la punibilidad también se puede determinar que no siempre a los sujetos que cometen actos que se contraponen a los ordenamientos legales y afectan al orden jurídico y social, le son aplicadas sanciones penales, si no otras sanciones conocidas como medidas de seguridad, recordando que la diferencia entre una sanción penal y una medida de seguridad, consiste en que el sujeto contenga una o algunas de las estipuladas dentro de nuestro ordenamiento

[17] PAVÓN VASCONCELOS, Francisco. *Manual de Derecho Penal Mexicano Parte General*, 14ª. ed., Porrúa, México, 1999, p. 497.

penal como causas de imputabilidad, es decir, que si el sujeto carece de la edad requerida para que se le pueda aplicar una sanción penal, únicamente se le podrá sancionar con una medida de seguridad, logrando llegar a uno de muchos supuestos dentro de los cuales no es necesario que exista una punibilidad aplicable al sujeto que requiere la existencia de un delito.

Del análisis anterior podemos concluir entendiendo al delito informático ya que aun no se cuenta con una definición legal concreta de lo que es esta figura jurídica, se han desglosado algunos elementos que determinan las sanciones aplicables a ciertos casos concretos según el daño que cause la utilización de la computadora para la obtención de un beneficio, pero es necesario entender que las leyes deban obligatoriamente irse adecuando a la actualidad, no dejando lugar al delito informático ya que son sancionados con penas que no constituyen una verdadera sanción para el sujeto que los comete.

Es preciso comentar que la sanción debe aplicarse de acuerdo al beneficio económico que obtuvo el sujeto al utilizar la tecnología, pero al igual, es de suma importancia atender a las facilidades y capacidades del individuo para llevarlo acabo, puesto que de ello depende la facilidad con la que cuenta el sujeto para tramar y llevar acabo la conducta delictiva, no olvidando que los sujetos que cometen los ilícitos, día a día procuran utilizar herramientas tecnológicas mas avanzadas que hacen mas difícil su captura y la sanción respectiva.

III. Presupuestos del Delito Informático

1. Sujeto Activo

Las personas que cometen los delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, el sujeto activo tiene posibilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter especial, o bien son hábiles en el uso de los sistemas informáticos, aun cuando, en mucho de los casos, no desarrollen actividades que faciliten la comisión de este tipo de delitos.

Se entiende como sujeto activo: “el hombre es sujeto activo del delito, por que únicamente el se encuentra provisto de capacidad y voluntad y puede, con su acción u omisión, infringir el ordenamiento jurídico penal. Se dice que una persona es sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible, siendo autor material del delito, o bien cuando participa en su comisión, contribuyendo a su ejecución en forma intelectual al proponer, instigar o compeler (autor intelectual) o simplemente auxiliando al autor con anterioridad a su realización, concomitantemente con ella o después de su consumación (cómplice y encubridor)”.[18]

Con el tiempo se ha podido comprobar que los que son autores de lo delitos informáticos en general son muy diversos y lo que los diferencia entre si es la naturaleza de los delitos cometidos, de esta forma la persona que ingresa a un sistema informático sin intenciones delictivas es muy diferente de cualquier sujeto con una actividad común.

El nivel de aptitud del delincuente informático es tema de controversia ya que para algunos este nivel de aptitudes no es indicador de delincuencia informática en tanto que otro 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 o un sujeto que tenga familiaridad con el mundo cibernético.

Teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, los estudiosos en la materia los han catalogado como “*White Collar Crime*” o traducido textualmente como “Delitos de Cuello Blanco” termino catalogado desde 1943 por el criminólogo norteamericano Edwin Sutherland, efectivamente este conocido criminólogo señala un sin numero de conductas que considera como delitos de cuello blanco, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de los cuales cabe destacar las violaciones a las leyes de patentes y

[18] *Ibidem,* p. 191.

marcas, de derechos de autor, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

Así mismo 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 o delincuente de cuello blanco es una persona que pertenece a grupos socioeconómicos acomodados, de prestigio social e influencia política, con fácil acceso a los servicios de salud, de educación superior, justicia, vivienda y medios de transporte propios, de ahí que resultan no marginados, si no tolerados y en parte aceptados.

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

Estadísticas demuestran que las personas que comenten delitos informáticos poseen generalmente las siguientes características:

- En generalmente son personas que no poseen antecedentes delictivos.
- La mayoría de sexo masculino.
- Actúan en forma individual.
- Poseen un inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; una actitud casi deportiva en vulnerar la seguridad de los

sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación "*hackers*"[19]

- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en si mismo.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.
- Dentro de las organizaciones, las personas que cometen fraudes han sido destacadas en su ámbito laboral como muy trabajadoras y motivadas.

2. Sujeto Pasivo

En primer termino tenemos que distinguir que el objeto pasivo o victima 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 victimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que utilizan sistemas automatizados de información, generalmente conectadas a otros.

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

[19] "El *Hacker* (del inglés *hack*, hachar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, *hardware* de red/voz, etc. Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo *hardware* o *software*. Se suele llamar *hackeo* y *hackear* a las obras propias de un *hacker*. El término "*Hacker*" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un *hacker* es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas". http://es.wikipedia.org/wiki/Hacker

Con lo anterior se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las victimas 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 victimas para que tomen medidas pertinentes a fin de prevenir la delincuencia informática, y si esto se suma a la creación de una adecuada legislación y un procedimiento que proteja los intereses de las victimas 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 campo de la lucha contra la delincuencia informática, ya que cada día tiende a expandirse mas.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de victimas 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.

3. Objeto Material

Como el delito esta formado de varios elementos, este elemento o presupuesto material lo conforman todos aquellos objetos o cosas materiales con que se cometió el delito, que constituyen su producción, es decir el objeto material lo conforman los episodios delictivos concretos no meramente a su abstracta precisión legal.

Para el autor Eduardo López Betancourt el objeto material lo define como "la persona o cosa sobre quien recae la ejecución del delito. Así, pueden ser los sujetos pasivos, las cosas inanimadas o los animales mismos."[20]

Este objeto lo pueden conformar personas, objetos, en el caso de las personas se puede observar como el sujeto pasivo de una acción delictuosa, según en diversos tipo de delitos, como por ejemplo el homicidio, lesiones, etcétera, pero a diferencia de estos delitos, cuando tratamos a las cosas como este objeto material nos podemos referir a este como su alteración o destrucción, por ejemplo, daño en propiedad ajena, contrabando, robo o fraude, etcétera.

Para el tema que nos ocupa se ha manejado el objeto material sobre el cual recae el delito puede ser el objeto inmaterial contenido en un sistema informático como la es la información la cual puede sufrir un daño o perdida de esta causando así un detrimento en el patrimonio de las personas.

Como se ha mencionado anteriormente ya que la información contenida en una computadora es fácilmente adulterable y es difícilmente comprobar que esta sufrió una alteración o daño o fue destruida, no se puede comprobar el delito como el robo o el homicidio, así entonces que es lo que la ley debe proteger respecto del delito informático.

4. Bien Jurídicamente Tutelado

Antes de comenzar será importante definir lo que es el bien jurídico tutelado el cual es "el bien o el derecho que es protegido por las leyes penales, el cual puede ser la vida, la integridad corporal, la libertad sexual, la propiedad privada, entre otros."[21]

Entendiendo que el bien jurídico tutelado no es otra cosa si no la preocupación social colectiva que es plasmada en un ordenamiento legal, que al momento de

[20] LOPEZ BETANCOURT, Eduardo, *op. cit.*, p. 57.

[21] *Ibidem*, p.58.

regular la conducta no refleja mas que la preocupación y el interés para erradicar y castigar sucesivamente el actuar de un sujeto que ponga en peligro o perjudique el bienestar social individual y colectivo de quienes conformemos la comunidad social.

Considerando el avance tecnológico de la sociedad, lo que consideramos como bien jurídico tutelado es única y exclusivamente lo que esta protegido por la norma penal, y como ejemplo se puede decir que para el delito de homicidio el bien jurídico tutelado es la vida, así como para el delito de lesiones lo es la integridad física, por lo tanto para el delito informático lo constituye el patrimonio entendido a este como sus bienes la información contenida en un sistema computacional, entendiendo lo que dañe, modifique, altere información dentro de un sistema informático para obtener un beneficio económico ya sean bienes, información o dinero, afectando así el patrimonio de las personas.

IV. Clasificación del Delito Informático

En todo delito de los llamados delitos informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometen debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y el fin que persiga debe ser la producción de un beneficio al sujeto o autor del ilícito: una finalidad deseada que causa un perjuicio a otro, o a un tercero.

Para Davara Rodríguez se pueden clasificar los delitos informáticos de acuerdo con la función y actividad que se realizan para cometerlos, ya que estos delitos centran su actividad principal en el acceso y/o manipulación de datos que se encuentran en soportes informáticos o de programas de ordenador utilizados en su procesamiento. Este autor hace una distinción de la manipulación mediante la informática en dos vertientes diferentes las cuales son:

“a) Acceso a manipulación de datos y
b) Manipulación de los programas.

Atendiendo a ello, consideramos determinadas acciones, que se podrian encuadrar dentro de lo que hemos llamado delitos informático, y, para su estudio, las clasificaremos, de acuerdo con el fin que persiguen, en seis apartados, a saber:

1. Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos,
2. Acceso a los datos y/o utilización de los mismos por quien no esta autorizado para ello,
3. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas,
4. Utilización de ordenador y/o programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro,
5. Utilización del ordenador con fines fraudulentos y,
6. Agresión a la <<privacidad>> mediante la utilización y procesamiento de datos personales con fin distinto al autorizado".[22]

El autor Julio Téllez Valdez, clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

"1. Como instrumento o medio.

En esta categoría tenemos a aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b. Variación de los activos y pasivos en la situación contable de las empresas.
c. Planeación o simulación de delitos convencionales robo, homicidio, fraude, etcétera).
d. Robo de tiempo de computadora.
e. Lectura, sustracción o copiado de información confidencial.
f. Modificación de datos tanto en la entrada como en la salida.

[22] DAVARA RODRÍGUEZ, Miguel Ángel, *op. cit.* pp. 341-343.

g. Aprovechamiento indebido o violación de un código para penetrar un sistema con el fin de introducir instrucciones inapropiadas (esto es lo que reconoce en el medio como el método del Caballo de Troya[23]).

h. variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la Técnica de Salami[24].

i. Uso no autorizado de programas de cómputo.

j. Insertar instrucciones que provocan interrupciones en la lógica interna de programas, a fin de obtener beneficios.

k. Alteración en el funcionamiento de los sistemas.

l. Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

m. Acceso a áreas informatizadas en forma no autorizada.

n. Intervención de las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo.

En esta categoría encuadramos a las conductas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

a. Programación de instrucciones que producen un bloqueo total al sistema.

b. Destrucción de programas por cualquier método.

c. Daño en la memoria.

d. Atentado físico contra la maquina o sus accesorios (discos, cintas, terminales, etcétera).

e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurológicos computarizados

f. Secuestro de soportes magnéticos, en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera."[25]

---

23 "El método del caballo de Troya es el aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas." TÉLLEZ VALDÉZ, Julio. *op. cit*. p. 165

24 "La Técnica del salami es la desviación del destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa." *Ibidem,* p.165.

25 *Ibidemt*. pp. 165,166.

También Existen diversos tipos de delitos que pueden ser cometidos ya que se encuentran ligados directamente a acciones afectadas contra los propios sistemas como son:

- Acceso no autorizado: Uso ilegitimo de *passwords*[26] y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: los daños causados en la red mediante la introducción de virus[27], bombas lógicas, etcétera.
- Infracción al *Copyright* de bases de datos: uso no autorizado de información almacenada en una base de datos.
- Interceptación de *e-.mail*[28]: lectura de un mensaje electrónico ajeno.
- Estafas Electrónicas: a través de compras realizadas haciendo uso de la red.
- Transferencia de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, *Internet* permite dar acceso para la comisión de otros tipos de delitos como son:

- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

---

26 "*Password* o contraseña. Se denomina así al método de seguridad que se utiliza para identificar a un usuario. Es frecuente su uso en redes. Se utiliza para dar acceso a personas con determinados permisos." http://www.mastermagazine.info/definicion/6239.php

27 "Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "*malware*" dentro de los virus, en el sentido estricto de esta ciencia un virus son programas que se replican y ejecutan por sí mismos. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden intencionadamente destruir datos en la computadora, aunque también existen otros más benignos, que solo se caracterizan por ser molestos. Los virus informáticos tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil." http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

28 "El Correo electrónico, o en inglés *e-mail,* es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos (normalmente por *Internet*). Esto lo hace muy útil comparado con el correo ordinario, pues es más barato y rápido. Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos." http://es.wikipedia.org/wiki/E-mail

- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitir consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de formulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas.

