UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

"LA VULNERACIÓN ILÍCITA CONTRA EL FUNCIONAMIENTO EN LOS SISTEMAS DE INFORMÁTICA A TRAVÉS DE INTERNET."

T E S I S

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN DERECHO
P R E S E N T A :
ADRIÁN GONZÁLEZ OCOTE

FES Aragón

ASESORA: DE TESIS:
LIC. MARISELA VILLEGAS PACHECO

MÉXICO, 2005

DEDICATORIAS

A MI HERMANO Y HERMANAS:

Juventino González Ocote

Margarita González Ocote

Teresa González Ocote

Elvira González Ocote

Laura González Ocote

Por haberme otorgado su cariño
y confianza insuperables.
Gracias.

A TODOS Y CADA UNO DE MIS SOBRINOS:

Como base de que en la vida se puede lograr los sueños. Y como testimonio de que se sigan superando.

A MI ASESORA DE TESIS.
LIC. MARISELA VILLEGAS PACHECO
Por su asesoramiento y apoyo fundamental para la elaboración de este trabajo, ya que sin ello seria difícil su realización

A TODOS Y CADA UNO DE MIS AMIGOS.
Lic. Adrián Benitez, Lic. Francisco Rubio, Lic. Miguel Ángel Hernández, Lic. Julio Godinez, Lic. Gabriela, Lic. Salvador, Lic. Jasiel Ocote, Lic. Carlos Arellano, Javier García, Pedro Tinoco, Saúl Ocote. Y aquellos que por falta de espacio no podré mencionar.
Por que me brindaron su amistad y compañerismo en los tiempos maravillosos como en los tiempos difíciles.

Y TODAS AQUELLAS PERSONAS QUE
ENFORMA DIRECTA E INDIRECTA COLABORARON
PARA LA REALIZACIÓN DE ESTE SENCILLO TRABAJO.

ÍNDICE

LA VULNERACIÓN ILÍCITA CONTRA EL FUNCIONAMIENTO EN LOS SISTEMAS DE INFORMÁTICA A TRAVÉS DE INTERNET

CAPÍTULO 4

MEDIOS DE PRUEBA QUE PERMITEN ACREDITAR LA VULNERACIÓN ILÍCITA EN LOS SISTEMAS DE INFORMÁTICA

INTRODUCCIÓN

INTRODUCCIÓN

Uno de los cambios más sorprendentes del mundo, hoy en día, es la rapidez de las comunicaciones ya que se permite el intercambio de información independientemente del lugar físico en que nos encontremos. Ya no nos sorprende la transferencia de información en tiempo real o instantáneo. Se dice que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma pública, se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones así como el Internet en el que funciona de manera mundial, han sido violadas por criminales informáticos desconocidos. A diario se reciben informaciones de ataques a redes informáticas: los archivos son alterados, los ordenadores se vuelven inoperativos, se ha copiado información confidencial sin autorización, etcétera.

Ciertamente en el surgimiento del Internet no exista ni requería una regulación pero en el momento que se dispuso su acceso al público en general, es necesario su regulación, hasta ahora existen leyes relativos a los delitos informáticos en un respectivo país, en forma estatal, pero es insuficiente en relación a ciertos delitos que influyen tratados internacionales, los cuales aún no funciona para la represión de estos delitos en razón de sus limitaciones.

Por lo anterior, es preciso la creación de leyes a su naturaleza del Internet, para esto, debe crearse tratados internacionales unificados, y tipos penales específicos para cada conducta en el mundo cibernético, garantizando los usos y costumbres de los estados participes, para su aplicación de dichas leyes es necesario un tribunal en el que se integre jueces que tengan conocimientos

especiales en delitos informáticos, como efecto también una eficaz ciberpolicías que tengan como función la vigilancia de los sitios web ilícitos o conductas denunciadas por los cibernautas.

Por lo que este trabajo en forma general, se enfocará a tratar de analizar ciertas conductas ilícitas que implica el buen funcionamiento de las redes telemáticas; por un lado se verá las conductas ya reguladas en nuestro Código Penal Federal que estable ciertas conductas con relación a los sistemas informáticos; y por otra parte se analizara nuevas conductas que en sí, es necesario regularlas, una de ellas es la Denegaron de Servicios (Denial Of Servicies o Distributed Deniel of Services (DOs)), que imposibilita o inhabilita un servido temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas. Lo anterior implica la urgencia de tratar ciertas conductas referente al crimen informático.

En primer lugar se hablara de la informática, sus orígenes y su relación con el Derecho, pero en sí, con el Derecho Penal, esto implica el Internet y su delincuencia cibernética, el perfil de los sujetos que lo conforman, y así entrar en materia con los sujetos que vulneran el buen funcionamiento de las redes telemáticas.

Por lo que se refiere al derecho Comparado, se mostrara ciertas legislaciones que regulan el crimen informático, y su penalidad.

Su propósito de este trabajo es analizar las conductas relevantes que inhabilitan las redes de tratamiento informático, por una parte su forma de acreditar el cuerpo del delito y su probable responsabilidad; y la segunda es su forma de comprobación, por lo qué es necesario llevar acabo ciertos peritajes electrónicos que lleven a la comprobación del crimen informático.

En síntesis, este pretendido trabajo de investigación, busca sin mas, estudiar conductas ilícitas en sistemas informáticos, su forma de vulneración y los medios de prueba para acreditarlo, que permitan dar una mejor justicia y seguridad a todo cibernauta.

1. CAPÍTULO 1.

1. CAPÍTULO 1.

GENERALIDADES

1. HISTORIA DE LA INFORMÁTICA

El mundo ha sufrido revoluciones tecnológicas que implica a la información, y que ha repercutido en tal forma que han transformado a la economía y a la sociedad. Por lo que las tecnologías de la información han sido un factor esencial que hace a la información un bien económicamente activa.

Atendiendo a la palabra Informática, éste tiene su origen a la fusión de los términos INFORmación y autoMÁTICA sugerido por Phillipe Dreyfus en el año de 1992; hace referencia al conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático y racional de la información por medio de ordenadores.

Téllez Valdes lo define como "...un conjunto de Técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones..."[1]

Durante el transcurso del tiempo el hombre inventó diversos mecanismos numéricos confiables y mucho más rápidos, y entre las primeras creaciones que le permitiera realizar operaciones de calculo tenemos:

El ábaco Babiliónico, se "...encuentra su raíz etimológica en la voz fenicia Abak que significa "...tabla lista cubierta de arena... estas tabletas de arcilla tienen una antigüedad de cuatro mil años y con ellas se llevaban registros de bancos y

[1] TÉLLEZ Valdés, Julio, "Derecho Informático". México, Edit. McGraw-Hill, 1998. P.5

empresas de prestamos que funcionaban en aquella época..."[2], y consistía en un tablero o cuadro con alambres o surcos paralelos entre sí, que se mueven bolas o cuentas, este ábaco era para realizar operaciones aritméticas.

Posteriormente en al año de 1614, Jhon Napier inventó un método para facilitar las operaciones de multiplicación y división, fue así como surgieron las tablas de logaritmos, en donde las multiplicaciones se traducen en sumas y las divisiones en restas, sin embargo la magnitud del esfuerzo que realizó Napier, las tablas tuvieron errores que fueron detectados tiempo después.

Fue hasta el año de 1642, cuando un joven de muy temprana edad, Blaise Pascal, desarrolla el primer sistema mecánico de cálculo, que consistía en un sistema de ruedas ordenadas, en cada una de las cuales estaban marcados los dígitos del cero al nueve, tres décadas después, sería perfeccionado por el igual célebre Gottfried Von Leibniz, al introducirle una rueda para simplificar su operación.

Podría decirse que en el año de 1834, el profesor de matemáticas, el ingles Charles Babbage, fue el principal contribuyente de las máquinas de cálculo, ya que concibió la idea de que cualquier tipo de información puede manipularse por procesos lógicos, siempre que previamente haya sido transformada en números.
Lo anterior fue una gran aportación, ya que fue determinante para lograr un diseño nuevo de lenguaje (lo que más tarde se llamó software), ya que cien años después sus bases sirvieron de pauta para la realización de la computadora electrónica moderna.

El Código de Herman Hollerith en 1880, fue el principio de la época de la tarjeta moderna, que consistió en emplear una cinta, que más tarde sustituyó por tarjetas en las que se grababa información mediante perforaciones en lugares determinados, gracias a dicho instructivo, era posible realizar operaciones tales

[2] Ibidem., p. 6

como clasificación, duplicación y copia de fichas perforadas. A raíz de los sucedido Hollerith crea la gran compañía de nombre *Tabaluting Machine Company*, que posteriormente se uniría para formar la *International Business Machine* (IBM).

Ya en el año de 1944, surgen los primeros sistemas electrónicos, a través del profesor Howard Aiken de la Universidad de Harvard, quien desarrolló ya en el seno de la compañía IBM, el primer ordenador conocido por ASCC (siglas de Automatic Sequance Controlled Calculator) o Mark I, el cual fue la primera computadora que funcionaba de manera automática, consistente en más de 200 mil piezas y 800 mil metros de cable.

Para 1946 se creo la primera máquina electrónica de calcular, fue construida en la Universidad Pensylvania, dándole el nombre de ENIAC, (Electronic Numerical Integrator and Automátic Computer), "...la programación del ENIAC se llevaba a cabo mediante el establecimiento de conexiones entre cables eléctricos y al accionamiento de un gran cantidad de interruptores..."[3], mientras que para su funcionamiento externo empleaba bulbos para procesar información.

A partir de este momento, el progreso de estas instalaciones fue de manera acelerado, y siguió una serie de etapas. Los estudiosos de la materia coinciden en dividirlos avances en etapas y que le dan el nombre de "generaciones", los cuales abarcan periodos determinados según el sistema físico o de lógico. Coinciden en señalar hasta ahora en cinco generaciones, los cuales son:

La llamada primera generación abarca de 1946 a 1958, que esta formada por los primeros ordenadores que se desarrollaron en los años 50° y 60° , utilizaban bulbos para almacenar información así como tarjetas perforadas, estas

[3] CERVANTES, Martínez, Jaime Daniel, "Justicia Cibernética como Alternativa ante un Nuevo Milenio", México, Cárdenas, 2001, 509 pp

primeras máquinas eran utilizadas con fines comerciales, y era capaz de realizar hasta 1,000 instrucciones por segundo.

La segunda generación comprende del año de 1959 a 1964, que constituye el invento del transistor, que consistía en un dispositivo electrónico que actuaba como un interruptor, ya que determinaba el paso o no de la corriente entre dos puntos en función de la tensión aplicada a un tercero; mismo transistor hizo que las computadoras fueran más pequeñas y mas fáciles en usar, durante esta época fue utilizado discos magnéticos para guardar información en la memoria de la computadora, así también aparecieron nuevos lenguajes, sistemas operativos, etc.

La tercera Generación abarca de 1964 a1971, se caracteriza por la integración de los circuitos integrados o chip que esta formado por decenas o cientos de componentes en una superficie de 25mm, instalados en la estructura y funcionamiento por lo cual las computadoras fueron mas pequeños, rápidos, expandían menos calor y mas eficientes. La computadora IBM 360 fue la primera en comercializarse usando circuitos integrados, utilizándose para realizar análisis numéricos como administración o procesamiento de archivos.

Cuarta generación (1971 a 1988), es la época mas destacada por sus dos grandes aportaciones que en la actualidad siguen utilizándose, como es el reemplazo de las memorias con núcleos magnéticos, por las de chips de silicio y la integración de mucho más componentes en un chip: producto de la microminiaturización de los circuitos integrados. Teniendo programas de gran nivel utilizados para diseño gráfico, imagen, sonido, animaciones, y transmisión y obtención de información.

El tamaño de los microprocesadores de chips hizo posible la creación de computadoras personales (PC), para uso personal y relativamente más baratas y que actualmente se utilizan en dependencias de gobierno, escuelas, hogares, etc.

A partir de esta generación con la aparición del microprocesador, permitió que la informática se popularizara en toda parte del mundo y aplicándose en las actividades del ser humano, en verdad es imaginable lo obtenido hasta esta época ya que es posible a través de la computadora, las telecomunicaciones, tratamiento electrónico de la imagen, las bases de datos, la inteligencia artificial, el desarrollo de sistemas expertos.

La quinta generación que comprende del año de 1981 y hasta ahora no se conoce su terminación, lo importante es que se caracteriza por la inteligencia artificial y robótica, tratando de desarrollar ordenadores inteligentes.

En las generaciones siguientes, las computadoras serán más versátil, intensamente rápida y más barata, que tendrá acceso a toda persona común, en cualquier parte del mundo ya globalizado, formando una sociedad dependiente de la información, y construyendo su entorno de manera computarizada

1.1. CONCEPTOS BÁSICOS DE LA COMPUTACIÓN

La computadora suele definirse según Téllez Valdes "...la máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida..."[4]

Mientras que los estudiosos de la materia en su mayoría, lo definen a la computadora como una máquina, que resuelve problemas aceptando datos, realizando operaciones preestablecidas sobre ella y entregando los resultados.

Computadora.- "...Es un rápido y exacto sistema de manejo de símbolos electrónicos (datos) que es proyectado, diseñado y organizado para aceptar y

[4] Op Cit, p 10

almacenar automáticamente datos de entrada, procesarlos y producir resultados de salida bajo la dirección de un detallado programa almacenado de instrucciones...".[5]

Los componentes de un sistema de tratamiento de la información se distingue claramente dos:

A. El equipo físico, también llamado Hardware, material o **soporte físico**.
Este lo constituye los circuitos electrónicos y dispositivos mecánicos que constituyen la parte tangible de la máquina.

B. El equipo lógico, también denominado Software, lógica o **soporte lógico**.
Esta parte inmaterial está formada por un conjunto de programas que determinan el funcionamiento de los circuitos físicos que están contenidos en un sistema informático.

A. Entre los circuitos electrónicos o dispositivos mecánicos que constituyen al Hardware, podemos distinguir en:

I. Unidad central
II. Canales de comunicación
III. Unidades periféricas

La forma de funcionamiento de una computadora es:

"En todo computador, el funcionamiento se desarrolla de la siguiente manera: a través de las unidades periféricas se capta y suministra al computador la información proveniente del exterior, luego, ésta se traslada a través de los canales a la Unidad Central, donde se procesa; con posterioridad, la información resultante y elaborada se traslada nuevamente a los periféricos a través de los canales, estos últimos tiene como única finalidad la comunicación entre las

[5] SANDER H. Donald "Informática: Presente y Futuro. México", Edit. MacGraw-Hill, 1987, P.9

unidades periféricas y la unidad central del computador, controlando a su vez a los periféricos que están asociados...".[6]

I. La Unidad Central es el encargado del procesamiento y manipulación de la información, la cual consta de dos partes:

Ahora bien es necesario desglosar cada parte de una computadora, los cuales son:

1. La CPU: Unidad Central de Procesamiento (Control Processing Unit).

2. La Memoria Central

1. La Unidad Control de Proceso (la CPU): Es aquel dispositivo en que se ejecutan operaciones lógicos-matemáticas

2. La memoria Central: "Es aquella parte del computador que esta destinada a almacenar el programa que se requiere ejecutar y sus datos, para suministrarlos a la CPU y los resultados que se generen..."[7], por lo cual es en esta parte donde se almacena los programas durante su ejecución y los datos necesarios durante su ejecución.