V. Características del Delito Informático

El delito informático como ya hemos visto se define de diferentes maneras según la necesidad de cada país y cada tema que le interese a cada autor pero sin embargo el delito informático tiene ciertas características comunes como las cuales menciona el autor Davara Rodríguez como:

"Al ser cometidos por medios informáticos o telemáticos y tener estas unas características especiales, los delitos que estamos tratando poseen peculiaridades que les hacen de alguna manera <<*sui generis*>> en cuanto a la forma de ser cometidos y en cuanto a la detección de los mismos, llegando, en algunos casos, a ser prácticamente imposible descubrir el beneficio producto de su actividad ilícita.

Enunciaremos como propias y especiales de este tipo de acciones ilícitas, y comunes a todas ellas, las siguientes características:

a. Rapidez y acercamiento, en tiempo y espacio, su comisión.
b. Facilidad para encubrir el hecho.
c. Facilidad para borrar las pruebas."[29]

El autor Julio Téllez también menciona cuales son las características del delito informático como:

[29] DAVARA RODRÍGUEZ, Miguel Ángel, *op. cit.* p. 350.

"1. Son conductas delictivas de cuello blanco (*White Collar Crimes*), en tanto que solo determinado numero de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
2. Son acciones ocupacionales por que muchas veces se realizan cuando el sujeto esta en el trabajo.
3. Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.
6. Son muchos los casos y pocas las denuncias, todo ello debido a la falta misma de la regulación jurídica a nivel internacional.
7. Son sumamente sofisticados y frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van mas allá de la intención
10. Ofrecen facilidades para su comisión a los menores de edad.
11. Tienden a proliferar cada vez mas, por lo que requieren una urgente regulación jurídica a nivel internacional"[30]

Como hemos podido darnos cuenta y conforme a lo descrito en este capítulo, nadie se imaginaba que al utilizar la tecnología, en el caso particular de la computadora se generarían conductas ilícitas que afectaran a un sujeto o mas ya sea en su persona o en su patrimonio, ya que hoy en día no es necesario utilizar una arma para causarle un daño a una persona, si no que a través de un medio informático se puede afectar a una o mas personas con teclear ciertas instrucciones que solo el lenguaje maquina comprende, es así como hoy los juristas se han puesto a estudiar y entender la combinación que existe entre el derecho y la informática para prevenir que un día la tecnología rebase los limites

[30] TÉLLEZ VALDEZ, Julio, *op. cit*., p. 163.

jurídicos establecidos, coincidiendo en que estas conductas conocidas como delitos informáticos puede se cualquier actividad ilícita susceptible de ser sancionadas por el derecho penal, que en su realización involucre el uso indebido de medios informáticos.

Asimismo como se ha visto existe un sin numero de clasificaciones de acuerdo a cada autor y de acuerdo a ciertas necesidades de lo que significa el delito informático. Independientemente de que todas estas clasificaciones antes presentadas son muy parecidas, para nuestro tema tomaremos en cuenta la clasificación que nos presenta el autor Julio Téllez, ya que las clasificaciones anteriores solo se tomaron como referencia para darnos cuenta de la diferencia que existe entre una clasificación que plantean otros autores para encuadrar los delitos informáticos dentro de sus necesidades

CAPÍTULO TERCERO
LEGISLACIÓN DEL DELITO INFORMÁTICO

I. Marco Jurídico Internacional del Derecho Informático

La legislación sobre la protección de sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación solo en aquellos aspectos en los que, basándose en 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, físicas y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas. Actualmente no solo nos encontramos frente al peligro de la informática sino frente a la posibilidad real de que individuos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de la privacidad, las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de la tecnología informática.

Es por eso que a continuación se realiza un estudio comparativo entre la legislación internacional y nuestra legislación, en donde se presentaran las legislaciones de diferentes países, ya que se han preocupado por disponer una legislación adecuada para regular la problemática que existe en el ámbito de la informática. Así mas adelante se podrá analizar y observar cuales son las medidas de seguridad que se podrá implantar dentro de la legislación nacional.

1. Tratados Internacionales celebrados por México

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes, es por eso que organismos

internacionales han comenzado a regular el delito informático sumando esfuerzos y creando acuerdos para proteger a personas físicas y jurídicas, y al mismo tiempo no se vean afectados en detrimento de su patrimonio.

A. ONU[1]

Actualmente en el ámbito internacional los organismos internacionales tienen como característica, la falta de acuerdos globales acerca de que tipos de conductas deben constituir delitos informáticos[2], ya que dada las diferentes legislaciones de una nación a otra existen conductas tipificadas como delito en algunos países mientras que en otras no es así, por ello tanto existe una ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

La Organización de las Naciones Unidas, en el marco del Octavo Congreso sobre prevención del delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se estableció que la delincuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había definido la comisión de actos delictivos.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, físicas y jurídicas, en aspectos fundamentales para el normal desarrollo y funcionamiento de diversas actividades bancarias, financieras, tributarias, provisionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las mas diversas disciplinas a un estado o particulares, es decir, no son los grandes sistemas de información los que afectan la vida privada si no la manipulación o el consentimiento de ello, por parte de los

[1] La Organización de las Naciones Unidas, que es conocida por sus siglas en ingles ONU (*Nationes Unit Organization)* es una organización internacional constituida para suceder a la Sociedad de Naciones para los Estados que aceptaron cumplir las obligaciones previstas por la Carta de las Naciones Unidas, firmada en San Francisco el 26 de Junio de 1945, a fin de instituir entre las naciones una cooperación económica, social y cultural. La ONU cuya sede se halla en Nueva York, comenzó a existir oficialmente el 24 de Octubre de 1945.
[2] Ver Anexo 1.

individuos poco concientes e irresponsables de los datos que dichos sistemas contienen.

Por otra parte el Manual de las naciones Unidas para la Prevención y Control de los Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

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 aumentan de modo creciente aun en países latinoamericanos, que 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 critica de un país como para los legisladores, las autoridades policíacas encargadas de las investigaciones y los funcionarios judiciales.

B. UNESCO[3]

Otro órgano internacional el cual esta interesado en proteger especialmente los derechos humanos de mujeres y niños que se ven afectados en su persona ya que son objeto de abusos y en especifico de la producción de pornografía distribuida a través de *Internet* es la UNESCO.

Este organismo, en sus pronunciamientos relativos a las autopistas de la información ha declarado que el aumento del acceso a redes y bases de datos interconectadas incrementan el valor de los principios éticos y legales incluyendo: la privacidad de la información y el derecho que tiene cada individuo a revisar sus

[3] La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, conocida por sus siglas UNESCO (*United Nations Educational Scientific and Cultural Organization*) es una institución de la ONU, creada en 1945-1946 con el objetivo de contribuir al mantenimiento de la paz y de la seguridad internacionales, estrechando la colaboración entre las naciones a través de la educación, la ciencia y la cultura, a garantizar el respeto de los derechos humanos y las libertades fundamentales. Su sede se encuentra en Paris.

propios datos como derecho humano fundamental, la lucha contra la piratería internacional y otros delitos, y la protección de los derechos de los creadores del *Software.*

Actualmente la propia UNESCO se ha pronunciado en contra del uso que se esta dando a estas redes de alcance global para la difusión de pornografía, y el comercio de mujeres e incluso de niños.

Las implicaciones de la delincuencia informática en su carácter internacional u el peligro de que la diferente protección jurídico penal nacional pudiera perjudicar el flujo internacional de información, conducen por consecuencia a un intercambio de opiniones y de propuestas de solución sobre la base de las posturas y de las deliberaciones surge un análisis comparativo de los derechos nacionales aplicables así como de las propuestas de reforma, las conclusiones político jurídicas condujeron en una lista de acciones que pudieran ser consideradas por los estados como mecedoras de una pena.

C. OCDE[4]

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

En 1983, la Organización de Cooperación y Desarrollo Económico inicio un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

[4] La Organización de Cooperación y Desarrollo Económico conocida por sus siglas OCDE (*Development Economic and Cooperation Organitation of*), es una organización internacional constituida en Paris en 1961. Sucesora de la OECE Organización Europea de Cooperación Económica, fundada en 1948 por los estados beneficiarios del Plan Marshal, fue instituida por 20 países de Europa Occidental y de América del Norte; actualmente, tras su progresiva ampliación, tiene 30 estados miembros, a los que ofrece un marco en el que analizan, elaboran y mejoran de modo concertado sus políticas económicas y sociales.

La OCDE, es una organización internacional intergubernamental que reúne a los países mas industrializados de economía, de mercado, en la OCDE, los representantes de los países miembros se reúnen para intercambiarla información y armonizar políticas con el objeto de maximizar su conocimiento económico y coadyuvar a su desarrollo y al de países no miembros.

En 1992, la OCDE elaboro un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los estados y el sector privado pudieran elegir un marco de seguridad para los sistemas informáticos el mismo año.

D. AIDP.[5]

La Asociación Internacional de Derecho Penal celebro en 1992 en Wurzburgo un coloquio en el que adopto diversas recomendaciones respecto a los delitos informáticos y otros delitos relativos a la tecnología de la información, estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no hasta con la adopción de otras medidas, además las nuevas disposiciones deberán ser precisas, claras y con la fidelidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es de limitar la responsabilidad penal con el objeto de que estos queden circunscritos primordialmente a los actos deliberados.

[5] La Asociación Internacional de Derecho Penal, conocida por sus siglas AIDP (*The Internacional Association of Penal Law*) creada en 1924 como sucesora de la Unión Internacional de Derecho Penal, constituye la más antigua organización mundial que reúne especialistas de las ciencias penales y una de las sociedades culturales mas antiguas del mundo. En especial, la AIDP ha desempeñado un papel muy importante en el establecimiento de una corte penal internacional permanente, a través de sus múltiples actividades, reuniones, publicaciones, así como de los congresos y comités de expertos organizados en colaboración con el instituto superior internacional en ciencias criminales (ISICC, Siracusa, Italia), que se encuentra bajo la tutela científica de la asociación.

Esta asociación considera el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, y recomienda que los estados deberán considerar de conformidad con sus tradiciones jurídicas, su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la lista facultativa, especialmente a la alteración de datos de computadoras y el espionaje informático, así como que por lo que se refiere al delito de acceso no autorizado , es conveniente precisar mas al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

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

Dada la presente situación de la delincuencia informática se debe considerar que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes para la dimensión internacional que caracteriza este problema, es por eso que para solucionar los problemas derivados del uso de la informática es necesario que se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada, durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

2. Legislaciones de otros países respecto al Delito Informático

Es preciso señalar que a nivel mundial diferentes países han logrado introducir en sus legislaciones correspondientes la regulación de los delitos de vanguardia tecnológica. Actualmente podemos encontrar que en varios países las legislaciones ya cuentan con estipulaciones referentes al buen uso de los medios informáticos.

El aumento de resultados favorables obtenidos en la búsqueda de legislaciones que comprendan el ingreso y consideración de esta nueva tecnología, a nivel

internacional, pues dependen diferentes razones para cada nación en llevar acabo las reglamentaciones correspondientes.

En el contexto internacional, pocos son los países que cuentan con una legislación apropiada y entre ellos se destacan los siguientes:

A. Alemania

En Alemania para resolver la delincuencia informática en 1986 adopta la Ley contra la Criminalidad Económica que contempla los siguientes delitos: a) espionaje de datos; b) estafa informática; c) alteración de datos, y d) sabotaje informático.