II. Los Canales de comunicación, como su nombre lo indica, comunica entre las unidades periféricas y la unidad central de computador; "La interconexión de estos elementos entre sí, y conducida a través de los canales, se realiza a través de *buses*, los cuales, en definitiva, no son mas que hilos por los cuales se trasmite la información en forma de corriente eléctrica..."[8]

[6] HUERTA, Miranda Marcelo, *et al*, "Delitos Informáticos", Segunda Edición, Santiago de Chile. Jurídica Conosur Ltda, 1998. P. 16
[7] Idem, p 22
[8] MARCELO Huerta, Op.Cit . p 24

IV. Las Unidades Periféricas.- "...son unidades de comunicación de la máquina, que permiten la captación y distribución de datos entre la memoria central y el mundo exterior..."[9], a su vez estas se clasifican en :

- Dispositivos de entrada: son aquellos que representan la forma de alimentación de información a la computadora, a través de datos e instrucciones realizados por las unidades periféricas, p.e, el teclado, mause, scanner, cd-ram, digitalizador, etc.
- Dispositivos de salida: esté dispositivo es el medio por el cual recibe los resultados del proceso efectuado, por ejemplo: pantalla, impresora, el trazador de gráficos o plotter, unidad de salida directa a microficha.

B. El Software, como se dijo, es la parte del computador que hace posible la realización, de una incalculable diversidad de servicios con un número limitado de componentes diferentes, a través de un conjunto de programas que determinan el funcionamiento de los circuitos.

Es así, que el software para que pueda funcionar adecuadamente, se requiere la utilización de mejores lenguas de programación, considerados como aquellos medios que permiten la comunicación entre el hombre y la máquina, es decir, entre la máquina y el usuario.

1.2. TELEINFORMÁTICA

Se le da el término a TELEMÁTICA, a todo lo que abarca la revolución tecnológica acelerada, en los campos afines de telecomunicaciones, computadoras, microinformática y bancos de datos. Es el término en boga en los países europeos

[9] Ibidem

Cabe mencionar que la información para ser transmitida en las autopistas de la información es necesario transformarla o convertirla en ceros y unos, el llamado código binario, a esto es lo que se llama digitalización. Con la ayuda de las autopistas de la información que son "...los canales a través de los cuales la información es transmitida y conducida a un fin u objetivo..."[10], da origen a la teleinformática o telemática, que lo definen como "...la disciplina que une a la informática con las telecomunicaciones, esta disciplina se identifica plenamente con la informática por su lado y las telecomunicaciones por el otro...".[11]

La telemática será una fuente para la comisión de crímenes informáticos, ya que la información y el flujo de datos que se produce entre ellos sobre los sistemas de comunicación que realizan una transmisión de manera digital, se encuentra codificada la información a nivel del computador; Es por ello la importancia de la informática en el derecho penal.

Las autopistas o supercarreteras de la información, contiene una simbiosis entre el conjunto de datos automatizados y las técnicas de comunicación, que permite que él computador sea un instrumento esencial para impulsar su expansión de la información a escala global.

Mientras la comunicación y la información automatizada se transmiten a grandes distancias, de la forma más rápida posible en este mundo global, la informática, como la telecomunicación y el del derecho siempre estarán ligados buscando la seguridad informática.

Cabe destacar que la telecomunicación, como se verá, será también un medio para la comisión de delitos contra ordenadores, o como nos dice Daniel R.

[10] RIESTRA Gaytan, Emma, "Curso Introductorio a los Delitos Informáticos", Impacto Tecnológica en la sociedad, Cuaderno de la PGR, P 5
[11] Ibidem, p 7

Nielsen: "...se puede decir que la estructura de las telecomunicaciones es la propia victima de esta nueva era de la información...".[12]

Para no entrar en confusión entre términos en necesario definir la telecomunicación y la telemática, el primer término se define en su artículo 2 del Reglamento de Telecomunicaciones como: "Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o informaciones de cualquier naturaleza por linea física, conductora eléctrica, radioelectricidad, medios ópticos y otros sistemas electromagnéticos"[13]; mientras que la telemática se define como la disciplina que une a la informática con las telecomunicaciones, es decir, la Telemática es un nuevo campo que une a dos áreas para dar origen a otro tipo de comunicación global y permanente en línea.

Ahora bien, no hay que confundir las vías de telecomunicación con la telemática, ya que el primero se conforma todo tipo de instrumento para la comunicación en todas sus formas, ya sea, vía satélite, telefónica, red ancha, etc., mientras la segunda utiliza las primeras para la transmisión de datos o información almacenada en un sistema informático que se encuentra conectado a las vias de la comunicación. Como se verá mas adelante las vías de comunicación no es el objeto material o el bien jurídico protegido de un hecho ilícito contra un soporte lógico de un sistema informático, si no mas bien, son los medios comisivos necesarios para un hecho jurídico punible de larga distancia.

Por ultimo, la telemática es ya una forma de distribuir la información almacenada en un sistema informático y será de gran importancia posteriormente por la técnica en su transmisión y distribución como vaya evolucionando las vías de la comunicación.

[12] NIELSON R. Daniel, "Los casos mas usuales de Criminalidad Informática y Cibernética", Catalana de Seguritat, Num 3, Diciembre 1998, Barcelona España.
[13] Reglamento de Telecomunicaciones, Ediciones Delma p. 481

1.3. DERECHO INFORMÁTICO

Las tecnologías de la información en México se a implantado a diferentes niveles en varios sectores en la sociedad de tal manera que el ex presidente de la República Ernesto Zedillo Ponce de León en su discurso de fecha 3 de Junio de 1998, mencionó: "En el México... las tecnologías de la información son un instrumento de la mayor importancia para la superación productiva de nuestro país y el bienestar de sus habitantes. . Para México es vital promover el uso y desarrollo de las tecnologías de información y procesamiento de datos, en las más diversas actividades de nuestra vida económica, política y social. De ahí que debemos atender el problema que, como ya se explicó, preocupa y ocupa actualmente a muchos de los gobiernos del mundo, a sus comunidades productivas y científicas y del que México, desde luego, no escapa. Es un problema en apariencia sencillo, pero que de no atenderse oportunamente, puede representar un grave riesgo para el funcionamiento de los sistemas de información computarizada."[14]

A través de este discurso implanta la necesidad de enfocarse a los riesgos que puede ocasionar los sistemas de información, es por eso que el derecho se ha desarrollado de tal manera que exista una fuente jurídica, es decir, una rama del derecho que pueda englobar los actos que pudieran alterar el orden jurídico, ya que "...todas las actividades, trabajos y distintas aplicaciones de las máquinas de computación, en sus múltiples manifestaciones, con motivo de la menorización y tratamiento de las informaciones, generan efectos y relaciones jurídicas que, en su conjunto, conforman el derecho informático..."[15]

[14] ZEDILLO Ernesto, "Las tecnologías de la información son un instrumento de la mayor importancia para la superación productiva de nuestro país y el bienestar de sus habitantes", (Discurso del Presidente de la República durante la ceremonia de instalación de la Comisión Nacional de Conversión Informática Año 2000), Los Pinos, México D.F., 3 junio 1998, Edit. Presidencia de la República 10 p.

[15] AZPILCUETA Tomás Emilio, "Derecho Informático", Mac Graw- Hill. P. 56

La palabra "Derecho" atendiendo a su etimología toma su origen de la voz latino *directus* que significa recto, directo, principio del verbo dirigere: dirigir; mientras que la voz latina Jus, designado en Roma al Derecho, no es mas que una contracción de Jussum, participio del verbo *jubere*, que significar mandar; Sin embargo no hay que olvidar que el derecho tiene entre sus objetivos esenciales la necesaria y continua búsqueda de la justicia y el bien común. [16]

Villoro Toranzo, citado por Téllez Valdes, nos dice que el derecho es el "...sistema racional de normas sociales de conducta, declaradas obligatorias por la autoridad, por considerarlas soluciones justas a los problemas surgidos de la realidad histórica..."[17]

Por su parte, Davara Rodríguez dice que la información "...es un bien que tiene unas características determinadas; es, no cabe duda, un bien económico, pero diferente a los demás bienes económicos existentes en un mercado tradicional...

La misma autora describe ciertos elementos que conforma la información, los cuales son:

a) La información es un bien que no se agota con su consumo, es más, puede que se enriquezca, en un desarrollo ideal y utópico, hasta valores incalculables, naciendo otra nueva y rica información, que cada vez va produciendo más información.
b) La información es un bien que puede ser utilizado por muchas personas... al mismo tiempo, sin que por ello se cause ningún daño o perjuicio al propio bien que, posiblemente, sea favorable a múltiples intereses distintos de aquellos para lo que se produjo.

[16] Cfr TÉLLEZ Valdés, pags. 19, 20
[17] Idem

c) La información se convierte en base de desarrollo de una nueva sociedad... que hace poderoso al que la posea y más poderoso aún a quien sepa tratarla y adecuarla a un fin determinado.
d) El centro de atención de las autopistas de la información es la propia información, quedando la llamada autopista como el medio a través del cual es comunicada o localizada."[18]

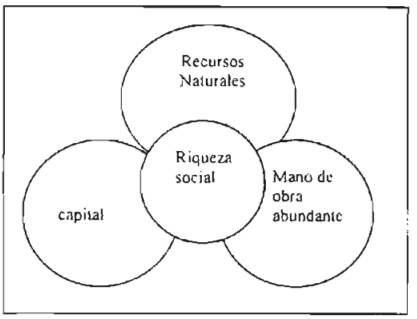
Ahora, la información como se dijo, es inagotable, pero a su vez, es la materia prima del conocimiento que cubre todos sus sustentos: como son los sonidos, palabras, textos, imágenes, datos señalados electrónicos y hasta percepciones; no permitiendo evaluarlos e identificarlos, es por ello que es éste bien no pierde, sino que se enriquece cuando se comparte: es un elemento esencial del cambio; y el derecho tiene el deber de proteger estas síntesis tecnológicas que implican a la transformación y a la evolución de la sociedad y que mas dependen de aquellas en la vida común.

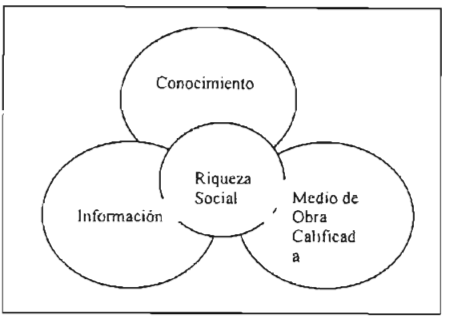
La información y el conocimiento, sustituyeron al capital y recursos naturales que eran factores para un crecimiento económico, sin olvidar también la mano de obra común. Dando origen al "... nacimiento de la *"sociedad de la información"*, en los términos adoptados por la Unión Europea o el inicio de la *era de la "información"* lo cierto que este fenómeno, ha sido reconocido casi en todas partes como el parteaguas en el que concluye la era industrial, para dar paso a la era del conocimiento". [19]

La siguiente figura se observa la diferencia de la sustitución del capital y los recursos naturales de la información y conocimiento:

[18] DAVARA, Rodríguez Miguel Angel, "De las Autopistas de la Información a la Sociedad Virtual", Aranzandi 1996.Pamplona España, p.50

[19] CORPORT México Academia Mexicana de Ciencias, "México Frente a la Era de la Información", Academia Mexicana de Ciencias 59 pp





En la declaración Universal de los Derechos Humanos, aprobada el 10 de Diciembre de 1948, existe un principio consagrado en su artículo 19, estableciendo que todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, de buscar y recibir información e ideas y el de difundir sin limitación de fronteras, cualquier medio de expresión.

Posteriormente en la ciudad de París la UNESCO en 1978, en la XX conferencia general, se aprobó una declaración sobre los medios de comunicación muy ligada a la información en donde se destacó el derecho a la libertad de opinión e información el cual es calificado de inalienable y con respecto a los sujetos que intervienen en el proceso de la información, deberán ser tratados en un plano de la igualdad y de equilibrio.

Ahora bien, lo anterior implica la importancia de la información en el campo del derecho para una protección legal, por lo que han denominado una nueva especialidad del derecho conocido como Derecho Informático el cual es una disciplina ya reconocida en el extranjero, contiene todas las características para ser un derecho especializado, se ha establecido en una ciencia de estudio, y sus resultados se han conjuntado en enciclopedias generales, trabajos jurídicos, etc.

El derecho debe de actualizarse con base a la formación de nuevas ramas que implique proteger la seguridad en una sociedad abstracta donde intercalan sujetos de diferentes partes del mundo en donde el derecho debe involucrarse formalmente.

La informática se ha introducido a la sociedad de una manera inimaginable que es preciso que el derecho controle las actividades relacionadas con la informática, así también que éste sirva para generar una equidad en sus usuarios, de lo contrario las empresas multinacionales serán las encargadas de controlarlos a sus intereses, como sucede con el Internet, que existe una anarquía insuperable de controlar.

Huerta Marcelo define al Derecho Informático como "...el conjunto de principios, instituciones y normas jurídicas de naturaleza fundamentalmente específicas que tienen por fin última la regulación de todo actividad derivada de las ciencias informativas...". [20]

Tamburrini Pietro, considera al derecho informático en un área que como "... fin contenga como objeto al análisis de la ciencia del tratamiento automatizado de datos, y que debe abordar el uso y el eventual abuso de la computación."[21]

Así que, el derecho Informático plantea un desafío, respecto a bienes inmateriales, en el que debe contemplarlos en legislaciones con profundidad y claridad para determinar lo que se requiere de protección; es por eso que hay distinguir el contenido con el continente, no se podrá regular como nuevos descripciones legales conductas que afecten a bienes materiales como el Hardware- que pueden ser encuadradas a tipos legales concretos, específicos,

[20] HUERTA, Miranda Marcelo, Op Cit. 56
[21] TAMBURRINI Pietro, "Computer Crimes en italia", Derecho de alta Tecnologia, Año VIII, No. 88-89 Diciembre 95/Enero 96

tradicionales; sin embargo el desafío es precisamente a bienes inmateriales- como el software- que necesariamente es la información, como bien jurídico a proteger, y de este emboca diversos elementos de gran valor, así como también el soporte lógico que tiene como función automatizar y controlar la información.

Para enfocar mas estrechamente los fines del derecho informático hay que dirigirnos a la definición del Téllez Vades, quien nos dice: "...es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la Informática)...".[22]

Ahora bien, la anterior definición contempla dos vertientes, la primera que se refiere a la informática jurídica, que lo define como "la disciplina interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de informática jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de la información jurídica necesarios para lograr dicha recuperación", es decir, la utilización de las computadoras en el ámbito del derecho. Mientras que la segunda vertiente es el derecho de la Informática, el cual será nuestra guía; que lo define como "...el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática...".[23] Este último es el que describe los fines del derecho objetivo, tratando de contemplar los hechos y actos indebidos basándose en las modalidades del uso de la informática y las comunicaciones, repercutiendo a bienes de la misma naturaleza, y que en tiempos de hoy es de trascendencia jurídico-penal, es por lo tanto que el derecho se amplia formando una nueva rama que pretende ampliar su esfera en ámbitos de una materia de distinta naturaleza, persiguiendo los fines jurídicos para una sociedad de transformaciones. Así lo sostiene Azpilcueta en su obra de Derecho Informático describiendo que " ...si se

[22] TÉLLEZ Valdes. Op. Cit. p. 22
[23] ibidem, p 26

confronta el desarrollo de la criminalidad que interviene en unión estrecha con el hecho informático, advertiremos de la necesidad de llenar los vacíos de nuestra legislación..." [24]

Por consecuencia, el derecho informático es o será una realidad tarde o temprano, ya que "...va adquiriendo carta de naturaleza, aún cuando no está todavía universalmente consagrado como nueva rama del Derecho, aunque si existen numerosas disposiciones legales, una variedad de jurisprudencia y bastantes textos doctrinales al estudio de la materia".[25]

1.4. LOS DELITOS INFORMÁTICOS

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese en todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada tiempo.