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 tubo que reflexionar acerca de donde radicaban las verdaderas dificultades para la aplicación del derecho penal tradicional a comportamientos dañosos en los que se desempeñan un papel esencial, la introducción del proceso electrónico de datos, así como acerca de que bienes jurídicos merecedores de protección penal resultaban así lesionados.

B. Argentina

En Argentina respecto de la legislación informática cuenta con el anteproyecto de ley de delitos informáticos el cual contiene apartados diversos que pretenden ser el primer paso para regular los delitos informáticos los cuales son: a) acceso ilegitimo informático; b) daño informático; c) fraude informático, y d) disposiciones comunes.

C. Chile

Otra nación que ya cuenta con un ordenamiento legal que comprende a los delitos informáticos dentro de su legislación cuenta con la Ley Relativa a los Delitos Informáticos, en donde esta ley se refiere a los siguientes delitos: a) la destrucción

o inutilización de los datos contenidos dentro de una computadora; b) conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento, y c) conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

D. Costa Rica

El país de Costa Rica también constituye uno de los países que cuentan con un principio dentro de la legislación de los elementos informáticos y actualmente cuenta con la legislación sobre delitos informáticos. Este ordenamiento penal determina claramente lo referente al delito de fraude cometido por elementos informáticos.

E. España

En España establece, en su legislación sobre delitos informáticos, que al que causare daños en propiedad ajena, se le aplicara pena de prisión o multa, en lo referente a: a) la realización por cualquier medio de destrucción, alteración, inutilización o cualquier oro daño a los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos; b) la violación de secretos, el espionaje o la divulgación y, c) en materia de estafas electrónicas solo tipifican las estafas con animo de lucro valiéndose de alguna manipulación informática.

F. Estados Unidos

Este país adopto en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionadas con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de julio del año 2000, el senado y la cámara de representantes de este país establece el acta de firmas electrónicas en el comercio global y nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante *Internet*, entre empresas y entre empresas y consumidores.

G. Perú

Por ultimo encontramos que un país como Perú no pudiera tener algún avance dentro de su legislación de delitos informáticos pero actualmente cuanta con esta y aventaja a otras naciones respecto al delito informático y se incorporo dentro de su código penal las siguientes conductas: a) la indebida utilización de una base de datos, sistema o red de computadoras con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información, y b) el que indebidamente interfiera, reciba, altere, utilice, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base o sistema de red.

Por ultimo es importante destacar que el objetivo de los legisladores y de organismos internacionales es aumentar la protección a los individuos y su patrimonio así como a negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas cumputalizados creados legalmente. Es decir, los legisladores y organizaciones internacionales han considerado que el aumento de la tecnología de las 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 y sus bienes, así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras mas relacionadas con al utilización de computadoras, sistemas y bases de datos.

II. Marco Jurídico Nacional del Delito Informático

Para el desarrollo de este capitulo se analizara la legislación que regula penalmente las conductas ilícitas relacionadas con la informática pero que aun les falta algunos aspectos que considerar para salvaguardar el bienestar del individuo y sus bienes.

Actualmente los delitos informáticos constituyen una laguna en nuestras leyes penales, así pues podemos decir que se necesita hacer un estudio de las pocas legislaciones penales que regulan las conductas ilícitas hechas a través de una computadora.

La problemática de los delitos informáticos requiere un estudio especial en nuestro país con la finalidad de adecuar todas aquellas conductas ilícitas relacionadas, tomando todo tipo de medidas en nuestra legislación tanto local como federal. Los programas de computación, las bases de datos y las infracciones derivadas actualmente se encuentran ordenados en ordenamientos administrativos como la Ley Federal de Derechos de Autor y el Código de Comercio respecto de la firma electrónica, pero nunca de manera directa y real el uso de los medios informáticos y de el *Internet* como medios y objetos básicos e indispensables para la comisión de dichas conductas delictivas.

1. Constitución Política de los Estados Unidos Mexicanos

Nuestra constitución política en su parte dogmática contiene garantías que todo individuo gozara como son la libertad de expresión, que se contempla en su artículo 6 que a la letra dice:

“artículo 6o.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el estado.”

Y la libertad de imprenta contemplada en su artículo 7º que dice:

“articulo 7o.- Es inviolable la libertad de escribir y publicar escritos sobre cualquiera materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz publica. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.”

Así como la garantía de legalidad respecto a las molestias en su persona o posesiones en el artículo 16 primer párrafo que dice:

“artículo 16**.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento.”

Estas garantías con las que cuenta cualquier individuo nos da pauta para establecer el fundamento constitucional en que se basa la investigación sobre el delito informático y que debería estar regulado ya que este delito solo se encuentra regulado en diferentes ordenamientos administrativos los cuales anteriormente mencionados y muy poco regulado en ordenamientos penales como mas adelante se expondrán.

Ya que el derecho penal tiene la función de proporcionar seguridad al usuario, al creador de programas, al inversionista, la seguridad de cualquier conducta que pudiera afectar sus intereses se debe prever y en su caso castigar las conductas realizadas a través del uso de la informática.

Para ello los fundamentos deben de estar contenidos antes que nada en nuestra constitución ya que esta debe de prever que se tomen las medidas necesarias para que se pueda proteger tanto al individuo como a sus bienes, es decir, ya que el estado es el guardián que debe cuidar nuestros derechos en todo ámbito, tanto el de ser un usuario de la informática, así como el de proteger la intervención de

la intimidad[6], proteger la información de todo tipo para tener seguridad de que no estamos desprotegidos y se haga un mal uso de información encontrada en una computadora o base de datos.

De esta manera se puede observar que en el artículo 16 se encuentra regulada la garantía de seguridad jurídica, y que es sin duda un ordenamiento amplio y suficiente que garantiza el derecho a la privacidad, a la intimidad de los individuos, ya que regula con precisión los requisitos que deben reunir un mandamiento legal transcrito, mediante el cual pueda afectarse o molestarse a la persona con la utilización de algún medio electrónico.

2. Código Penal Federal

A través del tiempo nuestra legislación mexicana ha encontrado diversas disposiciones con la finalidad de regular la conducta del hombre, para así vivir en armonía y en beneficio de la sociedad. A lo largo del tiempo, de las costumbres y de las tecnologías, así como las necesidades del individuo van aumentando, es de modo importante la creación de legislaciones y procedimientos que regulen distintas actividades del ser humano, de tal manera que el progreso con el que el hombre se va desarrollando sea conforme a derecho.

Los legisladores desde 1999 se han dado a la tarea de crear una reforma legislativa y punitiva para la prevención y penalización de esta conducta, creando un apartado que regula y penaliza el acceso ilegal a los sistemas y equipos de computo tanto públicos como privados; así como de la tutela y protección de la información oficial, comercial y personal, contenida en dichas computadoras. Estas últimas reformas hechas al Código Penal Federal referentes a la utilización de la informática se encuentran dentro del Titulo Noveno, Capítulo Segundo, en los artículos 211-Bis al 211-Bis7.[7]

---

6 "…el derecho a la intimidad se concibe en problemática relación con el derecho de y a la información, fundado en la dignidad de la persona humana, tendiente al libre y pleno desarrollo de su personalidad. Contiene en sí, un despliegue privatístico, que propende a la garantía de la libertad personal." PARELLADA, Carlos Alberto. *Daño en la Actividad Judicial e Informática desde la Responsabilidad Profesional*, ASTREDA, Argentina, 1990, p. 194.

7 Ver Anexo 2.

También dentro de dicho ordenamiento encontramos ciertos delitos referentes al uso de la informática como son:

- Modificación, destrucción o provocar la perdida de información contenidas en equipos informáticos.
- Conocer o copiar información contenida en sistemas o equipos.
- Uso y/o reproducción no autorizada de programas informáticos con fines de lucro.
- Ataques a las vías de comunicación y obtención de información que pasa por el medio de comunicación.
- Pornografía infantil.
- Asociación delictuosa y pandilla.

Respecto a las reformas hechas al Titulo Noveno se observa que las expectativas generadas por la publicación de este ordenamiento, superaron su contenido y aplicación practica, el cual involuntariamente representa solamente un pequeño avance en cuanto a la estructuración de una legislación amplia, ya que aun falta por proteger aspectos de suma importancia ya que es necesario que las consecuencias realizadas por los delitos informáticos el bien jurídico a tutelar será la intimidad, la fe publica, el honor, la dignidad, situaciones que nuestra legislación penal todavía no protege.

3. Código Penal del Estado de Sinaloa

Al estar constituido nuestro país como una republica representativa, democrática, federal, en la que los estados que la integran son libres y soberanos en cuanto a su régimen interior, si bien unidos por un pacto federal, encontramos que en la actualidad los asuntos informáticos que inciden en el ámbito del derecho penal, pueden ser regulados por cada una de las entidades federativas a su libre y mejor perecer.

Los estados pueden regular, en el ámbito de su competencia, las materias que no estén expresamente reservadas a la federación (establecido en el articulo 124

Constitucional); por lo que en esta esfera estarían los contratos civiles electrónicos, los delitos informáticos que inciden en el orden común, la admisión de documentos o medios electrónicos como prueba en los procesos penales, la protección a bases de datos privados y todo aquel asunto que no toque materia federal.

Dentro de diferentes legislaciones constituidas dentro de las cuales se encuentra el Estado de Sinaloa, fue muy difícil encontrar principios de legislación interna que tenga como elemento que lo conforme, a algún precepto que pretenda regular alguna actividad delictiva referente al uso de la informática.

No debemos olvidar que lo tipificado en los códigos estatales, solo aplicara para los delitos cometidos dentro de su territorio y por residentes del mismo (establecido en el artículo 121, fracción I, Constitucional).

El delito informático contemplado en esta legislación transcrito íntegramente esta definido de esta manera:

“LIBRO PRIMERO. PARTE GENERAL
TÍTULO PRELIMINAR. DE LAS GARANTÍAS PENALES
CAPÍTULO ÚNICO: DE LAS GARANTÍAS PENALES
CAPÍTULO V: DELITO INFORMÁTICO
ARTÍCULO 217. Comete delito informático, la persona que dolosamente y sin derecho:
I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.”

Se considera que la importancia y la necesidad es mayor cada momento y es preciso que otras legislaciones estatales comienzan legislar por primera vez lo que se refiere a la comisión del delito informático, es decir, con lo anterior se demuestra la gran importancia que consiste en lograr una plena y actual legislación de las nuevas tendencias delictivas dentro de nuestro ordenamiento penal.

4. Código de Comercio

En nuestro país debido a factores como el auge del comercio electrónico o *e-commerce*[8] como se conoce a nivel mundial, la aprobación de la firma digital hace que se trabaje en la estructuración de una ley que le brinde un marco legal a las prácticas del comercio electrónico (las transacciones por *Internet*) en nuestro país.

Para comprender mejor lo que es el comercio electrónico y las ventajas que ofrece entenderemos por comercio electrónico a la compraventa de productos y la contratación de servicios a través de *Internet*.

La transacción típica del comercio electrónico incluye tres fases. En la primera, un comprador potencial accede a una página *Web* para obtener información sobre cierto producto que le interesa adquirir. En la segunda fase, el comprador manifiesta su aceptación enviando una orden de pago al vendedor. Finalmente, el vendedor procesa la orden de pago y hace entrega del producto o prestación de servicio al cliente.

Las ventajas del comercio electrónico son evidentes: no hay que sujetarse a los horarios de las tiendas comerciales, se ahorra tiempo, se evita el estrés de las

[8] "El comercio electrónico (en inglés *Electronic Commerce, E-Commerce, ecommerce* o *EC*) consiste principalmente en la distribución, compra, venta, mercadotecnia y suministro de información complementaria para productos o servicios a través de redes informáticas como *Internet* u otras. La industria de la tecnología de la información podría verlo como una aplicación informática dirigida a realizar transacciones comerciales. Una definición alternativa lo vería como la conducción de comunicaciones de negocios comerciales y su dirección a través de métodos electrónicos como intercambio electrónico de datos y sistemas automáticos de recolección de datos. El comercio electrónico también incluye la transferencia de información entre empresas". http://es.wikipedia.org/wiki/Comercio_electronico

compras, puede ordenarse la mercancía de manera sencilla, se puede obtener información muy completa del producto que se desea adquirir, además de que permite el contacto y la compra directamente del productor. Al eliminar la intermediación de precios, en beneficio del consumidor.