En cierta manera es muy complejo definir el "delito Informático" conforme a su naturaleza, ya que la ciencia o profesión han manifestado conceptos a sus propios lenguajes y propósitos, eso impide en llegar a un concepto aceptable; ya que un concepto del delito informático es muy abstracto y necesario para ser compatible en el ámbito internacional por que el concepto estriba en las tecnologías de la información y estas tienen vida global.

En el ámbito internacional no se ponen de acuerdo en una definición sobre los delitos informáticos, pero tampoco se espera en crearlo por su complejidad que

[24] AZPILCUETA, Tomás Emilio, "Derecho Informático", Mac Graw- Hill. P. 38
[25] CARRASCOSA, López Valentín, "Regulación Jurídica del Fenómeno Informático", Informática y Derecho, Abril 1998. P. 36

es la informática, pero lo que si se enfocan en la necesidad de regular las conductas que vulneren a los sistemas informáticos.

Al respecto nos dice nuevamente Carrascosa que la criminalidad informática, tienen como característica esencial el empleo de sistemas informáticas para delinquir, usándolas como medio o fin. Así mismo, manifiesta que una de las principales características es la dificultad en descubrir, perseguir y comprobarla, por que son difícilmente de dejar rastros en los soportes lógicos, ya que se auto destruyen o desaparece en segundos, problemática que se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos y la capacidad de respuesta jurídica se halla fraccionando por las fronteras nacionales.[26]

Mientras Téllez Valdes expresa que, para dar una definición de delitos informáticos no es un labor fácil, ya que para hablar de delito en el sentido de acciones encuadradas en tipo legal, se requiere que tal denominación, es decir de delitos informáticos, este literalmente convidado en los códigos penales, y que en México aún no se ha establecido al igual que diversos estados a excepción del estado de Sonora; Sin embargo están conscientes de la necesidad de esto. Y como distinción entre lo atípico y tipo. Téllez lo define a los delitos informáticos en su forma atípica como "... actitudes ilícitas que se tienen a las computadoras como instrumento o fin; y como Típico como las conductas típicas, antijurídicas y culpables que se tienen a las computadoras como instrumento o fin."[27]

Por su parte, Davara Rodríguez en su manual de derecho Informático, define al delito informático como "...la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un

[26] Cfr CARRASCOSA López Valentín. *Op. Cit.* P.48
[27] Cfr TÉLLEZ Valdes. Op. Cit. P. 104

elemento informático, ya sea hardware o software...".[28] No se comparte su definición, respecto al valor que otorga a los componentes físicos, ya que estos simplemente se pueden tipificar en tipos actuales.

Ahora bien, existen también organizaciones internacionales que expresan su preocupación en los ilícitos informáticos, como la OCDE que lo define al Delito Informático o *computer relatad crimes,* como "...cualquier conducta ilegal, no ética, o no autorizada, que involucra el procesamiento automatizado de datos y/o la transmisión de los mismos...".[29]

Mientras que la UNESCO, en la XIV conferencia de autoridades Iberoamericanas, celebrada en la Habana, en noviembre de 1995, hizo un llamado a todos los gobiernos de los estados a tomar medidas legales por la creación y divulgación de virus informáticos, considerándolos como delitos y exhortándolos a penalizarlos.

El delito se conforma de varios elementos esenciales para su existencia, que faltando uno, deja de existir y no tendría vida jurídica en la norma penal

Para Cuello Calón, los integrantes elementos del delito son:

a) El delito es un acto humano, es una acción (acción u omisión).
b) Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido
c) Debe corresponder a un tipo legal (formula legal), definido por la ley, ha de ser un acto típico.

[28] DAVARA, Rodríguez Miguel Angel, "Manual de Derecho Informático", Aranzandi 2002, p. 338
[29] LLANEZA González Paloma, "Internet y Comunicación digitales; Regimen legal de las Tecnologías de la Información y la Comunicación". Bosh 2000, Barcelona España., 450 pp

d) El acto debe ser culpable, imputable a dolo (intención) o a culpa (negligencia) y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
e) La ejecución u omisión del acto debe estar sancionada con una pena.

Analizando el primer requisito, el derecho penal tiene como objetivo en regular el disvalor de las conductas en las leyes objetivas, a base del principio de *nullum crime sine conducta,* y dentro de los delitos informáticos, esta conducta es desplegada a través de los sistemas informáticos que son utilizados como medio o fin; debe ser claro que, el sistema informático no realiza la acción penalmente relevante, sino que la conducta humana realiza el funcionamiento determinado, para que el sistema informático lo desarrolle, es decir, una anticipación del resultado. Tal conducta para este tipo de delito en estudio, debe ser desplegada por un sujeto capaz de manipular el funcionamiento de algún programa o creación del mismo para fines ilícitos y disvalorada por su resultado.

El segundo, para su existencia del delito informático, la conducta debe lesionar o poner en peligro bienes jurídicamente protegidos, que la sociedad considera válidos y su necesidad de proteger, que en este caso es la información que se encuentra almacenada en los sistemas informáticos, en su caso.

En la vulneración contra el soporte lógico en los sistemas informáticos el bien jurídico a proteger sería el patrimonio o mas bien dicho la disponibilidad patrimonial informática; Sin embargo existe la posibilidad de la creación de un nuevo bien protegido por la norma la cual nosotros consideramos denominarlo como la seguridad funcional en los sistemas informáticos, pero tal término es necesario su explicación, describiéndolo que la "seguridad" en la red debe de consistir en la protección de la disposición en las operaciones informáticas, mientras que en su aspecto "funcional" consiste en la utilidad del servicio del soporte lógico para realizar tales operaciones.

El tercer elemento, es donde radica la existencia del delito informático, ya que sino se contempla el delito informático en un tipo penal, no existe, esto a partir del principio *nullum crimen, nulla poena sine lege*, es decir es una exigencia dogmática que requiere que la conducta se adecue en la formulación objetiva hecha por el legislador en un tipo (tipicidad).

Esta garantía de legalidad esta contemplada en el artículo 16 de nuestra Carta Magna y para no vulnerar los derechos fundamentales deberá ser necesario legislar sobre el tema en comento para evitar interpretar la ley analógicamente y contrario a derecho.

Mientras que el cuarto elemento requiere de la culpabilidad, y que según Cuello Calón esta debe ser a base de la culpa o dolo que pueda ser imputable a una persona. Estos dos elementos subjetivos, dentro de la teoría finalista, se encuentran en el tipo legal, por lo que en la culpabilidad se limita a la imputabilidad de la persona y la reprochabilidad del injusto en la exigencia de haber actuado de otra forma, y dentro de los delitos informáticos solo se puede realizar a manera de dolo.

El quinto elemento, que expresa que la ejecución u omisión del acto deben estar sancionado por una pena, esto a base con el principio de *nulla poena sine lage*, y, mientras no exista una descripción legal de la conducta y su respectiva pena no es posible sancionar el hecho ilícito.

Otro aspecto relevante es la forma de comisión, Davara nos dice que todo delito de lo que damos en llamar informáticos, hay que distinguir el medio y el fin. Para poder estudiar una acción, el medio para su comisión debe ser un elemento, es decir, un bien o servicio, patrimonial, en el ámbito de responsabilidad de la informática; y el fin que se persiga debe ser la producción de un beneficio al sujeto

o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, aun tercero.[30]

Asi, Tamburrini basándose en la definición del delito, define al delito informático como: "...toda conducta típica, antijurídica y culpable cometida contra el soporte lógico de un sistema de tratamiento automatizado de información (programas y datos de determinada naturaleza o importancia) generalmente a través de medios computacionales...". [31]

Es muy debatido los bienes a protegerse jurídicamente, muchos autores entre sus definiciones sugieren la protección bienes tangibles, es decir, los componentes de las partes de los sistemas informáticos, pero lo que debe de protegerse jurídicamente como se dijo, es el soporte lógico en su funcionamiento, y su contenido así como su manipulación de éstos, por que su propia naturaleza lo exige, son bienes intangibles que requieres ser reguladas. No hay que crear tipos innecesarios, ya que existen tipos clásicos que plenamente se tipifican en las conductas recaídas en sistemas informáticos, como es el caso de daños o robo en los componentes de un computador, así como fraude, homicidio..., que únicamente toman como medio un sistema informático, ya que no se puede engañar a un computador o realizar el delito de homicidio.

Téllez clasifica a los delitos informáticos conforme a su utilización para la comisión de un delito, es por ello que toma dos criterios; como instrumento o medio, o como fin u objetivo.

"Como instrumento o medio, contiene los siguientes actos ilícitos:

- Variación de los activo y pasivos en la situación contable de la empresas.
- Robo de tiempo de computadora.

[30] Cfr. DAVARA. Rodríguez Miguel Angel, "Manual de Derecho..., Op. Cit. p.338
[31] TAMBURRINI Op Cit p 42

- Rectora, sustracción o copiado de información confidencial.
- Modificación de datos, tanto en la entrada como en la salida
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (caballo de troya)
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia un cuenta bancaria apócrifa, método conocido como la "Técnica de Salami".
- Introducción de instrucciones que provocan "Interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como "consulta a su distribuidor".
- Alteración en el funcionamiento de los sistemas, a través de los cada vez mas temibles "virus Informáticos".
- Acceso a áreas informatizadas en forma no autorizada.
- Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

Y como fin u objetivo, lo clasifica en:

- Programación de instrucciones que producen un bloque total al sistema.
- Destrucción de programas por cualquier método
- Daño a la memoria-
- Sabotaje politico o terrorismo en que se destruya o surja un apoderamiento de los centros de neurológicos computarizados"[32]

Los medios y fines mencionados por Téllez Valdes, son los mas conocidos, pero como va desarrollándose la informática existirá más innovadores medios y fines que se puedan utilizar para la comisión del algún delito y la norma penal se debe encargar de obstruir y sancionar los actos antijurídicos.

[32] TÉLLEZ. Op Cit. P 105, 106

1.5. LA ERA DEL INTERNET Y SU DELINCUENCIA

El Internet, es ya, una necesidad fundamental para el desarrollo de una sociedad, y una fuente de comunicación tan extensa que interviene todos y cada uno de los estados del mundo globalizado. Es utilizado para transferir todo tipo de información, en donde el emisor y el receptor pueden ser cualquier sujeto conectado a la red, el cual permite almacenar, transmitir, modificar, encontrar y comunicar información en tiempo real, sin tener un límite de espacio, tiempo y volumen, con una mayor calidad.

Laquey Parker, citado por Morón Lerma, quien expresa que el "... Internet es una amalgama de miles de redes de ordenadores que conectan entre sí a millones de personas...".[33]

En esta era del Internet y la forma de su infraestructura al viajar la información, los sujetos que manejan la información contendida en esta red de redes en base de instrumentos informáticos, nace una sociedad nueva identificada por Davara Rodríguez como la sociedad de la información, y también denominada por Gore, citado por la misma como autopistas de la información, dicha sociedad "...abre el camino de la revolución cultural mas grande que ha conocido la humanidad, teniendo a desaparecer una especie protegida dentro del género humano, que es la de ser rutinario y gris que entra en una monotonía de comportamiento en sus actitudes en la vida y que no estará permitida o no será posible llevar a cabo ante el nuevo modelo social que se presenta...".[34]

Como se dijo que, la información y el conocimiento es poder, este instrumento que es la red de redes controla y engloba información almacenada en los ordenadores conectados en él, y acceder en cualquier parte del mundo, por

[33] MORON, Lerma Esther, "Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red", Aranzadi, 1999. p. 95
[34] Ibidem. p. 33

lo que "los grupos sociales de esta nueva sociedad serán los trabajadores del saber que serán aquellos que sepan aplicar el saber a un uso productivo

1.5.1. ORIGEN Y DESARROLLO DE INTERNET

El Diccionario de la Lengua Española define al Internet como: "**1.** amb. *Inform.* Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación." [35] (ORTOGR. Escr. t. con may. Inicial.)

Su origen del Internet fue a base militar tecnológica estadounidense, en plena guerra fría, con el fin de crear una red de comunicación menos vulnerable contra acciones atómicas militares soviéticas. El primer mensaje ni siquiera llego completo, llegando únicamente dos palabras, por lo cual tuvo mucho éxito.

Por lo que más tarde el gobierno estadounidense promueve una red experimental denominado ARPA (Agencia de investigación de proyectos avanzados) creada para centralizar todos los avances aplicables al ámbito militar, con el fin de facilitar la comunicación de investigadores científicos que investigaban y desarrollaban el tema, en diversas universidades situados en lugares lejanos.[36] Su propósito era crear una red conectada con varios ordenadores, para que la información pudiera viajar por un camino u otro, para el caso de existir una vulneración, la información llegase a su destinatario. De manera que esta red creció durante los años setenta y ochenta, ofreciendo nuevos servicios y conectándose a nuevas redes con el mismo lenguaje (TCP/IP).

A finales de los setenta deja de ser utilizado la red para fines militares , y, Internet fue recibida a la sociedad civil. Y para 1984 ya existían 1000 ordenadores

[35] http //buscon rae.es/diccionario/drae.htm Consultado en fecha 4 de Abril de 2005.
[36] Cfr. LAGARES García Diego, "Internet y Derecho ; Tecnología y Jurisprudencia. Dos Conceptos Obligados a Entenderse", Careria, p.17

conectados; cinco años más tarde ya era mas de 10.000; y es precisamente en 1990 donde se expande en las conexiones caseras.[37]

Actualmente, cualquier persona puede ofrecer su propia página, un lugar virtual en el WWW (World Wide Web) o abrir su propio foro de discusión, de los que hoy en dia existen alrededor mas de setenta mil y que abordan desde temas muy interesantes hasta muy deleznables incluyendo comportamientos criminales.

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar a la red, lo cual marca un principio universalmente aceptado por los usuarios y que a dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cual sería la *ratio iuris* o razón de ser de esta especial normatividad.

Actualmente es casi imposible calcular los sitios web que existen y los servidores a los que tenemos acceso. Internet se ha desarrollado en esta última década mucho, y en parte es debido a los fines comerciales de las empresas. Internet ya no es la red de investigación ni militar para lo que fue creada, ahora Internet es, ante todo, un negocio, y eso ha sido lo que ha empujado su desarrollo.

WWW (World Wide Web o telaraña mundial) es un sistema de servidores de páginas gráficas compuestas con imágenes, sonidos, textos y animaciones. Para poder visualizar estas páginas (que son las sobradamente conocidas páginas web) se utiliza el protocolo http (Hyper Text Transfer Protocol o Protocolo de Transferencia de HiperTexto).

La base de WWW son las páginas web. Las páginas web están escritas en un lenguaje de programación llamado HTML, y se basan en el hipertexto e hipermedia. Hipertexto son los enlaces de un texto a otro, entre páginas web, que

[37] Cfr. DAVARA, Rodriguez Miguel. "Manual de Derecho..." Op. Cit p. 91

no tienen porque estar situadas en el mismo lugar del mundo. Hipermedia son enlaces no solo a textos, sino también a sonidos, imágenes, animaciones, etc.