La primera vez que se legislo en materia de comercio electrónico en México fue en mayo del 2000, con las primeras reformas realizadas al Código de Comercio, posteriormente, en Agosto de 2003, se volvió a reformar el mismo ordenamiento incorporando en su Titulo Segundo referente al comercio electrónico[9], autorizando el empleo de medios electrónicas, ópticos y de cualquier otra tecnología en los actos de comercio y la formación de los mismos, sentando las bases de lo que se entiende por mensaje de datos y firma electrónica, estableciendo la necesidad de que se confirme el vinculo entre un firmante y los datos de creación de la firma electrónica mediante un certificado, que deberá de ser expedidos por un prestador de servicios de certificación autorizado en este caso por la Secretaria de Economía.

El Código de Comercio dicta los lineamientos para determinar cuando y donde se presume que un mensaje de datos ha sido enviado y recibido, las formalidades a seguir cuando el acto deba constar por escrito o ante fedatario publico, los requisitos para que una firma electrónica se considere fiable, las obligaciones del firmante y del destinatario, los requisitos para ser prestador de servicio de certificación, las obligaciones de los prestadores de servicio de certificación, las obligaciones de los prestadores de este servicio y los elementos de un certificado (nacional o extranjero) valido.

La situación del comercio electrónico parte desde sus características propias para las cuales debe considerarse que comprende no solo las ventajas o adquisiciones que el empresario y el usuario realizan a través de *Internet,* si no que engloba también todas las fases del negocio empresarial, siempre que esta se realicen a través de la red.

9 Ver Anexo 3.

Pueden sufrir conflictos relativos a la defensa de la propiedad intelectual, al incumplimiento de obligaciones contractuales, problemas con la firma virtual y en el ámbito penal delitos de diferente índole como difamación, fraude, entre otros.

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

5. Ley Federal de Derechos de Autor

A. Orígenes de los Derechos de Autor

Los antecedentes de los derechos de autor, hoy mejor conocido como *copyright* "©"[10] son difíciles de establecer ya que no existe fecha determinada en donde se encuentre plasmada la actividad intelectual y artística que ha existido durante siglos en el mundo. Dado que la característica primordial y fundamental del hombre en mayor o menor grado es la capacidad de crear, la creación intelectual es, en algunos casos innata y en otros adquirida. El Hombre para facilitarse la vida creaba cosas y al mismo tiempo dejaba huella de su historia a través de pinturas rupestres, obras plásticas, la creación de herramientas, etcétera, las cuales mostraban sus creencias, su cultura, sus costumbres y valores retratando

[10] "El símbolo del *copyright* "©" es usado para indicar que una obra está sujeta al derecho de autor. El derecho de autor (del francés *droit d'auteur*) es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado. En el derecho anglosajón se utiliza la noción de *copyright* que, por lo general, comprende la parte patrimonial de los derechos de autor. Una obra pasa al dominio público cuando los derechos patrimoniales han expirado. Esto sucede habitualmente trascurrido un plazo desde la muerte del autor. Por ejemplo, en el derecho europeo, 70 años desde la muerte del autor. Dicha obra entonces puede ser utilizada en forma libre, respetando los derechos morales." http://es.wikipedia.org/wiki/Copyright

a si a su sociedad, se podría decir que así nacieron las figuras jurídicas que hoy conocemos como derechos de autor o *copyright* y otros derechos de propiedad industrial.

Todo creador de una obra intelectual, sea esta artística -pintura, escultura, danza, arquitectura, etcétera- literaria, musical o de cómputo, es un autor. Para protegerlos a el y a su obra respecto del reconocimiento de su calidad autoral es decir es la facultad de oponerse a cualquier modificación de su creación sin su consentimiento, así como para el uso o explotación por si mismo o por terceros, existe un conjunto de normas denominados derechos de autor.

B. Regulación del Derecho de Autor

La legislación sobre el derecho de autor cambia de un país a otro. Las leyes de cada país difieren especialmente en los siguientes puntos: a) el plazo de protección, en la mayoría de los países, los derechos de autor expiran no mas allá de 70 años tras la muerte del autor, b) la situación de las obras de Estado, en muchos países los documentos publicados por el Estado para uso oficial están en el dominio publico, y c) el tipo de materia sujeto a derecho de autor.

En la actualidad y tal como lo establece la Ley de Propiedad Intelectual que data de 11 de Noviembre de 1987, puede decirse de modo general que, en caso mas simple y frecuente de un solo autor, los derechos de explotación de la obra duran toda la vida del autor y 70 años después de su muerte o declaración de fallecimiento.

Esta ley explícitamente recoge en el artículo 31 el derecho a la copia privada, es decir, el derecho a hacer copias privadas sin permiso del autor siempre que no exista animo de lucro y la obra haya sido ya hecha pública. Para compensar a los autores, introduce el pago de un canón compensatorio asociado a algunos soportes de grabación. Una excepción a la copia privada es el caso del *software,* donde solo se pueden hacer copias de seguridad, es decir, es necesario ser propietario del original para que la copia sea legal.

En cuanto a descargar obras a través de *Internet,* abogados especializados y asociaciones de consumidores afirman que es legal dentro del marco de la legislación actual, amparándose en el derecho de copia privada y siempre que no haya animo de lucro. Además, según el Código Penal, es imprescindible que haya ánimo de lucro para que exista un delito contra la propiedad intelectual.

Esta ley se encuentra fundamentada en la Constitución a través de sus artículos 6º, 7º y es reglamentaria del artículo 28.

La Ley Federal de Derechos de Autor, define a los derechos de autor, de la siguiente manera: “Articulo 11. El derecho de autor es el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el patrimonial”.

La finalidad de la protección de los derechos de autor es proteger los resultados de la creatividad intelectual, otorgando seguridad jurídica a toda obra intelectual o artística, dándole a su autor un monopolio sobre la reproducción y difusión de su obra.

La Ley Federal de Derechos de Autor reconoce dos grandes categorías fundamentales del derecho de autor, unos se han denominado derechos morales y los segundos que se han llamado derechos patrimoniales.

Los Derechos Morales, se derivan básicamente de la relación personal existente entre el autor y su obra. El autor realiza la creación de una obra, imprime en ella su capacidad para sentir, apreciar o investigar, por lo cual considera que el autor es el único que puede ser titular originario de un derecho sobre su obra.

Los Derechos Patrimoniales o Económicos se consideran que comienzan a existir desde el momento en que el autor divulga su obra, por cualquier medio de comunicación. Este derecho es considerado como la facultad que posee el autor de obtener una retribución por la explotación o uso público de sus obra con fines

de lucro, es decir, consideran que este derecho especifica la obtención de alguna ganancia para el autor, debido a que su obra es una consecuencia de su trabajo.

C. Marco Jurídico Existente para la Protección de Programas de Cómputo y Bases de Datos

La Ley Federal de Derecho de Autor en su artículo 101 define los programas de cómputo como: “la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica”

La ley protege programas tanto operativos como aplicativos y deja fuera a los que tienen por objeto causar efectos nocivos.

Autoriza al usuario legítimo a hacer las copias que le permita la licencia o bien, una sola que sea indispensable para la utilización del programa o sea destinada solo para resguardo.

El autor tiene derecho de prohibir además de la reproducción, la traducción o adaptación o arreglo al programa, así como a su distribución o de compilación.

Se prohíbe además la importación, fabricación, distribución y utilización de aparatos o prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo.

La violación de lo anterior, constituye una infracción en materia de comercio, sancionada con multa por el Instituto Mexicano de la Propiedad Intelectual.

6. Ley de la Propiedad Industrial

A. Origines y Antecedentes de la Propiedad Industrial

Al igual que los derechos de autor en la propiedad industrial no existe fecha determinada que establezca cuando se crea la Propiedad Industrial ya que cuando el hombre creaba herramientas, utensilios, aparatos o modificaba objetos no eran necesarios registrarlos ya que cuando el hacia una creación los demás hombres de su sociedad comenzaban a utilizarlo de forma común o cotidiana para la elaboración de sus actividades.

En los inicios de la civilización los inventos pasaban desapercibidos ya que el progreso técnico era muy lento, es probable que el propio inventor no distinguiese lo que era el producto de su imaginación, no fue hasta la Edad Media en que los soberanos comenzaron a otorgar privilegios con el objeto de fomentar manufacturas, este es el primer antecesor de lo que se conoce hoy como "patente".[11]

B. Aspectos Generales de la Propiedad Industrial en México

La Propiedad Industrial es el derecho exclusivo que otorga el Estado para usar o explotar en forma industrial y comercial las invenciones o innovaciones de aplicación industrial o indicadores comerciales que realizan individuos o empresas para distinguir sus productos o servicios ante la clientela en el mercado.

Este derecho confiere a su titular la facultad de excluir a otros del uso o explotación comercial de su prioridad si no cuenta con su autorización. La protección en nuestro país solo es valida en el territorio nacional y su duración depende de la figura jurídica para la cual se solicita su protección.

La propiedad industrial promueve y protege:

[11] "PATENTE. Autorización expedida por autoridad competente para el ejercicio de alguna actividad o función, hecha constar en documento autentico. // También se denomina así al Derecho de explotar en forma exclusiva un invento en sus mejoras. Asimismo recibe el nombre de patente el documento expedido por el Estado, en el que se reconoce y confiere tal Derecho de exclusividad". DE PINA VARA, Rafael. *Diccionario de Derecho*, 28ª ed., Porrúa, México, 2000, p. 398.

- La realización de invenciones e innovaciones a través de la protección de patentes, modelos de utilidad, diseños industriales y secretos industriales.
- La creación de signos distintivos como son: marcas, avisos y nombres comerciales y las denominaciones de origen.
- La protección jurídica de la propiedad industrial estimula a las empresas a emprender mejoras en sus proceso de producción, productos y formas de comercialización que utilizan en sus actividades de producción y comercialización, para reforzar su competitividad y obtener un mayor beneficio económico, sin verse afectados negativamente por la copia o imitación no autorizada de las mismas.

Si bien tanto la Ley de Derechos de Autor con la Ley de la Propiedad Industrial son reglamentarias del artículo 28 constitucional ambas son leyes administrativas en donde la primera menciona la protección a los programas de computación y las bases de datos en su capitulo cuarto, pero sin embargo no contempla las acciones o delitos que se pudieran cometer contra estos, y en la Ley Federal de Propiedad Industrial en su artículo 19 fracción IV se menciona que no se protegerán a los programas de computo ya que no se considera una invención para los efectos de esta ley, pero si se hace mención de las conductas que pudieran ser contempladas como delitos pero solamente para marcas, patentes, diseños industriales, contemplados solamente por la ley de la propiedad industrial y no protege a los programas de computación ni las bases de datos y estas están contempladas en el artículo 223 de la ley referida.

Ya que se ha hecho un análisis de estas dos leyes y de acuerdo a la experiencia histórica, se demuestra que para que nuestro país pueda proteger con eficacia a los programas de computo, las bases de datos así como su uso debe contar con un marco jurídico moderno, amplio, especifico y acorde a la realidad en que vivimos, que propicie un mejor ambiente para que los creadores puedan darse a la misión de acrecentar y elevar nuestro acervo cultural, y que establezcan las bases para un futuro con mejores expectativas en la educación, la ciencia, el arte y la cultura en donde la tarea principal del Estado es la de garantizar el respeto a la tutela de las obras del ingenio humano, ellos responde a la evidente

importancia que para el desarrollo cultural de cualquier civilización han tenido las ideas, cuya fuente primordial es el ser humano y su patrimonio.

7. Código Penal para el Estado de México.

Dentro de nuestra legislación penal nos damos cuenta que el Código Penal para el Estado de México no cuenta con tipos penales relacionados con el mal uso de las computadoras, lo cual da lugar a que se busque una modificación en esta legislación.