1.5.2. EL FUNCIONAMIENTO DEL INTERNET

Esta red de redes, permite conjuntar la información en sus diferentes formatos, utilizando la telemática para su transmisión, en donde el texto, la voz, el vídeo, el sonido, animaciones, etc., son convertidos en la lengua de la digitalización, dando un resultado eficaz, en su utilización. Kurcyn Villalobos, establece que su dos principales características es su convergencia y su digitalización. Convergencia: puesto que es un lugar donde diversas disciplinas, técnicas, sonido, imagen y texto convergen. Y digitalización ya que la convergencia ha sido posible gracias a esta nueva técnica de distribución de la información.[38]

La función del Internet en una comunicación directa en donde existe un punto de origen y destino, interviniendo las redes telemáticas, utiliza un sistema de fragmentación o conmutación de información en el lenguaje del conmutador (byte Kbytes, Mbytes, etc,), que son tratados individualmente y procesados en lo que se denomina *nodos de transmisión o Routers.*; a diferencia de las comunicaciones telefónicas en donde la comunicación se transmite en un solo paquete, sin intermediarios.

Morales García, expone cuatro niveles para su comprensión en la comunicación en las redes, cada una de las cuales permite la ejecución de secuencias necesarias para el envío y recepción de datos:

---

[38] Cfr. CORPORT México Academia Mexicana de Ciencias, Op. Cit p 23

1. "El primer niveles se trata de las aplicaciones, a base de un lenguaje específico como es el caso de "http; ftp; telnet; etc.", que el cliente utiliza para enviar información al servidor, obteniendo un servicio específico, como son; correo electrónico, transferencia de archivo, etc.
2. Para que esta comunicación de servicio sea viable, es necesario el siguiente nivel, denominado *aplicaciones*, para dicha comunicación es necesario el funcionamiento del Protocolo de Control de Transferencia (*TCP: Transfer Control Protocol*), que tiene como finalidad dar garantía en la integridad electrónica al enviar la información: y su función en recoger la orden y fragmentarla en paquetes, numerando cada uno de ellos. Para que de este modo, el ordenador que hace las veces de servidor, sabrá en el mismo nivel, si la información está completa o si falta paquetes de información, en cuyo caso, el servidor reclamara a la máquina cliente que vuelva a efectuar la petición.
3. El Protocolo de Control de transferencia viaja (envía los paquetes) al siguiente nivel, denominado el nivel de Red, éste utiliza un protocolo especifico, denominado protocolo de Internet *(IP: Internet Protocol)*, es decir, el *TCP* viaja sobre *IP*, lo que gráficamente se acostumbra a designar como *TCP/IP*. El Protocolo de Internet permite conocer el servidor, en este caso, cual o quién es el destinatario final de la información, en función de la dirección impresa que lleva la máquina cliente así como la dirección que dicha máquina reclama. El IP, en definitiva, es una sucesión de números que identifican tanto la máquina cliente como la del servidor al que ésta reclama un servicio determinado. Como sucesión numérica el IP contenía una dificultad intrínseca para la expansión de Internet como sistema, consistente en la complejidad numérica asociada a los servicios para ser memorizada.

De esta forma surge el sistema de Nombres de Dominio *(Domain Names)* que consiste en una conversión del IP numéricos en una sucesión alfanumérica que facilite, como recurso mnemotécnico la asociación del IP como destino elegido en el *host* por el usuario (cliente). Para facilitar dicha conversión en la dos vías

(alfanumérica, para la mejor compresión del usuario y numérica, pues el sistema continúa utilizando números en la lectura del origen y destino de la comunicación) fue creado el denominado *DNS: Domain Name System,* el Sistema de Nombres de Dominio: los nombres de dominio, por lo tanto, se limitan a facilitar la conexión de los usuarios de la red; pretenden su identificación en la misma, pero no su distinción.

El nombre de Dominio se estructura en tres niveles.

El *Top Level Domain* o Nombre de Dominio de Primer Nivel indica la localización territorial o genérica del servicio buscado. Se subdivide, pues, en dos clases, aunque funcionalmente idénticas: TLD territorial y TLD genérico. El primero responde a un determinado territorio estatal, expresado por dos letras, cuya regulación general se encuentra en la norma ISO 3166. Los TLD territoriales pueden dividirse, a su ves, en abiertos o restringidos, en función de las condiciones de registro impuestas a los usuarios en la normativa concreta que cada país efectúa respecto a su Código Territorial. Lo mismo sucede con los TLD genéricos, que serán abiertos o restringidos, en función de la capacidad de los usuarios para poder operar con ellos. El dominio de segundo nivel identifica propiamente el producto solicitado, es decir, el nombre que el usuario ha pretendido obtener al registrar un Nombre de Dominio. Por último, el nombre de dominio de tercer nivel identifica el tipo de servicio buscado, es decir, si se trata de una página web (www), una transferencia de archivo (ftp), de una actuación remota (telnet), etcétera.

4. En el nivel Sub-red, por lo tanto, lo que cabe analizar es el tipo de conexión establecida, esto es, conexión a través de *Red de Área Local* (LAN) o conexión Punto a Punto entre dos *Routers,* o la linea telefónica, que sustentará la comunicación desde un punto específico de la red." [39]

[39] MORALES, Oscar *et al.* "Contenidos ilícitos y Responsabilidad de los Prestadores de Servicios de Internet", Aranzad, 2002, número 8. P 179, 180, 181.

1.5.3. SU DELINCUENCIA INFORMÁTICA

La delincuencia informática a surgido desde el principio con las tecnologías de la información; el delincuente requiere un conocimiento especial, es decir, un conocimiento que permita manipular el funcionamiento de un sistema informático, que permita utilizarlo como medio o como fin para la comisión de un delito. Su protección es el anonimato, que este último es considerado un derecho del usuario del Internet.

No puede ignorarse las conductas más destructivas en el Internet que, sujetos mediante sus identidades anónimas, en la mayoría de los casos, vulnere passwords, correos electrónicos, software, e introduzca mensajes destructivos o imágenes con pornografía Infantil, etc.

Los sujetos activos que intervienen en la comisión de los delitos informáticos, se ha dicho que. deben poseer cierto conocimiento en la manipulación sobre la función de un sistema informático, y varios criminólogos aducen que son personas decididas, motivadas y dispuesto a aceptar cualquier reto tecnológico.

Los principales sujetos son:

Hackers: anteriormente eran denominados con ese término a las personas que tenían un cocimiento abundante sobre los sistemas informáticos; en la actualidad se les conoce a aquellas personas que ingresan a una computadora o redes de comunicación electrónica de datos, sin autorización o mas allá de lo autorizado, en virtud de la función selectiva del elemento subjetivo del injusto: vulnerar la intimidad, descubrir secretos, dañar, etc., a base de su sobrenombre: *nicknams.*

Su idiosincrasia del *hacker*, responde fundamentalmente al deseo de curiosidad, y reto constante a los sistemas informáticos. Y suele clasificarse en tres: los buenos (white), malos (black) e intermedios (gray)

Cracker: Son aquellos sujetos que no acceden por curiosidad o por que se represente un reto, sino con la finalidad de destruir información vulnerando los passwords. Suele ser la conducta posterior a la del hacker.

Existen dos tipos de cracker: a) son aquellos que acceden al sistema informático con el propósito de robar información, destruyendo el mismo; b) son los que se debilitan o destruyen el software.

Phreackers: Son los denominados "piratas telefónicos", que utilizan las telecomunicaciones para utilizarlos gratuitamente.
Sniffers: Son aquellos que realizan programas rastreadores, que se usan para acceder al disco duro de los ordenadores conectados en la red (Internet), buscando información determinada. Uno de los actos es que ya encontrándose en la red, un *sniffer* recoge los *mails* que por él circulan y permite su control y lectura.

Spamming: Los sujetos envían mensajes inconsentidos de mensajes publicitarios por correo electrónico a una multitud de desconocidos.

Existen por supuesto diversos sujetos con otros adjetivos que actúan utilizando nuevas herramientas innovadoras para la comisión de los delitos, que durante el transcurriendo el tiempo, la complejidad de su conducta es muy compleja y difícil en su identificación.

Estos sujetos activos en la nueva era de una delincuencia, como se observa, han tomado como fin o medio en su actividad instrumentos lógicos (inmateriales), como son: la información, o bien, el mismo soporte lógico, es decir, "... estos bienes materiales evolucionan hacia un concepto lógico, menos tangible

físicamente, pero con el mismo grado de relevancia por lo que se refiere a la necesidad de protección legal y actuación policial...".[40]

En México, las pocas leyes contra la delincuencia informática pueden ser vulneradas por no existir un adecuado ordenamiento legal para su regulación, por lo que si se quiere reglamentar de manera eficazmente se tendrá que realizar más acuerdos internacionales que tiendan armonizar las reglas aplicables a estos problemas. En otras palabras nos dice Ovilla Bueno "... los problemas que México tendrá en el futuro con respecto a Internet serán problemas relacionados con la aplicación de leyes (conflicto de leyes en el tiempo y en el espacio), y la determinación del juez competente para resolver un conflicto dependerá de la cultura y de la sensibilidad del juez en la interpretación de las normas por aplicar."[41]

1.6. LA VULNERACIÓN EN LOS SOPORTES LÓGICOS

La conducta contra los soportes lógicos es muy trascendente pero poco regulado en las diversas legislaciones tanto nacionales como internacionales, esto por que únicamente se enfocan a la información, pero olvidan el valor que tiene el programa que sirve como soporte a la misma, anexando a la conducta un resultado necesario que es la información destruida.

Existe la conducta dirigida especialmente a la destrucción a la información, en donde el soporte informático es utilizado como medio y como fin para la comisión del delito, pero incumbe a otro tipo de investigación.

---

[40] NIELSON R. Daniel, Op Cit. P. 21

[41] ORILLA Bueno Rocio, "Internet y Derecho de la Realidad Virtual a la Realidad Jurídica", Boletín Mexicano de Derecho Comparado, V.31, No. 92, Mayo- Agosto 1998, p 435

Por lo que el acto que vulnera al soporte lógico se caracteriza por que utiliza al sistema informático como fin, y no como medio, este es así por que el sujeto actuando dolosamente esta consciente de su actuar y el objeto material a vulnerar; no puede actuar culposamente, ya que su conducta, que, sin el debido cuidado que debiera tener, "introdujera un programa para destruirlo" o "manipulara el software para dañarlo" seria absurda. Estos actos generalmente son realizados personas que trabajan en la mismo fuente laboral o personas que crean el programa.

Es posible que se dañe el software alterando el funcionamiento, con una conducta directamente a los componentes físicos, pero en este caso se hablaría un daño material y otro daño inmaterial: pero el nuevo problema es que la conducta es acompañada de un instrumento lógico destructivo, es decir, introduciendo un programa denominado virus o manipulaciones al sistema lógico (inmaterial) para dañar el software (inmaterial) y por lo tanto su funcionamiento. Este punto esta muy abandonado en las legislaciones.

Al respecto el Código Penal, en su libro segundo, dentro del capítulo vigésimo sexto, denominado, De los delitos en materia de derechos de autor, en el artículo 424 bis fracción II establece "se impondrá prisión de tres meses a seis años y de trescientos a tres mil días multa: A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación." Dicho artículo expresa el desactivar los candados electrónicos para la desprotección del programa y así vulnerar su autoria como sujeto pasivo, sin embargo es necesario ir más allá en la protección de la autoria del programa, protegiendo al programa mismo como bien intangible y tipificarlo no únicamente como bien jurídico la intelectualidad, sino la seguridad del funcionamiento de un soporte lógico, por lo que el sujeto pasivo debe ser el estado no teniendo calidad especial.

Por su parte, dentro del Titulo Quinto "Delitos en materia de Vías de comunicación y de correspondencia", son tipificados las conductas siguientes:

> Artículo 167.- Al que interrumpiere la comunicación telegráfica o telefónica, alámbrica o inalámbrica, o el servicio de producción o transmisión de alumbrado, gas o energía eléctrica, destruyendo o deteriorando uno o mas postes o aisladores, el alambre, una máquina o aparato de telégrafo, de un teléfono, de una instalación de producción o de una línea de transmisión eléctrica.

Aqui la conducta tiene como dirección a la destrucción o deterioro material de los medios de comunicación como son: postes o aisladores, el alambre, una máquina o aparato de un telégrafo, de un teléfono, de una instalación de producción, o de una línea de transmisión eléctrica, es decir, la infraestructura útil para la comunicación.

Mientras que en el artículo 533 de la Ley de Vías Generales de Comunicación establece:

> Los que dañen, perjudiquen o destruyan las vías generales de comunicación, o los medios de transporte, o interrumpan la construcción de dichas vías, total o parcialmente interrumpan o deterioren los servicios que operen en las vías generales de comunicación o los medios de transporte, serán castigados con tres meses a siete años de prisión y multa de cien a quinientos veces el salario mínimo general vigente en el área geográfica del Distrito Federal.

Pero que se entiende por vías generales de comunicación, éste mismo ordenamiento reconoce como vías, las rutas de servicio postal; mientras el artículo

4 de la Ley Federal de telecomunicaciones en su artículo 3 fracción VIII, establece como Vías generales de Comunicación a:

- Las redes de telecomunicación: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencia de aspecto radioeléctrico, enlaces satelitales, establecidas, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como en su caso, centrales dispositivos de conmutación o cualquier equipo necesario.

- Sistema de comunicación vía satélite: el que permite el envío de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envia de regreso a la tierra para ser captadas por estación receptora.

Ahora bien, dichas normas se enfocan nuevamente a los medios de comunicación material, como las redes de telecomunicación y los sistemas de comunicación vía satélite, que en sus definiciones respectivas describen como están compuestas, pero no incumbe a la informática sino a la telemática, que es el medio de transporte, que utilizando las vías de comunicación transmite la información. Por lo tanto la informática es la fuente de la información almacenada y la telemática es el campo de transporte de la información almacenada utilizando las vias de comunicación, en consecuencia la norma no protege el soporte lógico donde se almacena la información sino únicamente las vías de comunicación, es mas, los bienes jurídicos a proteger son diferentes, ya que las normas transcritas protegen la comunicación, mientras el soporte lógico es el **patrimonio**, pero tal protección al funcionamiento del soporte lógico no existe aún.

Otro aspecto trascendente, es que tanto los sujetos que generalmente lo realizan- ya mencionado en el párrafo anterior- como en el Internet, existe una gama de posibilidades para realizar diversas modalidades de conducta, pero una

vez realizada el acto contra el soporte lógico dañado, se dificulta la investigación y persecución del delito.

1.6.1 CONDUCTAS QUE VULNERAN EL FUNCIONAMIENTO DEL SOPORTE LÓGICO

Ahora bien exponer las conductas trascendentes para que un sistema informática sea alterado en su funcionamiento normal. Lo más esencial es el daño producido a través de la conducta del sujeto activo, causando daños irreparables al soporte lógico del sistema.

No se le puede llamar Sabotaje informático este tipo de vulneración, ya que el delito como tal no existe en la legislación, por tal motivo es relevante que se tipifique de acuerdo a los supuestos jurídicos explícitos encontrados en la ley vigente, sin ninguna denominación específica; pero también existiría una serie de problemas jurídicos entre países, por no concordar el supuesto jurídico aplicable o denominación especial o en apartado especial entre legislaciones. Por lo que hasta ahora se considera partir de las conductas "digitales" y regularlas apegándose a delitos de patrimonio, ya que mientras no existe una regulación de los delitos con una denominación informática específica no se le puede llamar sabotaje informático.

En la doctrina internacional este tipo conducta se le ha denominado sabotaje informático, definiéndolo Salt Marcos como "...el daño causado a sistemas informáticos, ya sea en sus elementos físicos (hardware) o en la información intangible contenida en sus programas..."[42], no se concuerda con su opinión ya que un sabotaje informático no únicamente el daño recae en la

[42] Marcos, "Delitos Informáticos". Justicia Penal y Sociedad, Año 4, No 6, Abril de 1997, 49-69 SALT

información, no tomando en cuenta los programas que también es un bien intangible que se puede cuantificar en su utilidad funcional.

En el código penal de perú, clasifica al sabotaje informático en tres categorías al sabotaje informático:

1. "Atentados contra un sistema de tratamiento de la información o de sus partes componentes"

Comprende tanto la destrucción o inutilización de un sistema de tratamiento de la información.

2. Atentados en contra el funcionamiento de un sistema de tratamiento de la información.

Comprende tres tipos de conducta:

- Impedir el funcionamiento del sistema
- Obstaculizar el funcionamiento de un sistema
- Modificar el funcionamiento de un sistema

3. Atentados contra los datos contenidos en un sistema automatizado de tratamiento de la información. Se pueden clasificar en

- Alterar los datos contenidos en un sistema de tratamiento de la información.
- Dañar los datos, o
- Destruir los datos contenidos en un sistema de tratamiento automatizado de la información.

Estamos de acuerdo que estas conductas sancionadas por el código punitivo peruano son los actos adecuados que permiten vulnerar un soporte lógic. Estas conductas van dirigidas a desestabilizar el funcionamiento del soporte lógico

configurando un hecho ilícito que debería sancionar la ley penal mexicana, nosotros nos apegamos a las conductas por su trascendencia en su resultado: obstaculizar, modificar, destruir y la negación de servicios.

Ahora bien, Las personas que generalmente realizan estos tipos de vulneración, suelen ser aquellas que actúan desde dentro de la empresa o por propietarios de los programas que actúan de esta forma por el supuesto negativo del pago de la programación, generalmente estos actos pueden ser descubiertos sin dificultad. Existen condiciones con dificultad en donde las personas que vulneran se encuentran en otro estado, o bien personas que utilizan un ordenador ubicado en otro estado, utilizando un software en otro estado diferente, para que el resultado de su conducta recaiga en ordenadores ubicados en unas calles de su casa.

Este tipo de conductas tienen un riesgo, ya que existe "...la posibilidad de manipulación de sistemas informático de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, etc. Permite imaginar incontables posibilidades de comisión de conductas delictivas de distintas características que exceden el marco de los delitos económicos y contra la privacidad de las personas...".[43] Hasta el momento existe la vulneración mas cometida por la red redes, que es la negación de servicios, que es catalogada como una nueva conducta cibernética contra el funcionamiento contra el soporte lógico.

Las negaciones de servicio (conocidas como DoS, *Denial of Service*) son ataques dirigidos contra un recurso informático (generalmente una máquina o una red, pero también podría tratarse de una simple impresora o una terminal) con el objetivo de degradar total o parcialmente los servicios prestados por ese recurso a sus usuarios legítimos; constituyen en muchos casos uno de los ataques más sencillos y contundentes contra todo tipo de servicios, y en entornos donde la

[43] SALT Marcos, Op Cit p.51

disponibilidad es valorada por encima de otros parámetros de la seguridad global puede convertirse en un serio problema, ya que un pirata puede interrumpir constantemente un servicio sin necesidad de grandes conocimientos o recursos, utilizando simplemente sencillos programas, un módem y un PC casero.

Las negaciones de servicio más habituales suelen consistir en la inhabilitación total de un determinado servicio o de un sistema completo, bien porque ha sido realmente bloqueado por el atacante o bien porque está tan degradado que es incapaz de ofrecer un servicio a sus usuarios. En la mayor parte de sistemas, un usuario con acceso *shell* no tendría muchas dificultades en causar una negación de servicio que tirara abajo la máquina o la ralentizara enormemente; esto no tiene porqué ser - y de hecho en muchos casos no lo es - un ataque intencionado, sino que puede deberse a un simple error de programación.

De un tiempo a esta parte - en concreto, desde 1999 - se ha popularizado mucho el término 'negación de servicio distribuida' (*Distributed Denial of Service*, DDoS): en este ataque un pirata compromete en primer lugar un determinado número de máquinas y, en un determinado momento, hace que todas ellas ataquen masiva y simultáneamente al objetivo u objetivos reales enviándoles diferentes tipos de paquetes; por muy grandes que sean los recursos de la víctima, el gran número de tramas que reciben hará que tarde o temprano dichos recursos sean incapaces de ofrecer un servicio, con lo que el ataque habrá sido exitoso. Si en lugar de cientos o miles de equipos atacando a la vez lo hiciera uno sólo las posibilidades de éxito serían casi inexistentes, pero es justamente el elevado número de "pequeños" atacantes lo que hace muy difícil evitar este tipo de negaciones de servicio.

A pesar de las dificultades con las que nos podemos encontrar a la hora de prevenir ataques de negación de servicio, una serie de medidas sencillas pueden ayudarnos de forma relativa en esa tarea; las negaciones de servicio son por

desgracia cada día más frecuentes, y ninguna organización está a salvo de las mismas. Especialmente en los ataques distribuidos, la seguridad de cualquier usuario conectado a Internet (aunque sea con un sencillo PC y un módem) es un eslabón importante en la seguridad global de la red, ya que esos usuarios se convierten muchas veces sin saberlo en satélites que colaboran en un ataque masivo contra organizaciones de cualquier tipo. Cuanto más difícil se lo pongamos cada uno de nosotros a los piratas, mucho mejor para todos.[44]

Así, una vez expuesto algunas conductas relevantes que puedan vulnerar sistemas lógicos. se llega a la conclusión de la necesidad de crear o no tipos penales específicos con el fin proteger penalmente y de manera global todos los posibles comportamientos delictivos relacionados con la informática, tomando alternativas, como son:

a) "Creación de tipos específicos.
b) Reinterpretación de los tipos penales ya existentes, con la finalidad de subsanar las pequeñas lagunas y
c) En un último término, junto a una interpretación teolológica de los tipos existentes, añadir algún párrafo a éstos tendentes a la subsanación de dichas lagunas."[45]

Nosotros nos apegamos al inciso "a)" por la necesidad de que el derecho penal debe proteger bienes intangibles que por la naturaleza de la informática se creo y como característica esencial para su protección existe el elemento: utilidad funcional.

[44] Cfr. http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node275.html. Consultado el 18 de Septiembre de 2005
[45] MIR Puig Santiago "Delincuencia Informática", Promociones y publicaciones universitarias, 1992, Barcelona España, p.160

1.6.2 LA IMPORTANCIA PARA SU REGULACIÓN

La tecnología se va introduciendo en la vida cotidiana en todas sus formas, en estos tiempos se lee, se observa y se escucha muchos cambios en la tecnología, modernos instrumentos informáticos salen al mercado cada dos meses o posiblemente en menos tiempo, con una serie de funciones inimaginables, con una rapidez increíble, convirtiéndose en una necesidad para muchos en su vida.

En nuestro país es nuevo el tema del mundo cibernético, en comparación con otros estados desarrollados, sin embargo días tras día va en aumento la utilización de esta tecnología en cualquier parte del mundo, aún la mas pequeña y alejada de las grandes ciudades, englobando culturas, ideologías, religión, política, economía, y posiblemente el derecho, en el cual, conforme a los tiempos sería una necesidad que reclamaría un buen común en esta materia.

Ahora bien, el bien común es parte de los fines del derecho, y el derecho penal le permitiría otorgar a la sociedad una seguridad jurídica cuando los actos intervengan y perturben sus intereses comunes. Y su contemplación en una norma penal sería la forma de limitar comportamientos que perjudicaría, en ocasiones irreparables, el sistema lógico de un sistema informático pertenecientes a Instituciones de gobierno o dependencias privadas transnacionales.

La ley penal debe ser mas objetiva al regularlas, no debe inmiscuirse en elementos culturales e ideologías sin rumbo, es decir, al momento de constituirlas se debe observar que la persona que accede *de facto* a un mundo global cibernético (Internet) esta percibiendo una **realidad igual** en todos sus ángulos en cualquier parte en que se encuentre, su acto y su efecto al utilizar sus funciones específicas el resultado va a ser semejante ya que han sido programadas para un fin.

Por lo que respecta a los comportamientos que se estudia, es preciso señalar que el sistema lógico suele ser vulnerado para cualquier fin, ya sea un acceso ilicito, observar y obtener información restringida, intercepción de correos electrónicos, obtener información en PC's de pequeños y grandes negocios, etc., ya que es necesariamente manipular dicho sistema inmaterial para conseguir lo deseado. Es por aquello su importancia y valor de un sistema lógico por que para cualquier acto sea licito o no, es necesario su manipulación.

Existen conductas como son: obstaculizar, modificar, destruir y la negación de servicios, que todas y cada una de ellas, son las formas de vulnerar con mas eficaz a través de mecanismos informáticos, el sistema lógico perteneciente al estado. Por lo que nosotros consideramos que dichas conductas es el eje primordial que permite a base de su regulación en un tipo penal una limitación en todos los actos que tiene como fin vulnerar un sistema lógico.

Teniendo un Código Penal Federal a la adecuación a las necesidades que se originan a través de la tecnología, y a su vez teniendo las herramientas legales para subsanar aquellos espacios no conocidos por el temor de conocer un mundo diferente a lo acostumbrado, así como no estudiar conductas innovadoras con relación al uso de la misma tecnología, con la limitante de que dichas conductas no refiere nada desconocido de lo conocido. Por lo anterior si tuviéramos la voluntad de analizar todo este nuevo mundo con el apoyo de especialista en la materia de informática, congresistas y todos aquellos que buscan dicha seguridad jurídica en la informática, obtendríamos un conjunto de leyes eficaces para combatir los actos, que se traducen en manipulaciones informática, y que cada día son poderosos, obtendríamos la materialización de leyes que se necesitan para este mundo mas peligroso.

2. CAPÍTULO 2.

2. CAPÍTULO 2.

MARCO LEGAL

2. EL TRATADO DE LIBRE COMERCIO

TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLC)

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

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

De esta forma, debe mencionarse que los tres Estados parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado procedimientos y sanciones

penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

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

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

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

2.1. CONSTITUCIÓN DE LOS ESTADO UNIDOS MEXICANOS

> **Artículo 6.** 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.

El citado artículo consagra la libertad de expresión como garantía de individual, estableciendo una libertad de expresar toda idea, es decir, existe un libre pensamiento y una potestad de exteriorizarlo sin inquisición judicial, administrativa

o militar, sin embargo existen condiciones limitadas al ejercer tal derecho, que éste no debe en contra de las buenas costumbres, a la moral, los derechos de tercero, perturbe el orden público o cometa algún delito; la Suprema Corte aún no ha establecido y determinado la moral u orden público, esto permite que dichas autoridades judiciales y administrativas la interpreten subjetivamente produciendo actos mas allá de lo permitido y en consecuencia actuar inconstitucionalmente.

Ahora bien, es preciso señalar que esta manifestación de ideas se ha vulnerado en una esfera incontrolable - como el Internet – en donde es más propicio la divulgación de ideas antisociales y su persecución es mas compleja.

Por otro lado, en su último párrafo del artículo en comento, establece el deber del Estado de garantizar el acceso a la información, por tal es consecuencia del proceso ilimitado de adquisición y transmisión de información, ubicado en cualquier dependencia o equipo de almacenamiento, por tal motivo, existe la Ley de acceso a la Información que señala los lineamientos legales para controlar la distribución de la información. El estado no esta obligado a informar sino proteger o asegurar el derecho a la información.

ARTÍCULO 14 CONSTITUCIONAL

> **Artículo 14.** Nadie podrá ser privado de la vida, de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante tribunales previamente establecidos en el que se cumplan las formalidades esenciales del procedimiento y conforme a las leyes expedidas con anterioridad al hecho.

En su párrafo tercero, establece que "en los juicios de orden criminal queda prohibido imponer, por simple analogía y aún en mayoría razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito que se trata.

Esta garantía individual, que toda persona encontrándose en territorio mexicano dispone, consiste basándose en el principio "nulle pena, nulle delictum sine lage", es decir, no hay pena, no hay delito sin ley, que en virtud de no existir una ley aplicable al caso concreto queda prohibido imponer pena, como lo establece nuestra carta magna, por simple analogía, por consiguiente queda prohibido en el campo criminal, imponer pena que no esté estrictamente descrito en una hipótesis normativa. Esto atribuye que el legislador considere la necesidad de definir las conductas que se involucra con los instrumentos informáticos y plasmarlos en la ley, ya que sin las modificaciones necesarias se aplicara la ley con interpretaciones que vulnere la legalidad y seguridad jurídica que garantice las garantías individuales que otorga la carta magna.

Ahora bien, como se dijo, en la red de redes (Internet), existe una serie de ilícitos cometidos contra bienes de interés social, que el derecho debe proceder a penalizarlos, teniendo que clasificarlos para tener una eficaz tipificidad, para llegar a establecer las conductas trascendentes e innovadoras, para no caer en el error de regular actos que ya están tipificados o regulados en leyes secundarias.

2.2. CÓDIGO PENAL FEDERAL

Aunque se regulo ciertas conductas ilícitas en contra de sistemas informáticas, hoy han quedado obsoletas, es necesario nuevamente ampliar la gama de situaciones posibles a fin de proteger ciertos bienes intangibles que no pueden ser tipificados con normas tradicionales, así nos dice Gómez Alejandro "... la aplicación de técnicas informáticas ha creado nuevas posibilidades de uso indebido de computadoras y demás mecanismo informáticos que no pueden encuadrarse en conductas tipicas preexistentes, lo que ha generado la imperioso

necesidad de tipificar nuevas conductas que prevean la comisión de los denominados delitos informáticos".[46]

En la exposición de motivos de la iniciativa del Ejecutivo Federal, presentada ante el Senado de la República el 13 de noviembre de 1998, reconoció que el uso de la tecnología informática es un instrumento que facilita a la sociedad su desarrollo económico y cultural, mediante su empleo en todas las áreas del desarrollo nacional.

Así mismo reconoció las conductas ilícitas que constituyen los "delitos cibernéticos", como son: el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de la información, el sabotaje por computadora, la interceptación de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos, sin embargo no son lo únicos a regular dentro de la esfera informática quedándose limitado la visión problemática de estos hechos ilícitos. Por lo que se refiere al bien jurídico a proteger dentro de los tipos penales que propusieron son: la privacidad y la integridad de la informática.

Se intereso a proteger las instituciones que integran el sistema financiero ya que han sido con mayor frecuencia las víctimas en la comisión de este tipo de conductas, protegiendo la información de su propiedad, agravando la penalidad aquellas conductas fueran cometidas por miembros de las instituciones que integran el sistema financiero.