Con esto nos damos cuenta de que si alguien destruye, mediante los medios que sean, la información almacenada en una computadora no comete un delito, pero sin en cambio rompe el *Hardware* será penalizado. Estos ordenamientos sancionan algunos delitos contra el honor, robos, fraudes, falsificaciones, trafico de menores, pornografía, narcotráfico, etcétera., todas estas conductas pueden ser cometidas utilizando como medio la tecnología electrónica, pero nada se refiere a los delitos cometidos sobre la información como un "bien"[12].

Un inconveniente y el cual no hay forma de probarse era el estado anterior de los datos contenidos dentro de una computadora, puesto que la información en estado digital es fácilmente adulterable, el problema surge en que los datos almacenados tienen el valor que el dueño de esos datos le asigna y que forman parte de su patrimonio, ya que son bienes intangibles en donde solo el individuo puede valorar los datos almacenados.

Ya que en esta legislación antes mencionada y ante la inexistencia de normas que tipifique delitos cometidos a través de una computadora, es necesario y de suma importancia que la ley contemple accesos ilegales a las redes como a sus medios de transmisión.

[12] "BIEN. Cosa material o inmaterial susceptible de producir algún beneficio de carácter patrimonial". *Ibidem.* p.126.

CAPÍTULO CUARTO
LA CONVENIENCIA DE REGULAR EL DELITO INFORMÁTICO

I. Exposición de Motivos.

El análisis del presente trabajo tiene como finalidad demostrar el vacío legislativo, que tienen los diferentes ordenamientos legales, creado por el vertiginoso desarrollo tecnológico que han sufrido los sistemas informáticos en los últimos años, los cuales han cambiado los hábitos y costumbres de una gran parte de la población nacional y mundial, generando con ello nuevas figuras delictivas que deben ser sancionadas, para evitar la impunidad.

Estas figuras delictivas que vienen aumentando conforme se magnifica el uso de los sistemas informáticos, volviéndose más complejos conforme avanza la tecnología, motivo por el cual se generan ciertos problemas al momento de legislar en la materia, como determinar la jurisdicción competente cuando se realiza un ilícito, los delitos cometidos a distancia o los daños ubicados desde paginas *web* ubicadas en otros estados, así como también es un problema latente la forma de obtención de medios probatorios e identificación del autor del ilícito.

Es de suma importancia tener presente que la informática a inundado el mundo, llegando a los lugares mas alejados ya que aun en donde no hay energía o corrientes eléctricas las personas pueden utilizar la *Internet* en cualquier momento, ya que ahora cualquier persona que tenga una *Laptoc* o computadora personal sofisticada (ya que actualmente estas operan a través de comunicaciones inalámbricas o vía satélite) puede utilizar esta herramienta, así mismo mediante la telefonía celular se pueden efectuar operaciones bancarias desde cualquier parte, lo cual puede permitir que personas inescrupulosas accedan a su información y puedan aprovecharse de la misma en perjuicio de sus propietarios.

Cabe señalar que los delitos informáticos más comunes son:

La pornografía, que es una de las fuentes más prominentes y que mueve más dinero que muchas empresas multinacionales. Las autoridades policiales y las organizaciones no gubernamentales están muy preocupadas por que la pornografía infantil vía *Internet* sigue creciendo a pasos agigantados pese a todos los esfuerzos realizados para erradicarla.

Los fraudes, subastas y ventas ilegales en *Internet* están a la orden del día, ya que empresas ficticias que se valen de la buena fe de las personas consiguen adueñarse de grandes cantidades de dinero a costa de los incautos clientes.

El sabotaje informático, el cual es llevado acabo en la mayoría de los casos por empleados descontentos.

Delitos contra la propiedad intelectual como lo es el pirateo de programas de computo, de videos, de música, etcétera el cual causa perdidas millonarias para cada una de estas industrias.

Delitos de calumnias e injurias, usurpación de identidad y revelación de secretos (este ultimo contemplado en nuestro Código Penal Federal en los artículos 211-Bis al 211-Bis7).

Delitos de tráfico de órganos y de estupefacientes, este delito en especial también ha ido en aumento ya que ahora las transacciones se hacen a través de *Internet*, pudiendo después borrar toda evidencia del contacto de la transacción.

La autoridad debe tener presente que la información es un bien jurídico que debe especialmente ser protegido por el Estado puesto que de ella y de su administración, depende el giro normal de las relaciones comerciales y civiles de la sociedad.

Respecto al comercio electrónico o *e-commercere*, este trae diferentes tipos de problemas referidos a la propiedad intelectual, la protección al consumidor, el

documento electrónico y la firma digital, la regulación en las autopistas informáticas, la seguridad y la privacidad en la información, los que van a requerir estructuras legales mas amplias.

Como hemos mencionado la informática esta en casi todos los campos de la vida moderna y con mayor o menor rapidez todas las ramas del saber humano se acoplan ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se realizaban manualmente

El progreso más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza y al alcance de millones de interesados y usuarios. Pudiendo sostener que hoy en día las perspectivas de la informática no tiene límites previsibles, dándonos cuenta de que este es el panorama de este nuevo fenómeno tecnológico en las sociedades modernas.

Por ello ha llegado a sostenerse que hoy en día la informática es una forma de poder social. Las facultades que el fenómeno pone a disposición de instituciones y de particulares, con rapidez y ahorro en tiempo y energía, configuran un cuadro de posibilidades de actos lícitos o ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación nueva en el medio social.

Esta marcha de las aplicaciones de la informática no solo cuenta con ventajas 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, Australia y Japón, representan una amenaza para la economía de los países, para la sociedad en su conjunto y en especial al sujeto en su persona y en su patrimonio.

El espectacular desarrollo de la informática ha abierto puertas a nuevas posibilidades de delincuencia antes inimaginables. 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 morales y materiales. Pero no solo la cuantía de los perjuicios así ocasionados es a menudo superior a la que es usual en la delincuencia tradicional, sino que también son mucho mas elevadas las posibilidades de que no lleguen a descubrirse, ya que se trata de una delincuencia de personas capaces de borrar toda clase de huellas de los hechos.

En este sentido la informática puede ser el objeto del ataque o el medio para cometer 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. La idoneidad proviene básicamente, de la gran cantidad de datos que se acumulan, con la siguiente facilidad de acceso a ellos y la fácil manipulación de datos.

Si se tiene encuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre millones de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades bancarias, financieras, tributarias y de identificación de las personas. Y si a ello se le agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a una institución o a particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que nuestro ordenamiento jurídico penal debe proteger.

No es la amenaza potencial del avance de las computadoras sobre el individuo lo que nos preocupa, sino la utilización que hace el hombre de los sistemas de información con fines delictivos, puesto que no son los grandes sistemas de información los que afectan la vida privada de las personas, sino la manipulación

o el consentimiento de ello, por parte de individuos astutos y concientes de poder obtener un beneficio económico al manejar los datos que contienen dichos sistemas.

Con el tiempo se ha podido demostrar que los autores de estos delitos son muy diversos y lo que los diferencia entre si es la naturaleza de los delitos cometidos. De esta forma, la persona que ingresa a un sistema informático sin intenciones delictivas es muy diferente al empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Como se puede observar el delito informático debe adecuarse a nuestro ordenamiento penal para el Estado de México para prevenir que estas conductas sigan en aumento ya que perjudican económicamente a una de las poblaciones más conurbadas dada la cercanía que tenemos con el Distrito Federal y entidades que nos rodean.

II. Crítica al Delito Informático

Uno de los principales limitantes que tiene la problemática acerca del delito informático es la débil infraestructura legal que tiene nuestro país con respecto a la identificación y ataque de este tipo de delitos, no obstante que poseen los criterios suficientes sobre la base de la experiencia de otras naciones para el adecuado análisis e interpretación de este tipo de actos delictivos.

El presente trabajo tiene como finalidad el mostrar cuales son las características que debe tener en cuenta el legislador para incorporar el delito informático dentro del Código Penal para el Estado de México, por ello es importante vincular tal delito con las instituciones jurídico-penales existentes en nuestro Código Penal Federal.

La red mundial *Internet*, esta favoreciendo la comisión de infracciones de diferente índole en materia informática, el submundo que se crea por dicha red hacen que las conductas contra derecho sean difíciles de perseguir, no solo por la

complejidad del entorno donde se produce sino por la ausencia de tipificación de las modalidades y de los medios utilizados para cometer tales conductas.

Siempre la electrónica, la informática y la telemática han participado activamente en la economía activamente, en una economía globalizada como la de hoy, la producción en dichos sectores junto con el reconocimiento del valor de la información hacen sin duda que los recursos resultantes de sus actividades, asuman una importante estrategia competitiva tanto para el Estado como para la comunidad, y que estas deban de protegerse.

Cabe hacer mención de las distintas etapas por las que a atravesado la denominación de nuestro cuerpo punitivo. “La norma jurídica abarca tanto la conducta humana como la consecuencia jurídica, aquella adquiere relevancia en merito de la amenaza de coerción estatal determinada por el precepto legal como resultado de maleficio; sin aquella, este no puede prevalecer, y una pena sin conducta referible pierde toda significación, en ocasiones, al legislador se le olvida prever los caracteres de la conducta, o por inadecuada técnica incurre en el error de no configurarla, para que pueda estimarse como típica… y entonces aun, unida a la imprecisa enunciación que quiso crear el tipo, la pena no podrá aplicarse porque faltaron los requisitos de la tipicidad que el derecho liberal exige”[1]

De lo anterior se desprende del mismo modo, que ciertas formas típicas carecen de una pena congruente con el delito que se comete, y solo para los efectos del análisis doctrinario se puede hablar de delito sin pena y de pena sin delito; pero en la realidad jurídica y de la concepción unitaria de la norma de derecho positivo, seria un disparate hablar de delincuente sin delito, y de delito al que no le sobreviene pena y de pena sin un tipo.

Es decir lo que se pretende decir con este pequeño análisis es que el estudio analítico lo exige la doctrina para la correcta interpretación de la ley, para los fines dogmáticos, y lo que se trata de lograr es destacar que sin la existencia de la

[1] PALACIOS VARGAS, J. Ramón. *Delitos Contra la Vida y la Integridad Corporal*, 2ª. ed., Trillas, México, 1985, p. 11.

tipicidad, resulta inútil cualquier esfuerzo de legislar, ya que todo se convertiría en un estudio de fines restringidos ya a la dogmática, sin repercusiones en el derecho, ya que no podemos crear sin estructuras o bases un nuevo tipo de delito si no tenemos los fundamentos necesarios para poder crear las raíces necesarias para que pueda realmente funcionar la pena que se le aplique, y no se convierta en un esfuerzo mas del legislador para solo crear leyes sin fundamento y sin repercusión legal, y que solo se busque como finalidad la evasión de esa misma ley. Por eso se considera que para que se pueda tipificar el delito informático debe basarse en fundamentos lógicos, teóricos y prácticos, en como solucionarlo, y no solo ir con la mentalidad de cómo sancionarlo sin poner remedio a ese mal, teniendo en cuenta que si el Código Penal para el Estado de México podría contemplar este delito dentro de los delitos de orden patrimonial se imponga pena de prisión bastante amplia ya que no nos interesa que el delincuente pase mucho tiempo dentro de los centros de readaptación social si no lo que se busca es que el delincuente haga la reparación del daño que causo ya que afecto los bienes ya sea de un sujeto o más.

A lo largo de la historia de nuestra legislación mexicana y de la legislación internacional se han encontrado diversas disposiciones con el propósito de regular la conducta del hombre, para así poder convivir en armonía y en beneficio de la sociedad, es a través del tiempo de las costumbres y de la tecnología, como las necesidades del mismo van creciendo, de modo que es imperativo e importante crear legislaciones y procedimientos que regulan las distintas actividades del ser humano de manera que el proceso con el que el hombre se va desarrollando sea conforme a derecho y con las regulaciones que esta ofrece.