Una forma también de gravar la conducta que vulnera la información almacenada en los sistemas informáticos consiste en que el sujeto activo acceda a los sistemas informáticos propiedad del Estado o al sistema financiero y aquél

[46] GOMEZ Sánchez Alejandro, "Nueva Legislación sobre delitos Informáticos", Revista Mexicana de Justicia, Nueva Época, No. 8, 1999, México, D.F. p. 159

tenga algún mecanismo de seguridad y sea vulnerada con el propósito de alterar o provocar la pérdida de la información.

Se transcribe los artículos adicionados al Código Penal Federal, para posteriormente analizar las conductas específicas que prohiben.

TÍTULO NOVENO

REVELACIÓN DE SECETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO I

REVELACIÓN DESECRETOS

ARTÍCULO 210. Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin causa justa, 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 sus servicios profesionales o técnicas o por funcionario o empleado público, o cuando el secreto revelado o público sea de carácter industrial.

ARTÍCULO 211 BIS. La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspención 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 público sea de carácter industrial.

CAPÍTULO II

ACCESO ILÍCTO 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 impondrá de seis meses a dos años de presión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos de 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 o 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 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 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 perdida 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 integren 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.

El Código Penal Federal, ya reformado, se formulo en su capítulo dos denominado acceso ilícito a sistemas y equipos de informática una serie de hipótesis normativas que describe conductas que están vinculadas a los sistemas de informática como instrumento o como fin delictivo, y como se dijo, hoy en día es un grave problema, ya que las leyes y los sistemas de procuración e impartición de justicia, así como el ordenamiento legal internacional, no se han adecuado a los cambios tecnológicos en forma coordinada.

Los artículos 211 bis 1 hasta 211 bis 7, describe situaciones jurídicas enfocándose únicamente a las conductas de "modificar", destruir", "provocar pérdida" así como "conocer" y "copiar", con la distinción de aquellos que acceden a equipos y sistemas de informática "sin autorización", es decir, intrusismo informático, con aquellos que teniendo la autorización, cometa alguna de las conductas de gran trascendencia con el desarrollo de la tecnología, en esta evolución acelerada refleja una gama de conductas teniendo como ejemplo: conociendo y copiando la información protegida, una vez que accede ilícitamente al sistema o equipo informático, el sujeto divulgue o comercialice dicha información; así como la transmisión telemática de información, en el cual se "intercepte" dicha información protegida, o el que diseñe un programa, códigos o instrucciones o comandos informáticos para vulnerar el funcionamiento del soporte lógico (software). Por tanto es menester tipificar conductas que alteren a la información como el soporte lógico, que estos dos bienes jurídicos (información y soporte lógico) deben ser de interés jurídico que el derecho necesariamente debe tutelar, con el fin de disponer y manejar con la seguridad jurídica que otorga la constitución.

El establecimiento de las acciones descritas en el código en comento, se enfocan únicamente a la protección de la información, es valido esta protección ya que el resultado de estas nuevas tecnologías, el bien jurídico a proteger es la misma información, sin embargo, no es el único bien a proteger que nace con la tecnología de comunicación informática, sino también un bien de la misma naturaleza que la información, es decir, un bien intangible que se le denomina soporte lógico, y que ambos son susceptibles de vulnararlo, y si éste se daña la información en sus diferentes formatos es imposible su control virtual. Dicho bien es el alma de un sistema o instrumento informático, el que realiza todas las funciones de naturaleza informática, y que es de gran utilidad e interés en las empresas, instituciones gubernamentales, universidades, etc., que utilizan ordenadores o sistemas de red local o Internet para almacenar o transmitir información de gran validez; ahora bien estor ordenadores son susceptibles de

ser vulnerados en sus funciones, es decir, en el soporte lógico, teniendo como consecuencia resultados irreparables, ocasionando la inhabilitación en el sistema. Por lo anterior es de gran importancia legislar y actualizar el ordenamiento jurídico a los tiempos que lo requieren.

En sus artículos se establece la conducta de "copiar", sin embrago el verbo "copiar" se define: "Reproducción exacta de un escrito impreso, obra, artista, etc.,"[47] en los sistemas informáticos la información esta representado por imágenes, sonidos, y texto, por lo tanto no se puede denominar "copiar" si el bien jurídico protegido es la información, estaría muy reducido y solo se adecuaría a una conducta ilícita tradicional como utilizando un bolígrafo y copiar un texto a un lugar perceptible por los sentidos, por lo tanto nosotros lo determinamos por "gravar" que se define como: "tr. e intr. Registrar imágenes, sonidos o información de manera que se pueda reproducir" [48], este verbo es mas acorde con la protección de la información por que se puede almacenar en un disckett , cdrw, disco duro o en cualquier instrumento de almacenamiento.

Otro factor importante es señalar, ¿qué se entiende por mecanismo de seguridad?, ya que la ley no lo define, dejando en estado de indefensión al agraviado así como al sujeto pasivo no cuente con mecanismo de seguridad en el sistema o equipo informático vulnerado, teniendo que hacer el juez complementar con información de especialistas en la materia.

Los actos que afectan a la información contenido en sistemas o equipos de informática que pertenezcan al estado se agravan la penalidad, y es mayor la sanción cuando estando autorizado "modifique", "dañe o provoque pérdida de información", que el que "accede" sin autorización; mientras que todo acto sin autorización que accede a instituciones que integra el sistema financiero protegido por algún mecanismo de seguridad se aplique la pena básica. Todo la regulación

[47] Diccionario de la Lengua Española, Larousse, Primera Edición, México, 1994. P. 176
[48] Ibidem p. 326

establecido en este capítulo del Código Penal Federal, tiene como contenido la protección de la información al servicio del estado e indirectamente al servicio de la sociedad.

Existiendo únicamente en materia penal las normas descritas, los juzgadores no tendrán otra alternativa que aplicar tipos penales que no se adecuan a los hechos ilícitos de naturaleza informática, ya que "...la falta de una adecuada tipicidad nos obliga a usar analogías que..., no se aplican en materia penal, por lo que se entiende que tales conductas, hasta ahora y sólo que ingresen a otros tipos de delitos, como el fraude, violación a derechos de autor o propiedad intelectual, o daños que pudan (sic) ser probados, serían perseguibles sólo civilmente...".[49] Reclamando daños y perjuicios ocasionados.

TÍTULO VIGÉSIMOSEXTO
DE LOS DELITOS EN MATERIA DE DERECHO DE AUTOR

ARTÍCULO 424 BIS. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa
Fracción I. ...
Fracción II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación

Al establecer este artículo la prohibición de crear un dispositivo electrónico de protección, no se está hablando de programa o instrumento electrónico que vulnere la protección de un sistema o equipo informático u electrónico para acceder y vulnerar la información contenida en ellos, sino la creación de un dispositivo, es decir esta ley sanciona al autor del que elabore dicho dispositivo, la

[49] BARRIO, Garrido, Gabriela. Internet y Derecho en México, Mac Graw – Hill, México, p.104

conducta de "crear", no de acceder o vulnerar sistemas o equipos informáticos, por el cual el bien jurídico en este caso es la información, sin embargo existe la real posibilidad de que dichos dispositivos no únicamente pueda perjudicar la información sino el mismo sistema en su función.

Al existir tal delito descrito en el precepto transcrito, debe existir el lucro exigido por el tipo penal, pero generalmente no es así, ya que la forma de crear un dispositivo electrónico dañino hoy en día, no es difícil de diseñarlo, por que en las redes de información como el Internet existe una serie de formas sencillas para construir un dispositivo ilícito, sin necesidad de comprarlas o venderlas para tener un lucro. En síntesis es suprimir tal palabra, para equiparar mas conductas que en el mundo fáctico suceden y penalizarlos.

Por otro lado, ya los dispositivos dañinos creados, como pueden ser: Virus, Bombas lógicas, Spam, Sniffer, etc., son generalmente elaborados sin el fin de lucro, sino únicamente para acceder a sistemas informáticos con el objeto de conocer información confidencial, hasta vulnerar en su totalidad el soporte lógico así como la información contenida en él.

2.3 . NUEVO CÓDIGO PENAL DEL DISTRITO FEDERAL

CAPÍTULO III
FRAUDE
ARTÍCULO 231...

> **FRACCIÓN XIV.** Para obtener algún beneficio para así o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución; o

Es el único artículo del Nuevo Código Penal del Distrito Federal que establece y regula la conducta que se realiza a través de medios informáticos, en éste artículo describe que el fin de la conducta es el manejo indebido del sistema para un beneficio para así o un tercero, cabe resaltar que este artículo por un lado la conducta se realiza por cualquier medio y por el otro no existe un a prohibición en su acceso, la primera es adecuada, sin embrago en segundo sería conveniente tal prohibición en el acceso agravándolo en la penalidad.

Contempla tres conductas los cuales son "accese, "entre" o se "introduzca", dichas conductas son la forma de intervención a los sistemas o programas de informática del sistema financiero, los cuales tienen como objetivo acceder a los mismos para llevar acabo el manejo ilícito para un beneficio ya sea personal o no, a través de transacciones, operaciones o movimientos de dinero o valores, tal manejo únicamente podrá ser realizados al entrar al sistema informático, por lo que nuevamente debe resaltar la importancia de sancionar a aquellos que acceden ilícitamente como a aquellos que teniendo la autorización de acceder realizan tales operaciones, con diferente sanción; sin embargo sería contemplar también que se adicione, en este código penal, las conductas que vulneren su soporte lógico en las instituciones financieros, así como las instituciones del gobierno, así como diversas conductas que se relaciona a las nuevas tecnologías de información.

Algunos tratadistas manifiestan que el tipo penal en comento debería ser tipificado pero en el ámbito federal, argumentando que los delitos financieros tienen tal carácter y por lo tanto el código penal del Distrito Federal no debería tipificarlo ya que está reglamentando conductas que debería sancionar el Código Penal federal.

2.4. OTRAS LEYES EN RELACIÓN CON LOS DELITOS INFORMÁTICOS

CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

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

Titulo Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

> Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:
>
> Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o
>
> Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
>
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos dias multa.

El Código Penal de Sinaloa, es la única ley sustantiva a escala nacional que tipifica el delito informático, el cual lo define, así como describe diversas conductas, tales como el intrusismo informático, es decir, el acceso ilícito a un

sistema informático con el objetivo de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar o bien, obtener dinero informático.

Cabe destacar que en este Código Penal contempla la conducta del que "dañe", "destruya" o "altere" un soporte lógico o programa de computación, es decir, conductas que en este sencillo trabajo de investigación trate de impulsarlas, ya que su realización de tales actos son relevantes ante la innovación de formas de cometer algún ilícito contra el mundo informático a través de Internet.

Ley de derecho de autor

> **Artículo 101.** Se entiende por programa de computación 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.
>
> **Artículo 102.** Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.
>
> **Artículo 106.** El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;
II. La traducción, la adopción, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el de ensamblaje.

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

2.5. LEGISLACIONES COMPARADAS

ALEMANIA.

Se establece en tipos específicos, en los artículos 303 a) y 303 b), (regula exclusivamente el sabotaje informático), del Código Penal Alemán (StGB)

Párrafo 303 a) Destrucción de Datos. "Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos (de los previstos en el párrafo 202 a), par. 2°) será castigado con pena privativa de libertad de hasta dos años con pena de multa."
Párrafo 303 b).- Sabotaje informático. "Quien destruya una elaboración de datos en especial significación para una fábrica ajena, una empresa ajena o una administración pública, a través de: la comisión del tipo previsto en el párrafo 303 a), PAR. 2°; o por la destrucción, deterioro, inutilización o alteración de un sistema de elaboración de datos o de los portadores de los datos, será castigado con pena privativa de libertad hasta de cinco años o con pena de multa.

FRANCIA

Artículo 463-3 Code Penal. Sabotaje Informático.

"Quien intencionalmente y con menosprecio de los derechos de los demás, impida o falsee el funcionamiento de un sistema de tratamiento automático de datos será castigado con prisión de tres meses a tres años y con multa de 10, 000 a 100,000 francos o con una de las dos penas"

ESPAÑA.

En el caso de España regula el sabotaje informático, sin denominarlo como tal en su artículo 264.2 del código penal, adicionado en la reforma de 1995.

Artículo 264. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticinco meses el que causare daños expresados en el Artículo anterior, si concurrieren algunos de los supuestos siguientes:

Fracción 2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro medio dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Hay que señalar las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:
VII) 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.

CHILE

Ley No.:19223

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectare los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 3º: "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

COSTA RICA

COSTA RICA: LEY No. 8148

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

Decreta:

ADICIÓN DE LOS ARTÍCULOS 196 BIS, 217 BIS Y 229 BIS AL CÓDIGO PENAL LEY Nº 4573, PARA REPRIMIR Y SANCIONAR LOS DELITOS INFORMÁTICOS

"Artículo 229 bis.- Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

ITALIA

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

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

GRAN BRETAÑA

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

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

HOLANDA.

El 1° de Marzo de 1993 entró en vigencia la **Ley de Delitos Informático**

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

3. CAPÍTULO 3.

3. CAPÍTULO. 3.

ELEMENTOS DEL DELITO DE LA CONDUCTA ILÍCITA EN CONTRA DEL FUNCIONAMIENTO EN LOS SISTEMAS DE INFORMÁTICA

3. CONDUCTA

Antes de desarrollar y analizar todos y cada uno de los elementos del delito, es preciso desarrollar una hipótesis, el cual se propone para estudiarlo en este capítulo y así mismo para impulsar la tipificación en esta materia en Código Penal Federal:

> "El que sin autorización y sin derecho altere, introduzca, programe, provoque la transmisión o ejecución de programas con el fin de modificar, destruir, o cause negación de servicio, por cualquier medio en contra de su función de los programas o sistemas de naturaleza informática, se le impondrá de seis meses a dos años de prisión.
>
> Cuando es en contra de sistemas financieros de imposible reparación se le impondrá de dos a cinco años de prisión.
>
> Cuando es en contra de sistemas del estado federal y de imposible reparación se le impondrá de tres a siete años de prisión"

El derecho no pretende otra cosa que ser un orden regulador de conducta coercitiva, de ahí el principio de *"nullum crimen sine conducta"* como elemento de garantía jurídica, es decir, no hay delito sin conducta, y como tal se entiende la

actividad consciente del fin, y según Welzel citado por Zafaronni, la acción humana se desarrolla en dos fases, una interna y la otra externa:

Interno: El aspecto interno de la conducta pertenece la proposición de un fin(1) y la selección de medios de los medios para su obtención (2), siempre que nos proponemos un fin retrocedemos mentalmente desde la representación del fin para seleccionar los medios con que poner en marcha la casualidad para que se produzca el resultado querido. En esa selección no podemos que representarnos también los resultados concomitantes.

Externo: Terminado esta etapa, pasamos a la exteriorización de la conducta, consiste en la puesta en marcha de la casualidad en dirección a la producción del resultado. [50]

Según la hipótesis expresada resalta las conductas: Alterar, Modificar, Destruir, Negación de Servicios". Según el Diccionario de la Lengua Española se definen:

"Alterar.- tr. Cambiar la esencia o forma de algo.
Destruir.- Reducir a pedazos o cenizas algo material v. Tr. Ocasionarle un grave Daño. Utc. Prnl.II2 deshacer, inutilizar algo no material.
Inhabilitar.- Imposibilitar para una cosa." [51]

Ahora bien, todos y cada una de las conductas citadas permiten la vulneración contra los soporte lógicos, ya que la conducta alterar como su definición lo describe permite cambiar la esencia o forma de algo, ahora si lo equiparamos hacia el funcionamiento de un programa tendría como efecto que el funcionamiento del mismo actuaría con un fin no establecido ocasionando pérdidas incalculables en la información establecida en el programa o en el programa mismo, el ejemplo seria que un virus que alteraría el funcionamiento de

[50] Cfr. ZAFFARONI, Eugenio Raúl, "Manual de Derecho Penal", parte general. Segunda edición, México, Cardenas, 1988, p.362
[51] Diccionario de la Lengua Española, "Real Academia Española", Vigésima segunda edición, 2001

un programa del estado financiero, las operaciones realzadas obtendrían resultados irreparables para el estado o a la sociedad, como puede ser pérdidas de información o el manejo del mismo.

La segunda conducta señalada que es modificar se define como limitar, determinar o restringir las cosas a un cierto estado o calidad en que se singularicen y distingan unas de otras, esta conducta se refiere a limitar o restringir el buen funcionamiento de un programa informático, no cambiarlo en su totalidad sino en algunas de sus finalidades, esto tendría como efecto que las operaciones realizadas en las dependencias tengan resultados no deseados ocasionando daños y perjuicios irreparables; y es que la modificación del un programa no destruye la información o se pierde sino que se encuentra almacenado en el disco duro pero el programa no funciona correctamente obstaculizando el servicio y la utilidad y una serie de intereses del estado.

La conducta de destruir consiste en reducir a pedazos o cenizas algo material, esta definición existe una gran diferencia con los soportes lógicos o sistemas informáticos por que al ser vulnerado no se destruye físicamente sino que el soporte lógico o el contenido del disco duro se destruye quedando en pedazos o en cenizas en forma figurada, imposibilitando el funcionamiento, teniendo generalmente como resultado la perdida total de la información y del soporte lógico ocasionando daños y perjuicios irreparables en las operaciones de la dependencia afectada, es el caso de un virus transmitidos por Internet a través de un correcto electrónico que se activa al abrirlo distribuyéndose en el disco duro, así como destruyendo los archivos de arranque y de sistema dando como resultado el irreparable y valioso información o servicios de gran interés.

Otra conducta que puede vulnerar es la de inhabilitar que consiste en "imposibilitar para una cosa", aquí la información no se destruye, no se modifica, no se altera, sino que el programa o el sistema informáticos sufre un estancamiento en sus funciones, una diferencia entre estas dos, es que el

programa es un elemento particular de un sistema informático mientras el sistema informático es un todo, ahora bien, dicha conducta crea ciertas finalidades en el diseño del dispositivo lógico que lo aplica para lesionar un sistema lógico dependiendo el querer del sujeto, en la doctrina internacional lo denominan "Denegación de Servicios".

Toda conducta que vulnere un soporte lógico o sistema informático estriba en la configuración del dispositivo lógico (programa dañino) para poder alterar, modificar, destruir, denegar servicios, es decir, la conducta del sujeto activo consiste en manipular el dispositivo dependiendo a sus finalidades deseadas, el programa únicamente se desarrollara conforme a lo establecido por el sujeto que puede ir más allá dependiendo lo configurado pero generalmente un dispositivo enviado a través de Internet no hay control en la distribución y daños. Por ejemplo un Sistem Crash con un Time Bombas distribuido por Internet es que el primero es un virus que produce un gran daño no solo al programa sino todo al sistema informático y que puede reproducirse por toda la red de Internet y que por lo general no tiene destinatario, mientras que el segundo por lo general tiene destinatario ya que una vez entrado al sistema seleccionado no lo daña sino que debe de realizarse una operación informática para su activación que puede ser abriendo un programa, un correo electrónico o hacer cualquier operación y que una vez activado este estalla y puede destruir, modificar o inhabilitar .todo el programa o sistema informático.

Actualizando la conducta que se despliega hacia un mecanismo informático cualquiera señalado, se cumple las dos fases del acto, el aspecto interno y externo, es decir, la conducta se va a desprender valorando el plan seleccionado en la mente, para así ejecutar o llevar a cabo en el mundo exterior, en este caso ante un bien tangible pero directamente ante un bien intangible.

Debe de quedar claro que la conducta desplegada por el sujeto activo debe recaer únicamente sobre los elementos lógicos para configurar el hecho ilícito que

se analiza, por lo que sí se "daña" el soporte físico (hardware) se estaría hablando de un daño patrimonial, esto es, se configuraría un delito de daño por el quebranto material, encontrándose éste tipificado en el Código Penal Federal, Orts nos dice en ese sentido "La aplicación de esta infracción, tradicionalmente reservada a cosas corpóreas, para la tutela de otros bienes de carácter inmaterial no es sino la consecuencia de la propia evolución social, y de la aparición de determinados valores inmateriales, susceptibles de destrucción o inutilización, a los que se atribuye igual o mayor valor que los bienes tangibles. Precisamente, esta especificidad del objeto de tutela ha llevado al legislador a regular los llamados <<daños informáticos>> en un apartado separado de la tradicional figura de daños".[52]

3.1. RESULTADO

El resultado de la acción, es la producción o consecuencia de la realización de la conducta y varia dependiendo la representación y finalidad del sujeto activo así como el curso causal de la conducta, dicho resultado y el nexo causal ya no pertenece a la conducta sin embargo lo acompaña necesariamente; sin embargo existe una relación extrema entre la conducta y el curso causal, la primera con una dirección vidente establecida en el contenido de la voluntad, representada en la mente, posteriormente el curso causal de la dirección en la conducta que puede ser alterada, sin embargo tal alteración o no, produce una alteración al mundo fáctico, ocasionado un resultado ilícitamente relevante, enfocándose al contenido de la conducta mas no el resultado, pero este sería la base de las circunstancias en el momento de la ejecución del a conducta.

Y según la hipótesis descrita, el resultado es la vulneración en los soportes lógicos es decir cuando el soporte señalado sea ineficaz en sus funciones

[52] ORTS, Berenguer Enrique y Roig Torrez Margarita, Delitos Informáticos y Delitos Comunes cometidos a través de la Informática, Tirant Lo Blanch 2001, 195 pp.

ocasionando un resultado, ya representado por la mente del sujeto activo, y que a través del curso causal llevo a cabo tal conducta, por lo que los legisladores deberán de enfocarse al daño, es decir, el resultado que provocaría una conducta como tal, ya que ésta produjo una alteración dentro de un sistema tangible, es decir, en un bien inmaterial en que dichos bienes son valorados conforme a su utilidad y función.

Cabe considerar que un resultado a base de un virus informático o cualquier otro instrumento lógico dañino, puede ser lesionado una serie de bienes, es cuando su resultado se dificulta, como consecuencia de un único comportamiento, los resultados lesivos se van reproduciendo por si mismo y afectan a múltiples programas, en muchas ocasiones de forma indiscriminada e incalculable, incluso para el propio sujeto. Aun cuando para que una conducta pueda calificarse como dolosa no se exija que el sujeto conozca y quiera el resultado lesivo, en todo caso el sujeto ha de conocer el efectivo y exacto peligro que esta supone.

3.2. NEXO DE CAUSALIDAD

El nexo de causalidad es un proceso, una cadena de causas y efectos. "Toda condición que puede ser mentalmente suprimida sin que con ello desaparezca el efecto, es causa" (teoría sine qua non).

La conducta tiene como primer elemento la voluntad, que para el sistema finalista, debe ser vidente, es decir un sentido de dirección, un actuar consciente hacia un fin determinado. Solo es relevante la causalidad material dirigida por la voluntad de acuerdo a un fin" señala Enrique Bacigalupo citado por Zafaronni

El nexo de causalidad se da a base de un acción humana produciendo un resultado, es decir, entre la conducta humana y el resultado existe un nexo de causalidad, y este elemento es un proceso, una cadena de causa y efectos.

Al manipular un mecanismo informático, el sujeto preveé el curso de su proceder, tiene la previsión de su conducta, su dirección y los posibles efectos de su actuar, una vez ejecutado su conducta en el mecanismo informático, el curso de acto procede conforme a su finalidad propuesto. Ahora bien generalmente en estos delitos su proceder está mas determinado, ya que la causalidad toma una dirección establecida y programada, sin embargo suele pasar excepciones delimitadas, pero estas se encuentran dentro de la conducta, porque aún puede que exista un error producido ya por algo externo independientemente de la conducta, tenía la previsión y finalidad de su objetivo. Por ejemplo: la persona que introduce un virus en la red de redes y lo trasmite, encontrándose el sujeto en Japón, vulnerando un sistema de un organismo de Estado, su conducta es introducir ilícitamente y sin autorización al sistema dicho virus, pero éste esta programada su actuar, una vez ejecutado o activada el virus por una causa externa, que no es necesario, el nexo causal esta ya previamente determinado su proceder, y muy difícil puede ser alterado ese proceder sino existe una alteración al mismo o el medio donde viaja el virus, para que el virus llega a su destino programado y vulnere el sistema informático como su objetivo principal.

Sin embargo, una vez ejecutado la conducta consistente en introducir el virus en la red de Internet, "suele existir para su consumación "un tiempo", para que el virus pueda lesionar o poner en peligro un bien, es decir, puede existir un lapso de tiempo entre una conducta, en sí misma sin eficacia lesiva, y otra, que provoque directamente los resultados lesivos, pero únicamente, en cuanto existía esa conducta previa. En lo supuestos en los que, para que se inicie la destrucción de los datos o programas, ha de pasar únicamente un lapso de tiempo se suscitan ambos problemas: inicio de la ejecución y momento de la consumación"[53]

Otro aspecto de gran interés respecto a los efectos de la conducta contra los bienes intangibles es que puede concretarse un resultado plural, es decir, un

[53] Cfr, MIR. Puig Santiago, Op. Cit, p.150

concurso ideal, en donde de una conducta suele producir varios delitos, esto por que los resultados lesivos se van reproduciendo, un ejemplo es un virus que se autoreproduce afectando múltiples programas, ordenadores, información, la misma red, y que en muchas ocasiones es de forma indiscriminada e incalculable, incluso para el propio autor material, eh aquí la relevancia del dolo, determinándolo como un dolo eventual, por su no-exigibilidad que conozca y quiera el resultado lesivo (autoreproduciéndose el virus de forma inimaginable), sino en todo caso el sujeto ha de conocer el efectivo y exacto peligro que éste supone.

3.3. SUJETO ACTIVO.

Se define como sujeto activo, el que realiza todo o una parte de la acción descrita por el tipo penal.

El acto y la omisión deben corresponder al hombre, por que únicamente es posible que éste realizar las situaciones descritas en los preceptos penales, es decir, es el único capaz de voluntariedad.

En el precepto que se propone, se señala que el sujeto activo puede ser cualquier persona, todos son potenciales a realizar las situaciones establecidas en tal hipótesis, sin embargo generalmente los sujetos que realizan tales acciones, tienen un conocimiento especial, una técnica para manipular un instrumento informático y ejecutar conductas que dañen al soporte lógico, tienen un perfil.

El perfil del sujeto activo se caracteriza de que conoce el lenguaje informática, por tal motivo tiene la técnica para vulnerar cualquier tipo de sistema informático, sin embargo no es elemento necesario contar con tal conocimiento para ocasionar un ineficaz funcionamiento de un sistema, por que por ejemplo: el que obtiene un virus a través de Internet y lo transmite en un sistema informático, tal persona no

tiene el conocimiento especial pero lo puede obtener el dispositivo informático para dañar. Por tal motivo cualquier sujeto es potencial para cometer este tipo de conductas como total o parcialmente.

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

Estos son algunos de los principales sujetos de los delitos informáticos:

Hacker.- El término "hacker" deriva de la palabra inglesa "hack" que significa hacha.

Es quién intercepta dolosamente un sistema informático para destruir la información que se encuentra almacenada en las computadoras pertenecientes a entidades privadas o públicas.

Se le conoce como "piratas informáticos", personas que ingresan sin autorización a una computadora y exploran su interior.

Cracker.- Es el tipo hacker que no ingresa al sistema por curiosidad o por que le representa un reto para entender el funcionamiento de cualquier sistema. El cracker conscientemente ingresa a un sistema con la finalidad de destruir información.

3.4. SUJETO PASIVO

Es el ente sobre el cual recae la conducta realizada a través de un acción o omisión que realiza el sujeto activo.

Las víctimas pueden ser tanto personas físicas o morales, que utilizan medios informáticos, sistemas de computo, o generalmente *sui generis* medios electrónicos.

La hipótesis describe que no requiere calidad específica alguna para el sujeto pasivo, ni forma especial de intervención.

Cabe destacar que el delito de vulneración ilícita en el funcionamiento en los sistemas de informática, el sujeto pasivo necesariamente deber ser el Estado, por tal motivo dichas sujetos pasivos- físicas o morales- deben pertenecer dentro de la jurisdicción federal.

3.5. ELEMENTO MATERIAL

Al realizar una conducta existe una alteración, mutación en el mundo exterior, ya que antes de realizar un acto las cosas se encontraban en un estado deferente y después de éste se da un cambio, una alteración, una transformación, a esa mutación externa suele llamarse resultado, a esa consecuencia de la conducta ilícita humana se le llama objeto material.

Tal resultado puede ser cualquiera con tal de que se afecte un bien. En el caso de las conductas que se involucra con los instrumentos informáticos, suele se el elemento material el computador, el sistema u ordenador informático.

3.6. BIEN JURÍDICAMENTE PROTEGIDO

Por lo que respecta al bien a proteger jurídicamente en las conductas iícitas en contra de instrumentos de informática, encontramos que la información seria el bien a proteger, dicho bien es el que protege el Código Penal Federal; sin

embargo para nosotros y de acuerdo a la hipótesis establecida sería *el patrimonio federal.*

Para entender lo anterior, analizaremos lo que es el bien jurídico protegido: y según Zafaronni, el bien jurídico tutelado "...es la relación de disponibilidad de un individuo con un objeto, protegida por el estado, que revela su interés mediante la justificación penal de conductas que le afectan...".[54]

Por que el bien no es propiamente el honor, sino el derecho a disponer del propio honor, como el bien jurídico no es la propiedad, sino el derecho a disponer de nuestro patrimonio.

El "ente" que el orden jurídico tutela contra ciertas conductas que le afectan no es la "cosa en sí misma" sino la "relación de disponibilidad" del titular con la cosa. Dicho en otras palabras más simples: los bienes jurídicos son los derechos que tenemos a disponer de ciertos objetos.

Los bienes tutelados por los artículos 211 bis 1 al 211 bis 7, es la información que puede ser vulneradas en base en las conductas que describe el tipo penal.

Pero el bien jurídico que protege el tipo penal, que es la disponibilidad de la información, dejando al arbitrio el legislador el bien que permite almacenar la información que es de igual vulnerable, estamos hablando del soporte lógico.

Por lo que se refiere al hecho ilícito de Vulneración en contra del Funcionamiento del Soporte Lógico, *es el patrimonio del estado*, ya que si al desglosarse este bien a proteger, es una "función" que se define como "la capacidad de acción o acción de ser apropiada a su condición natural (para lo que existe) o al destino dado por el hombre (para lo que se usa).

[54] ZAFFARONI, Eugenio Raúl, Op. Cit. P. 410

La finalidad de la conducta para adecuarse al tipo que el legislador debe contemplar para su creación, es que tenga una dirección, un sentido vidente para vulnerar el funcionamiento en sí, al "ente" y no a la información como tal, he aquí donde radica la diferencia entre estos dos aspectos, y que diversos criterios en la doctrina se apegan al último (el criterio de Zafaronni).