El derecho penal coloca en primer lugar la organización del Estado, y los peores delitos son aquellos que atentan contra este orden, y los delitos sociales serían aquellos que no afectaran al individuo, sino a la colectividad, al grupo, en sus derechos o intereses, podemos ver que el tema de nuestro trabajo es el delito informático y si lo localizamos en el ámbito de la libertad, y en el ámbito de la propiedad y la posesión, tomando en cuenta que en esta ultima localizaríamos el patrimonio de los sujetos, entonces si estudiamos detenidamente que si no hay libertad en este sentido la entenderíamos como el libre acceso a programas de

computo, información, la propiedad y posesión las entendemos como el patrimonio de cada uno de los sujetos que navegan en *Internet* y requieren de servicios o bienes, con esto podemos ver que este no es el problema esencial, el problema fundamental es que se tenga acceso a todo tipo de información, pero sin lucrar con ella y que en momentos que entramos a bases de datos para obtener un beneficio estamos en presencia de un delito informático.

Es cierto que la razón de muchos delitos tipificados que existen han sido producto de la necesidad de que sean penalizados, pero esa misma necesidad nos lleva a que sin fundamentos lógicos y congruentes se legisle solo por legislar, y que a la larga esa finalidad sea contraproducente, por que esa penalización va generando deficiencia y peor aun nuevos delitos, que tienen que ser penalizados, y no solo esto si no que también en ello influye mucho el avance tecnológico como es el caso de nuestra investigación, ya que nuevos adelantos científicos y tecnológicos acarrean nuevas acciones que deben ser calificadas como conductas típicas, pero el problema no es una ni otra sino la finalidad que se le da a cada una. Y si tomamos la idea de que se legisla por necesidad, debemos partir también de que esa necesidad debe estar bien fundamentada, valorando los argumentos a favor y en contra que conlleve dicha toma de decisión para legislar cierta conducta típica.

La importancia para que se pueda concretar una iniciativa de ley que regule el delito informático se ve reflejada en otras legislaciones como el Código Penal para el Estado de Sinaloa. La propuesta que se hace de la tipificación de este tema como delito, ya que busca mas que nada la protección a los usuarios y mas que buscar un castigo privativo de libertad para los que cometen dicho delito, la propuesta seria resarcir el daño, pero para que pueda resarcirse este, deben implementarse métodos, mecanismos, técnicas, para que una vez sean descubiertos estos tipo de sujetos paguen un monto económico a el sujeto victima del detrimento en su patrimonio, además de que en determinados casos se de la privación de la libertad, y esta ultima tomarla solo en los casos donde se amerite debido al monto que se afecto, y tomando en cuanta la seguridad de que el individuo no llegare a querer evadirse de la pena impuesta.

El crimen informático aumenta con delitos que van desde robos de computadoras portátiles hasta millonarios fraudes a través de *Internet*, y debido al potencial de aprovechamiento de la red para la información, la educación, el entretenimiento y la actividad económica a escala mundial es muy importante; por ello es necesario garantizar un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público. Los suministradores de acceso a *Internet* y los suministradores de servicios de ordenador central desempeñan un papel decisivo para dar acceso a los usuarios, a los contenidos de *Internet,* sin embargo no debemos olvidar que la responsabilidad primordial de los contenidos recae sobre los autores y los suministradores de contenidos, por ello es imprescindible señalar con exactitud la cadena de responsabilidades con el fin de situar la responsabilidad de los contenidos ilícitos en sus creadores.

Debido a que se han formado vertientes que proporcionan argumentos en contra de la regulación informática estas son en tres tipos de casos:

a) El derecho a la Intimidad,
b) la libertad de expresión y,
c) la libertad de acceso a la información.

Para entender el punto anterior se puede decir que podemos tener un derecho a la intimidad, una libertad de expresión, y una libertad de acceso a la información sin que con ello caiga en un abuso, que nos perjudique, tanto en nuestros derechos de autor como en nuestro patrimonio, la cuestión es que podemos tener acceso a todo ello con la debida responsabilidad de nuestra parte, ya que toda persona que maneja una computadora, sabe delimitar, por lo menos de manera esencial el fin que le esta dando a esa información, previendo que las personas que requieran un bien o servicio vía *Internet* tengan la seguridad de que las empresas que se supone están ofreciendo un bien o servicio sean legales y que realmente existan y que no sean solo creadas para que se aprovechen de los usuarios en lo que están requiriendo, y estafen a los sujetos, con productos o servicios que nunca recibirán, y lo peor aun que proporcionen sus cuentas, teniendo la seguridad de recibir ese bien o servicio y que después ya no tengan nada en sus cuentas de tarjetas de crédito o bancarias.

La problemática que se ha venido suscitando a través del análisis del delito informático dentro de los sistemas computacionales, ha generado como se ha comentado, un desastre internacional que en ocasiones ha traído consigo consecuencias catastróficas implicando la seguridad internacional, y a pesar de que haya ordenamientos que contengan dichos delitos tienen severas lagunas con relación a la materia informática, ya que como hemos venido mencionando se protegen aspectos de suma importancia como lo es la intimidad, seguridad patrimonial, dignidad e inclusive daños morales.

III. La conveniencia de la regulación del Delito Informático.

Es notable la necesidad que existe en que el delito informático sea integrado dentro de nuestro ordenamiento penal para el Estado de México puesto que la autoridad en la actualidad esta encaminando a algunos organismos especiales para la localización de delincuentes cibernéticos, para lo cual es necesario que se tenga un sustento jurídico acorde para el momento de capturar a estos sujetos y se le aplique una sanción (de tipo pecuniaria mas que privativa de la libertad), provocando la reducción en los altos índices delictivos respecto del delito informático.

Por lo tanto es importante destacar que el legislador debe de estar informado de que la tecnología creada para facilitar tareas y costos hoy es utilizada para delinquir y obtener beneficios económicos dañando así el patrimonio y también la privacidad de las personas, de esta forma debe de existir una norma penal que cuide y proteja tanto el patrimonio como la privacia del particular, tomando en cuenta todos y cada uno de los elementos del delito, así como de los presupuestos del mismo.

Para entender un poco mas de la propuesta del presente tema, es necesario establecer cuales son las bases para incluir el delito informático dentro del Código penal para el Estado de México, dando así una posible solución a este problema.

Como se expuso anteriormente el único ordenamiento que se refiere exactamente a lo que se debe entender por delito informático es el Código Penal

para el Estado de Sinaloa dentro de su apartado de delitos contra el patrimonio, siendo este el bien jurídicamente tutelado, sin embargo considero que se ubica bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, es destacable que los delitos informáticos van mas allá de de una violación a los derechos patrimoniales de las personas, ya que debido a las diferentes formas de comisión de los delitos, no solamente se lesionan estos derechos, sino otros como el derecho a la intimidad o a la privacidad respecto de las informaciones privadas.

Los elementos que se deben de tomar en cuenta para la correcta inclusión del delito informático dentro del Código Penal para el estado de México debe de requerir un apoyo que nos especifique acerca de que tipos de conductas deben de constituir los delitos informáticos.

Por ello continuación propongo que se cree un artículo dentro del apartado de delios contra el patrimonio tomando en cuenta cada uno de los elementos que debe de contener el delito informático.

Primeramente debemos saber lo que se entiende por delito informático refiriéndonos a la conducta ilícita desplegada por un sujeto con el interés de causar un daño u obtener un beneficio económico, en donde esta persona debe ser castigado debido ya que en el apartado del sujeto activo, anteriormente expuesto, mencionamos que no se trata de cualquier persona que tenga una computadora y este conectado a una red sino que requiere de conocimientos de informática, computación, sistemas, etcétera, para poder lograr su finalidad ilícita, y que conozca mucho mas las técnicas cibernéticas dañando o perjudicando tanto moralmente como económicamente a otra persona.

Al mismo tiempo por ende debemos saber que este tipo de conductas son de acción ya que el delincuente necesita dar ordenes a la computadora para que pueda realizar una operación ya sea borrar, transferir o modificar la información para que produzca el resultado que espera el sujeto, es decir ya que la utilización de las computadoras fueron creadas solo y con la finalidad de servir al individuo, disminuyendo el trabajo, aminorar errores, hacer mas veloz el tiempo de

transferencia de la información, realizar transacciones en el menor tiempo, facilitar información de manera gratuita, etcétera, para que el individuo tuviera a su alcance información de cualquier parte del mundo, de cualquier tema, sin que saliera de una habitación para ello, pero la naturaleza del ser humano es el modo de sobrevivir y no esta mal, lo malo y lo ilícito es que se utilice este medio para sobrevivir de manera que ciertos individuos se basen en el trabajo arduo de otras personas para obtener un lucro o un beneficio, simplemente con acceder a la red, no olvidando que para que el sujeto actué en contra de otro debe de estar conciente de la intención dolosa con la que actúa.

Otro aspecto importante que el legislador debe tomar en cuenta es que la conducta ilícita que realiza el sujeto se adecue respecto del tipo o la norma penal ya que el sujeto al actuar ilícitamente con la intención de ocasionar un daño u obtener un beneficio al utilizar un sistema informático, este aspecto debe de estar descrito cuidadosamente dentro del ordenamiento penal ya que si este no toma en cuenta que el sujeto activo daño, modifico, o destruyo la información causando un daño y si no hay una adecuación al tipo penal se puede decir que no existe el delito.

Es igualmente importante resaltar que el hecho o la conducta que despliega el sujeto al contravenir una estipulación legal penal esta cometiendo un delito, es decir infringe una prohibición de la cual debe estar enterado ya que como se ha mencionado anteriormente el sujeto activo de este delito esta preparado académicamente o técnicamente para utilizar un sistema informático.

Es así que para que se pueda llagar a un tipo penal es importante tener en cuenta la relación del daño hecho y la intención del sujeto activo de producirlo, es decir, entender el por que el actuar del sujeto para producir un daño a otra persona o cuales fueron las causas que lo motivaron a actuar en forma dolosa y como anteriormente se ha mencionado estos sujetos están preparados académicamente para utilizar estos sistemas al mismo tiempo que tienen la iniciativa o el reto de vencer obstáculos tecnológicos, es así como la relación del sujeto con el delito existe ya que para que exista la culpabilidad se requiere la

exigibilidad de la posibilidad de comprender la conducta antijurídica, es decir la desobediencia consiente y voluntaria de infringir la ley.

Como se ha explicado cuando el sujeto realiza una conducta con la intención de dañar, modificar o destruir la información contenida dentro de una computadora con la finalidad de obtener un beneficio económico, es necesario que el delito informático tenga en consideración el monto del daño causado, es por eso dada estas causas que no se busca una pena[2] privativa de la libertad ya que al sujeto pasivo no le interesa que el delincuente informático pase demasiado tiempo dentro de los centros de readaptación social, ya que como sabemos no cumplen con su cometido de readaptar a los sujetos si no al contrario estos al salir no solamente volverán a cometer los mismos delitos si no que adentro de estos centros aprenden a cometer todo tipo de delitos de toda índole, mas sin embargo a la persona que sufrió un detrimento en su patrimonio lo que se propone es que el delincuente haga la reparación del daño[3], con esto se propone que la idea de la reparación del daño el delincuente pague los daños que ocasionó con el fin de que las personas afectadas puedan recuperar una parte del monto económicamente que sufrieron en su patrimonio.

En consideración a lo anteriormente expuesto nos referiremos un poco más a la reparación de daño para poder comprender el daño o perjuicio que una persona sufre en lo material o en lo patrimonial, lo que se expresa con el empleo de los términos “material o patrimonialmente”, es la exclusión de la persona, ya que cuando se causa un daño a una persona, en ningún caso es posible la recomposición o la vuelta a un status anterior con esto hago referencia a la vida humana, razón por la cual se habla de un desagravio o satisfacción. Por lo tanto es imprescindible, que el bien dañado sea de características tales que pueda, por su esencia y función componerse, por lo cual es necesario determinar si, después

---

2 “Pena es el castigo que el Estado impone, con fundamento en la ley, al sujeto responsable de un delito.” AMUCHATEGUI REQUENA, Irma G. *Derecho Penal*, Harla, México, 1993, p 108.

3 “Cuestión debatida es si la reparación de los daños ocasionados por el delito debe comprender también los daños morales. Cuando la afección moral se traduce en decrecimiento del patrimonio económico, es relativamente fácil la valuación de aquél; pero no así cuando esa relación sea imposible de establecer, pues entonces mas que reparación lo que existiera será nueva pena. Pero las legislaciones modernas van siendo constantes en la admisión, también, la reparación del daño moral.” CARRACA Y TRUJILLO, Raúl y CARRACA Y RIVAS, Raúl. *Derecho Penal Mexicano Parte General*, 19ª. ed., Porrúa, México, 1997, p. 829.

de lesionado el bien, existe interés en el ofendido por ese tipo de reparación, ello hace posible que exista una composición de la misma cosa.

Es conveniente la creación de un tipo penal referente que impulse y no restrinja con demasiadas provisiones o sanciones el desarrollo de la informática, pues este elemento constituye un estratégico y vital instrumento para fomentar el progreso de los países, así como propiciar las condiciones idóneas para lograr el avance del derecho.

Recordando y haciendo énfasis que es de suma importancia resaltar que aparte de conceptualizar el delito informático dentro del Código Penal para el Estado de México y se introduzca a su vez dentro del apartado de delitos contra el patrimonio ya que para el autor Roberto Reinoso Dávila el delito informático afecta el patrimonio de las personas tanto físicas como jurídicas haciendo mención de que: "El mundo contemporáneo enfrenta actos engañosos por el uso de computadoras: un sector de los llamados "delitos informáticos". Por ejemplo: un estafador, mediante una computadora, puede lograr alterar los registros bancarios, y, en esa forma, hacer creer a los empleados del banco que el saldo de su cuenta es superior al real".[4]

IV. Beneficios de regular el Delito Informático

El lenguaje y la norma son herramientas fundamentales en la vida del hombre, que la ley y la comunicación inciden en la vida social, lo que reclama cada vez más una puntual, amplia y diversificada información. El avance de la tecnología y de la informática en la sociedad, requiere considerar no solo aspectos que permitan acceder a respuestas puntuales y adecuadas.

Un beneficio que tiene la evolución de la tecnología y de la informática, han propiciado que su uso adquiera un carácter estratégico, para elevar los niveles de bienestar de los individuos y para mejorar la competitividad y la productividad de la sociedad.

[4] REYNOSO DÁVILA, Roberto. *Delitos Patrimoniales*, 1ª. ed., Porrúa, México, 1999, p. 328, 329.

Un beneficio que la tecnología ha permitido es el acceso mas ágil a la información lo que permite la realización de actividades de una manera más eficiente pero esta información debe estar regulada para que no pueda ser utilizada con fines de lucro o sea adulterada para afectar el patrimonio de una persona.

La protección jurídica de la innovación y la inventiva han sido preocupación constante de las personas, empresas y países, y que el análisis del problema presenta líneas que dificultan el consenso en la creación de los mecanismos de solución.

Otro beneficio que nos brinda el derecho para la intimidad o privacidad es un derecho fundamental que asiste a los sujetos del derecho consistente en la facultad de mantener reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que pueda ser develado por existir un derecho superior de terceros o para el bienestar común. Por lo que se debe de asistir a la garantía de legalidad en cuanto a lo que respecta a reparar las posibles molestias a la persona o propiedades y posesiones, conforme a las normas constitucionales que regulan los derechos fundamentales.

Lo mencionado anteriormente nos muestra la realidad refiriéndonos en que nos estamos quedando atrás de los avances tecnológicos e informáticos y con ello los delincuentes buscan nuevas formas de delinquir y por no tener legislación aplicable a cada caso en concreto, dejamos que los delitos queden impunes.

Las acciones para erradicar estos problemas deben de comenzar por tener a la mano legislaciones bien cimentadas en las causas y resultados que producen dichas conductas delictivas.

Los beneficios que se pueden alcanzar con estas nuevas regulaciones y controles jurídicos son diversos, ya que con figuras penales adecuadas a la conducta desplegada por el sujeto activo y el daño que producen se puede garantizar una mayor seguridad para toda persona que utiliza la informática para diversas funciones.

Otro beneficio palpable seria tener mayor seguridad firmeza para avanzar en investigaciones tecnológicas, logrando con ello colocarnos al margen de los países líderes en tecnología y generando con ello un bienestar general sin olvidar lo seguro que seria realizar tales operaciones.

Sin olvidar que otro beneficio, seria el provocar que los individuos que tienen estos conocimientos y que podrían en un dado caso cometer un delito, detenerse y concienciar un poco mas en su actuar ya que no únicamente se le sancionaría por determinado tiempo y cantidad en multa, sino que igualmente al momento de establecer la perdida de posibilidades de seguir ejerciendo su profesión y técnica informática, estaría siendo castigado por haber realizado un mal uso de sus conocimientos.

CONCLUSIONES

A lo largo de la historia del hombre se han creado tecnologías cada vez mas modernas que ponen en alerta al individuo para seguir adelante sin parar y lograr así la perfección, percatándonos entonces que el avance desmesurado con el que se desarrolla la informática en el mundo globalizado de hoy, a traído consigo enormes beneficios a la humanidad que facilitan en gran medida las tareas y actividades del ser humano trayendo consigo desafortunadamente, conductas ilícitas que en determinadas ocasiones ponen en peligro la intimidad, el patrimonio e inclusive la propia vida de la persona.

Quedando así establecido que dicho avance tecnológico debe y tiene que regularse en cada entidad de nuestro país tomando en cuanta también todos los tratados internacionales, acuerdos y convenios realizados entre estos, para así poder obtener una cooperación y un resultado eficaz por parte de dichos países o entidades de nuestro país una vez instituidas sus legislaciones, y así poder combatir determinadamente las conductas ilícitas realizadas por los delitos informáticos.

En la actualidad en nuestro sistema legal, no existe un concepto de delito informático (a excepción del Código Penal para el Estado de Sinaloa, en su artículo 127) por lo que es importante que se realice no solo para conocer las limitantes de este, si no también para lograr que se tipifique este delito como tal en nuestro Código Penal para el Estado de México y así poder sancionarlo y regularlo.

Es importante e indispensable conocer los tipos de delitos informáticos reconocidos por la ONU (Fraudes cometidos mediante manipulación de computadoras. Entre este tipo se encuentran la Manipulación de los datos de entrada, la manipulación de datos de salida; Falsificaciones informáticas como objeto y como instrumento; Acceso no autorizado a servicios y sistemas informáticos; Piratas informáticos o *Hackers*; La reproducción no autorizada de programas informáticos de protección legal y Daños o modificaciones de programas o datos computarizados como es el sabotaje informático a través de

los virus, gusanos y la bomba lógica) antes que nada para poder tener en claro las consecuencias que se producen con la realización de estas conductas ilícitas y sobre todo por que con esta referencia se podrá prevenir firmemente dichas consecuencias.

Se ha dejado en claro que la ligereza con las que se realizaron las reformas al Código Penal Federal en materia de derechos de autor así como de acceso ilícito a sistemas y equipos de informática, dejaron dudas por resolver como por ejemplo: ¿en que parte del Código Penal Federal se encuentra tipificado el Delito Informático como tal? o ¿ante que autoridad con conocimientos en informática deberá presentarse la victima de estas conductas ilícitas? o ¿Qué procedimiento se deberá seguir para sancionar este tipo de delitos, o es acaso que se tendrá que seguir el procedimiento penal con la ausencia implícita de un representante experto en la materia de informática?.

Si bien se entiende que la Ley Federal de Derechos de Autor hace una remisión al Código Penal Federal, para que tenga conocimiento de las conductas especificadas en la Ley Federal del Derecho de Autor y además no solo las tenga contempladas sino que señale aparte las multas. Es también muy cierto que aunque se presenten estas multas, las cuales son casi simbólicas ya que el beneficio pecuniario que se obtiene de dichos conductas es a veces desorbitante, no se encuentra tipificado el delito como tal y solo se multan ciertas conductas dejando a la deriva impunemente muchas otras conductas ilícitas que requieren necesariamente pagar un castigo por los daños causados, que en muchas de las ocasiones no se pueden restituir.

Con todo lo anterior se propone que se establezca un tipo penal denominado delito informático, protegiendo los bienes jurídicos a tutelar como lo son la intimidad personal, la seguridad patrimonial y la dignidad, señalando el procedimiento especial a seguir dada la naturaleza del mismo. Además de que este delito deba encontrarse en el Código Penal para el Estado de México dentro del apartado de Delitos contra el Patrimonio.

GLOSARIO

Chip: es una pastilla o *chip* muy delgado en el que se encuentran miles o millones de dispositivos electrónicos interconectados, principalmente diodos y transistores, y también componentes pasivos como resistencia o capacitores. Su área puede ser de un cm2 o incluso inferior. Algunos de los circuitos integrados más avanzados son los microprocesadores que controlan múltiples artefactos: desde computadoras hasta electrodomésticos, pasando por los teléfonos móviles.

Cibernética: Es la ciencia que se ocupa de los sistemas de control de comunicación entre las personas y en la maquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes.

Ciberespacio: Palabra acuñada por William Gibson en su popular novela de ficción científica Neuroromancer, para describir la esfera dinámica cultural de la gente y las maquinas trabajando dentro de los confines de las redes computacionales.

Comercio electrónico o *e-commercee*: El comercio electrónico (en inglés *Electronic Commerce, E-Commerce, ecommerce* o *EC*) consiste principalmente en la distribución, compra, venta, mercadotecnia y suministro de información complementaria para productos o servicios a través de redes informáticas como *Internet* u otras. La industria de la tecnología de la información podría verlo como una aplicación informática dirigida a realizar transacciones comerciales. Una definición alternativa lo vería como la conducción de comunicaciones de negocios comerciales y su dirección a través de métodos electrónicos como intercambio electrónico de datos y sistemas automáticos de recolección de datos. El comercio electrónico también incluye la transferencia de información entre empresas.

Computadora: Es una maquina capaz de efectuar una secuencia de operaciones mediante un programa que realiza un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida.

Coreo electrónico o *e-mail:* El Correo electrónico, o en inglés *e-mail*, es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos (normalmente por *Internet*). Esto lo hace muy útil comparado con el correo ordinario, pues es más barato y rápido. Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos.

Dato (s): Un dato es una representación simbólica (numérica, alfabética, etcétera), de un atributo o característica de una entidad. El dato no tiene valor semántico (sentido) en sí mismo, pero convenientemente tratado (procesado) se puede utilizar en la realización de cálculos o toma de decisiones. Es de empleo común en el ámbito informático.

Derechos de Autor o *Copyright*: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Fax: El facsímil (o simplemente *fax*), como el servicio de telex, requiere de equipo especializado para enviar y recibir mensajes, pero no requiere que los usuarios se suscriben al servicio de transmisión proporcionado por algún mensajero particular o proveedor de equipo.

Hacker: El *Hacker* (del inglés *hack*, hachar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, *hardware* de red/voz, etc. Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo *hardware* o *software*. Se suele llamar *hackeo* y *hackear* a las obras propias de un *hacker*. El término "*Hacker"* trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un *hacker* es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Impresora: Una impresora es un dispositivo de salida de una computadora cuya función es transcribir un documento (imagen o texto)

Información: La información es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno.

Informática: La informática es una rama de la ingeniería que estudia el tratamiento de la información mediante el uso de maquinas automáticas. Entre las tareas mas populares que ha facilitado esta tecnología se encuentran: elaborar documentos, enviar y recibir correo electrónico, dibujar, crear efectos visuales y sonoros, manejar la información contable en una empresa, reproducir música, controlar procesos industriales y jugar.

Internet: Es una red mundial de computadoras interconectadas entre si, que permite accesar a cualquier tipo de información y transmitirla.

Jurimetría: La jurimetría es la disciplina que tiene como propósito o razón la posibilidad de la sustitución del Juez por la computadora, finalidad que por los momentos es inaceptada, simplemente porque a través de la jurisdicción se emana una sentencia, y para ello, que mejor candidato que un ser humano que por supuesto tiene el sentido racional, con lo pueda acudir al sistema de integración y poder a través de las interpretaciones y lógica jurídica dar una sentencia llena de la interrelación de la paz y la justicia, para lograr verdaderas sociedades, verdaderas democracias y libertades.

Lenguaje de programación: es un conjunto de palabras y de reglas de sintaxis para facilitar la comunicación con la compradora.

Memoria: tiene como función almacenar datos antes de ser procesados, durante su proceso y después de que este haya terminado mientras la información es dirigida a las unidades de salida.

Multimedia: Es el uso de diversos medios (texto, audio, gráficos, animación, video e interactividad) de transporte de la información.

Password o contraseña: Se denomina así al método de seguridad que se utiliza para identificar a un usuario. Es frecuente su uso en redes. Se utiliza para dar acceso a personas con determinados permisos.

Plotter: Un *plotter* o trazador gráfico es un dispositivo de impresión conectado a una computadora, y diseñado específicamente para trazar gráficos vectoriales ó dibujos lineales: planos, dibujos de piezas, etc. Efectúa con gran precisión impresiones gráficas que una impresora no podría obtener. Los primeros usaban plumillas de diferentes trazos ó colores. Actualmente son frecuentes los de inyección, que tienen mayor facilidad para realizar dibujos no lineales y en múltiples colores, son silenciosos y más rápidos y precisos.

Programa de Computo: Un programa es simplemente una secuencia de instrucciones que orienta a la CPU en el desarrollo de los cálculos. Por ultimo, este programa debe expresarse de forma que pueda ser entendido por la CPU.

Ratón o *mause:* Pequeño aparato manual conectado a un ordenador o a una terminal, cuya función es mover el cursor por la pantalla para dar órdenes.

Red: Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de computadoras y/o dispositivos conectados por enlaces de un medio físico o inalámbricos y que comparten información, recursos y servicios.

Scanner: (del idioma inglés: *scanner*) es un periférico que se utiliza para convertir, mediante el uso de la luz, imágenes impresas a formato digital.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Virus: Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "*malware*" dentro de los virus, en el sentido estricto de esta ciencia un virus son programas que se replican y ejecutan por sí mismos. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden intencionadamente destruir datos en la computadora, aunque también existen otros más benignos, que solo se caracterizan por ser molestos. Los virus informáticos tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Web: La *World Wide Web*, la *Web* o *WWW,* es un sistema de navegador *web* para extraer elementos de información llamados "documentos" o "páginas *web*". Puede referirse a "una *web*" como una página, sitio o conjunto de sitios que proveen información por los medios descritos, o a "*la Web*", que es la enorme e interconectada red disponible prácticamente en todos los sitios de *Internet.*

ANEXO 1

DELITOS INFORMATICOS RECONOCIDOS POR LA ONU, 11/28/2002

TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS

FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS

Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

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

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

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

Manipulación Informática aprovechando 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 ven sacando repetidamente de una cuanta y se transfieren a otra.

FALSIFICACIONES INFORMATICAS

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo u8n experto puede diferenciarlos de los documentos auténticos.

DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS.

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

Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede

ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos: Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

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

Acceso no autorizado a servicios y sistemas informáticos: Es el acceso no autorizado a sistemas informáticos 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 uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o

puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal: Esta 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.

ANEXO 2

CÓDIGO PENAL FEDERAL (Reformas del 17 de Mayo de 1999)[1]

TITULO NOVENO: Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

CAPITULO I: Revelación de secretos

Artículo 210.- 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.

Artículo 211.- 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.

Artículo 211 Bis.- 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.

Capitulo II: Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

[1] http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s=

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

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

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

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

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

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero,

protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

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

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

ANEXO 3

CÓDIGO DE COMERCIO (Reformas del 3 de Abril de 2003)[2]

TITULO SEGUNDO: De Comercio Electrónico

CAPITULO I: De los Mensajes de Datos

Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

[2] http://info4.juridicas.unam.mx/ijure/tcfed/2.htm?s=

Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría: Se entenderá la Secretaría de Economía.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Artículo 90.- Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

I. Por el propio Emisor;
II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o
III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

Artículo 90 bis.- Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía, resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el Destinatario o la Parte que Confía, haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o
II. A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

Artículo 91.- Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue:

I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que ingrese en dicho Sistema de Información;
II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el Mensaje de Datos, o
III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos ingrese a un Sistema de Información del Destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.

Artículo 91 bis.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del Emisor o del Intermediario.

Artículo 92.- En lo referente a acuse de recibo de Mensajes de Datos, se estará a lo siguiente:

I. Si al enviar o antes de enviar un Mensaje de Datos, el Emisor solicita o acuerda con el Destinatario que se acuse recibo del Mensaje de Datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:
a) Toda comunicación del Destinatario, automatizada o no, o
b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el Mensaje de Datos.
II. Cuando el Emisor haya indicado que los efectos del Mensaje de Datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el Mensaje de Datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el Emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del Mensaje de Datos;
III. Cuando el Emisor haya solicitado o acordado con el Destinatario que se acuse recibo del Mensaje de Datos, independientemente de la forma o método determinado para efectuarlo, salvo que:
a) El Emisor no haya indicado expresamente que los efectos del Mensaje de Datos estén condicionados a la recepción del acuse de recibo, y
b) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio.
El Emisor podrá dar aviso al Destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el Emisor reciba acuse de recibo del

Destinatario, se presumirá que éste ha recibido el Mensaje de Datos correspondiente;
IV. Cuando en el acuse de recibo se indique que el Mensaje de Datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

Artículo 93.- Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 93 bis.- Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y
II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 94.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y
II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

Artículo 95.- Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor, o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido.

Se presume que cada Mensaje de Datos recibido es un Mensaje de Datos diferente, salvo que el Destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo Mensaje de Datos era un duplicado.

CAPITULO II: De las Firmas

Artículo 96.- Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.
La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

Artículo 98.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99.- El Firmante deberá:

I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;
II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;
III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas.
El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo,
IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

CAPITULO III: De los Prestadores de Servicios de Certificación

Artículo 100.- Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:

I. Los notarios públicos y corredores públicos;
II. Las personas morales de carácter privado, y
III. Las instituciones públicas, conforme a las leyes que les son aplicables.

La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 101.- Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;
II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;
III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado, y
IV. Cualquier otra actividad no incompatible con las anteriores.

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;
II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;
III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;
IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por

delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;
V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;
VI. Establecer por escrito su conformidad para ser sujeto a auditoría por parte de la Secretaría, y
VII. Registrar su Certificado ante la Secretaría.

B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 103.- Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Artículo 104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;
II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;
III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;
IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por

medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;

V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;

VI. En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;

VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y

IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:

a) La identidad del Prestador de Servicios de Certificación;

b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;

c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;

d) El método utilizado para identificar al Firmante;

e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;

f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y

h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Artículo 105.- La Secretaría coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

Artículo 106.- Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Artículo 107.- Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

I. Verificar la fiabilidad de la Firma Electrónica, o
II. Cuando la Firma Electrónica esté sustentada por un Certificado:
a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y
b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Artículo 108.- Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;
II. El código de identificación único del Certificado;
III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;
IV. Nombre del titular del Certificado;
V. Periodo de vigencia del Certificado;
VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;
VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y
VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Artículo 109.- Un Certificado dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;
II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;
III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado;
IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe, y
V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 110.- El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 111.- Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Artículo 112.- Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos

competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 113.- En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación, que para tal efecto señale la Secretaría mediante reglas generales.

CAPITULO IV: Reconocimiento de Certificados y Firmas Electrónicas Extranjeros

Artículo 114.- Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y
II. El lugar en que se encuentre el establecimiento del Prestador de Servicios de Certificación o del Firmante.

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se

tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de Firmas Electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

BIBLIOGRAFÍA

ALLISON, G. Burguess. *The Lawyer´s Guide to the Internet*, ABA, USA, 1995.

AMUCHATEGUI REQUENA, Irma G. *Derecho Penal*, Harla, México, 1993.

ARECHIGA G, Rafael. *Introducción a la Informática*, 1ª. ed., Limusa, México, 1994.

BARRIOS GARRIDO, Gabriela, *et al., Internet y Derecho en México*, 1ª. ed., McGraw-Hill, México, 1998.

BEEKMAN, George. *Introducción a la Informática*, 6ª. ed. Pearson Prentice Hall, Madrid, 2005.

CARRACA Y TRUJILLO, Raúl y CARRACA Y RIVAS, Raúl. *Derecho Penal Mexicano Parte General,* 19ª. ed., Porrúa, México, 1997.

CASTELLANOS TENA, Fernando. *Lineamientos Elementales del Derecho Penal*, 4ª. ed., Porrúa, México, 1999.

COROMINAS, Joan. *Breve Diccionario Etimológico de la Lengua Castellana*, Gredos, España, 1983.

DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Informático*, 4ª. ed. ARANZADI, Madrid, 2002.

DE PINA VARA, Rafael. *Diccionario de Derecho*, 28ª ed., Porrúa, México, 2000.

FERREYRA CORTES, Gonzalo. *Virus en las computadoras*, Macrobit, México, 1990.

GRATTON, Pierre. *Protección Informática*, 1ª. ed., Trillas, México, 1998.

LOPEZ BETANCOURT, Eduardo. *Teoría del Delito*, 7ª. ed., Porrúa, México, 1999.

MORA, José Luís, ENZO MOLINO. *Introducción a la Informática*, 4ª. ed., Trillas, México, 1991.

PADRÉS JIMÉNES, Manuel Alexandro. *La Regulación Jurídica de la Libertad de Expresión en el Internet,* ITAM, México, 1998.

PALACIOS VARGAS, J. Ramón. *Delitos Contra la Vida y la Integridad Corporal*, 2ª. ed., Trillas, México, 1985.

PALAZZI, Pablo Andrés. *Delitos Informáticos*, 1ª. ed., AD-HOC SRL, Argentina, 2000.

PARELLADA, Carlos Alberto. *Daño en la Actividad Judicial e Informática desde la Responsabilidad Profesional*, ASTREDA, Argentina, 1990.

PAVÓN VASCONCELOS, Francisco. *Manual de Derecho Penal Mexicano Parte General*, 14ª. ed., Porrúa, México, 1999.
REAL ACADEMIA DE LA LENGUA, *Diccionario de la Lengua Española*, Espasa-Calpe, España, 2001.
REYNOSO DÁVILA, Roberto. *Delitos Patrimoniales*, 1ª. ed., Porrúa, México, 1999.
TÉLLEZ VALDÉZ, Julio. *Derecho Informático*, 3ª. ed., McGraw-Hill, México, 2004.
TREMBLAY, Jean Paul, BUNT, Richard B. *Introducción a la Ciencia de las Computadoras*, 1ª. ed., McGraw-Hill, México, 1986.

LEGISLACIÓN CONSULTADA

México, *Constitución Política de los Estados Unidos Mexicanos*, Diario Oficial de la Federación, 5 de Febrero de 1917.
México, *Código Penal Federal*, Diario Oficial de la Federación, 2 de Febrero de 1931.
México, *Código Penal para el Estado de México,* Publicado en la Gaceta del Gobierno del Estado de México, 20 de Marzo del 2000.
México, *Código Penal para el Estado de Sinaloa*, Publicado en el P.O. No. 131, 28 de Octubre de 1992.
México, *Código de Comercio*, Diario Oficial de la Federación, 17 de Octubre de 1889.
México, *Ley Federal del Derecho de autor*, Diario Oficial de la Federación, 24 de Diciembre de 1996.
México, *Ley de la propiedad Industrial*, Diario Oficial de la Federación, 27 de Junio de 1991.

SITIOS EN LA RED

Biblioteca de Consulta *Microsoft*® *Encarta*® 2004. © 1993-2003 *Microsoft Corporation.*

http://es.wikipedia.org/wiki/Chip

http://es.wikipedia.org/wiki/Comercio_electronico

http://es.wikipedia.org/wiki/E-mail

http://es.wikipedia.org/wiki/Esc%C3%A1ner_de_ordenador

http://es.wikipedia.org/wiki/Fax

http://es.wikipedia.org/wiki/Hacker

http://es.wikipedia.org/wiki/Plotter

http://es.wikipedia.org/wiki/Privacidad

http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

http://es.wikipedia.org/wiki/Web

http://info4.juridicas.unam.mx/ijure/tcfed/2.htm?s=

http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s=

http://www.mastermagazine.info/definicion/6239.php

http://www.monografias.com/trabajos/cibernetica/cibernetica.shml

http://www.monografias.com/trabajos22/iuscibernetica/iuscibernetica.shtml