Ahora bien, existe un criterio contrario a lo manifestado, al definir el concepto de "cosa", el cual se describe: "Todo lo que tiene entidad, ya sea corporal o espiritual, natural o artificial, real o abstracta"[55]; es posible equiparar el daño al soporte lógico en los delitos patrimoniales, ya que es un bien intangible y de acuerdo a la definición descrita concuerda con el soporte lógico concretándose que éste tiene una función y utilidad para una protección penal. Al respecto nos dice Corcoy Bidasolo: "Los daños se conciben como destrucción, inutilización o deterioro se puede entender como destrucción de la sustancia de la cosa...las propiedades esenciales de una cosa pueden ser comprendidas bajo el aspecto de su funcionalidad, lo que supone el paso de un concepto naturalístico de la sustancia a un concepto normativo...daño será, por tanto una cosa que tenga un interés para la propia existencia de la cosa. En consecuencia, la transformación de la sustancia de la cosa será daño, habrá daño si la cosa no funciona correctamente o si se disminuyen sus posibilidades de aplicación o de eficacia."[56]

También nos dice Enrique Orts con relación a estos delitos que el bien jurídico es el Patrimonio, manifestando "...si bien en este delito la acción del sujeto activo no lleva aparejada la incorporación de la cosa a su patrimonio o al de un tercero, ni se requiere siquiera que de su comisión se siga alguna suerte sobre el menoscabo económico. Los daños reposan exclusivamente sobre el menoscabo causado en una cosa ajena...".[57]

---

[55] Gran Diccionario Enciclopédico Asuri. Dir. Lorenzo Portillo Sisiniega, v.4, España, 1989, 1497 pp.
[56] MIR, Puig Santiago, Op. Cit p.170, 171

[57] ORTS, Berenguer Enrique y Roig Torroz Margarita, "Delitos Informáticos... Op. Cit p.78

Nosotros nos apegamos al primer criterio ya que debe existir su capitulo especial dentro del Código Penal Federal normas que engloben este tipo de hechos ilícitos y otros actos de trascendencia informática, pero también que el bien jurídico a tutelar deber ser a la naturaleza del objeto material que contrae a los datos, programas, documentos electrónicos, redes o sistemas informáticos, es decir, elementos lógicos, teniendo estos una función y una utilidad, no afectando a la información sino al patrimonio en sí que debe de existir y garantizar a toda persona física o moral que actúe dentro de un mundo virtual global.

Existe un criterio que pretendemos manejar que consiste en que efectivamente el patrimonio es el bien jurídico tutelado vista a todas luces, sin embrago es menester señalar que puede surgir un aspecto diferente al valorar el resultado ilícito obteniendo un bien jurídico sustentable respecto a la utilidad del soporte lógico y del sistema informático surgiendo un nuevo bien a proteger jurídicamente que es *la seguridad en la función en los sistemas de informática,* por que tiene una función dentro del sistema y sin tener esa utilidad ocasiona perjuicios y daños que el derecho en esta de la informática es necesario tipificar.

3.7. MEDIOS COMISIVOS

Los medios comisivos para cometer este tipo de vulneración en contra del soporte lógico suelen ser en forma física y forma lógica, la primera suele ser un instrumento informático y redes, como por ejemplo un computadora portátil o personal, una agenda electrónica, y hasta ahorita ya se puede vulnerar hasta con celulares conectados al Internet, también las redes son medios que utilizan como medio de transporte para acceder a un sistema y vulnerar el soporte lógico.

Por otro lado en el aspecto lógico suele utilizar los virus, bombas lógicas, crash programs, cáncer routine, caballo de troya, sistem crash, etc.

Virus.- Son programas capaces de multiplicarse y contaminar los otros programas que se encuentran en el disco duro del ordenador y/o los programas y datos de otras empresas o sucursales en el transcurso de una conexión de estas.

Los principales síntomas del virus son:

- Una mayor lentitud en la ejecución de los programas.
- El bloqueo del funcionamiento de la pantalla o la operación de ésta de signos extraños.
- La desaparición de información que se encontraba en el disco duro.

Crash Program.- Programas de destrucción progresiva. Con estos programas se pueden borrar un gran número de datos en un corto periodo de tiempo. Estos programas pueden ser de utilidades, escribirse por sí mismos o actuar como (caballo de Troya), creando rutinas dentro del programa de aplicación o dentro del sistema operativo.

Time Bombas.- Bombas lógicas de actuación retardada. La destrucción de los ficheros de produce, tras un lapso de tiempo, en virtud de indicaciones precisas como la presencia o ausencia de un dato, de una hora, de un código, de un nombre, etc.

Cáncer rutine.- Esta modalidad de sabotaje consiste en introducir una serie de ordenes que provocan su propia reproducción en otros programas, arbitrariamente escogidos. Estas rutinas pueden ser destacadas y sacadas por el usuario, pero si queda una de estas rutinas el (cáncer) puede continuar reproduciéndose y extendiéndose.

Sistem Crash.- Este método de reciente creación, es el más contundente, básicamente en la introducción de una orden que provoca el bloqueo del sistema

informático, echando abajo el sistema operativo y los programas, en una palabra todo el contenido del disco duro del ordenador.

Por tal motivo, los instrumentos utilizables para cometer la ineficaz vulneración en los sistemas informáticos, son a través de materiales físicos o lógicos como se explico, por lo que la naturaleza de del bien jurídicamente a proteger es material abstracto los medios utilizables generalmente son lógicos.

3.8. ELEMENTOS NORMATIVOS.

Los elementos normativos que se contemplan en la hipótesis descrita y que es:

> "El que sin autorización y sin derecho altere, introduzca, programe, provoque la transmisión o ejecución de programas con el fin de modificar, destruir, o cause negación de servicio, por cualquier medio en contra de su función de los programas o sistemas de naturaleza informática, se le impondrá de seis meses a dos años de prisión.

El elemento normativo es "sin autorización", pero para señalar el elemento normativo en la citada hipótesis, es preciso señalar que se entiende por elemento normativo y que por el mismo se define como la valoración ética o jurídica, que el juez debe realizar cuando los tipos penales no contengan cierta precisión en el contenido del tipo penal.

Referente a la hipótesis que se propone para ser un tipo penal, se señala que debe ser "sin autorización", este concepto se requiere de una valoración jurídica que el juzgador debe realizar dependiendo a las circunstancias del hecho.

Cabe destacar que un derecho penal que abusan de los elementos normativos, se lesiona la seguridad jurídica. Los elementos normativos pertenecen al tipo penal, ya que se caracteriza por ser uno de los elementos que permite adecuar de manera eficaz a la conducta en sus circunstancias de facto, para dar una seguridad jurídica.

3.9. ELEMENTO SUBJETIVO

Conforme a la teoría clásica, el elemento subjetivo es la relación entre el aspecto psicológico y el resultado, y se encontraba dentro de la esfera de la culpabilidad.

Según la teoría teleológica o finalista, el elemento subjetivo se contemplaría dentro del tipo y no en la culpabilidad, ya que sería erróneo si un sujeto al delinquir se estudiase para acreditar el delito los primeros dos elementos del mismo – tipicidad y antijuricidad - para después analizar si el sujeto quiso o no la realización del hecho prohibitivo, es decir conocer el contenido de la voluntad, por lo que se traslado el elemento subjetivo al tipo penal, desapareciendo la culpabilidad subjetiva quedando esta como una valoración únicamente normativa, creando en el tipo penal objetivo y subjetivo.

3.9.1 DOLO

El dolo es el elemento nuclear y principalísimo del tipo subjetivo y frecuentemente, el único componente del tipo subjetivo, (en el caso de que el tipo no requiere otros).[58]

En consecuencia, "...el dolo es el querer realizar los elementos objetivos del tipo...".[59]

[58] Cfr. ZAFFARONI, Eugenio Raúl, Op. Cit. 428

[59] DÍAZ Aranda Enrique, "DOLO Causalismo-Finalismo-funcionalismo y la reforma penal en México", Editorial Porrúa, Tercera Edición, México 2001, p- 124

Como se sabe el Dolo se compone de dos elementos, El cognocitivo y volitivo, la primera se conforma por un conocimiento efectivo, mientras la segunda en una voluntad de querer realizar.

En la realización de los delitos relacionados con la informática, el sujeto activo previamente conoce subjetivamente el andar de su conducta, y sus posibles consecuencias concomitantes, posicionándose en el mundo fáctico que su actuar consiste en conocer ciertas técnicas necesarias en materia de informática para manipular instrumentos de la misma naturaleza, ocasionando dentro del nexo de causalidad de su acto querido un resultado vulnerable en el funcionamiento de un sistema, ocasionando como efecto concomitante la pérdida, la alteración o destrucción de la información contenida en el software.

Ampliando lo anterior, el dolo dentro de este tipo de delito que se estudia, se compone de un conocimiento eficaz y actualizable, dicho conocimiento no debe basarse en solo una posibilidad, que no es aún conocimiento, en la doctrina este conocimiento se le denomina conocimiento potencial, pero en el dolo requiere siempre un conocimiento efectivo y no un conocimiento potencial, a modo de ejemplo: una persona que quiere ingresar un virus dañino para vulnerar el funcionamiento de un sistema informático, no se integra con la posibilidad de conocer de que el virus es dañino al momento de ingresarlo al sistema, sino debe tener un conocimiento de que el virus que trata de ingresar se trata de un programa dañino al sistema, es decir, un conocimiento efectivo, sin ese conocimiento efectivo la voluntad del actor no puede tener el fin de vulnerar en el funcionamiento, y por ende, no puede ser una voluntad delictiva. Citando nuevamente a Zafaronni, el conocimiento eficaz puede ser actual o actualizable. "...es conocimiento actual el que tenemos acerca de un objeto, cuando focalizamos sobre él nuestra actividad consciente... y actualizable cuando se recuerda y atrae el objeto que anteriormente observo." [60]

[60] ZAFFARONI, Eugenio Raúl, Op.Cit. p.430

En síntesis el dolo es el querer la realización del tipo objetivo, sin embargo el querer implica un conocimiento de los elementos objetivos y el conocimiento de la antijuricidad, pero éste último no sería un conocimiento efectivo, sino potencial, a modo de ejemplo: un sujeto que accede a un sistema informático con la finalidad de programar un soporte lógico para modificar su funcionamiento, conoce su trascendencia de su acto ilícito doloso y su posible contradicción con el derecho; como a aquél que conociendo su actuar ilícita no tiene interés de averiguar si actúa o no antijurídicamente, ambos no desaparece el dolo.

En el aspecto conativo del Dolo, el querer realizar un resultado ilícito sea como fin directamente propuesto o como uno de los medios para obtener ese fin, en el primero se representa a un instrumento a dañar en forma directa (soporte lógico), mientras que la segunda será un objeto necesariamente a dañar para realizar su objetivo directo (información contenida en el soporte lógico) que se le denomina dolo indirecto, o dolo eventual que una vez introducido un virus se reproduzca en la red, ya una vez aceptado las posibles efectos del introducción del virus en el soporte lógico y aún así lo acepta tales efectos.

3.9.2 ELEMENTOS SUBJETIVOS DISTINTOS AL DOLO

Zafaronni lo define como "...particulares direcciones de la voluntad que varı más allá del mero querer la realización del tipo objetivo; otros sin particulares disposiciones internas del sujeto activo...".[61]

Se caracterizan por una particularidad suposición del ánimo del actor, consideramos que hay tipos que contienen elementos subjetivos distintos del dolo, que pueden considerarse la tendencia interna sobrante o trascendente y otros de tendencia interna peculiar.

[61] ibidem p. 447

Aquél sujeto que se propone dañar un sistema informático indeterminado a través de un virus, introduciéndolo en el Internet, con una tendencia interna de fastidiar, de que su virus tenga fama dentro de los usuarios del Internet, de que su capacidad intelectual rebase a lo normal, su propósito interno se halla más allá del puro resultado o producción de la objetividad típica.

Mientras en los tipos de tendencia peculiar, son los "llamados momentos especiales del ánimo" que suele consistir en tomar una conducta dependiendo las circunstancias de tiempo, modo y ocasión y lugar, ocasionando un impulso interno por las facilidades para cometer el hecho ilícito a modo de ejemplo común para representar tal elemento subjetivo es aquél que aprovechando la oportunidad de poder vulnerar un ordenador de una universidad que se encuentra débil en su protección, y que el actor obtiene la contraseña para acceder sin ningún problema, bloqueando su funcionamiento y así no permitir que la universidad comporta información de investigación, ocasionando perjuicios a una cierta población que tiene interés el sujeto activo.

3.10. *ITER CRIMINIS*

"Suele denominarse como el camino del delito, por el cual se desarrolla la esfera interna y externa de la ejecución de la conducta, he aquí la delimitación de una punibilidad a través de la tentativa, que consiste en una acción objetiva y subjetiva en función de un dispositivo amplificador de la tipicidad que permite captar la acción de su dinámica desde el comienzo de su ejercicio y hasta que se completa la tipicidad del delito...".[62], es decir, "...no se trata de un tipo con un aspecto subjetivo completo y su aspecto incompleto por que ambas están por lo general incompletas...".[63] ya que el aspecto subjetivo no se concreta al no ligarse con el

[62] ZAFFARONI, Eugenio Raúl, et al, "Derecho Penal", parte general. Porrúa, México 2001, P. 775
[63] idem

aspecto objetivo, ya que la planeación subjetiva no es tentativa ante un bien jurídico tutelado que puede ser lesionado o estar en peligro.

Las etapas del Inter-criminis en donde la decisión como producto de la imaginación del autor hasta el agotamiento de la ejecución del delito, tiene lugar un proceso temporal suele consistir en una dinámica y cronológico del delito: "concepción, decisión, preparación, comienzo del ejecución, culminación de la acción típica, acontecer del resultado típico y agotamiento del hecho.

En las etapas descritas que se encuentra la limitación prohibitiva ante una tipicidad penal, llegando a esta limitación una tentativa que permite conocer el contenido de una voluntad anticipada que detiene el poder punitivo para no exceder en su fin, que éste tiene como visión conocer el camino del peligro de lesión y alcanzar hasta el momento anterior a la consumación. El poder punitivo debe limitarse a aquellas conductas ante una lesión o peligro real, ante la aproximación de la conducta con el resultado en sus dos aspectos (lesión o de peligro) penalmente relevante.

Esto es por que dentro de la vulneración contra un soporte informático debe establecer la esfera delictiva que se encuentra el sujeto activo, teniendo en su aspecto subjetivo y objetivo, he aquí su desarrollo a titulo de ejemplo: El sujeto activo se propone vulnerar cuanto sea necesario una serie ilimitada de servidores en su función natural, con el cual en su aspecto subjetivo se plantea un fin (la vulneración como objetivo), selecciona los medios para su obtención de su objetivo, por el cual su instrumento esencial es un instrumento informático y el conocimiento necesario para poder vulnerar y diseñar, en este estado es necesario regresar mentalmente a la finalidad y selecciona el medio adecuado, una vez representado mentalmente también se visualiza los efectos concomitantes que pueden producirse con su conducta.

Ya una vez en la parte externa pone su aspecto subjetivo en el mundo fáctico, realizando las operaciones necesarias en el medio seleccionado, creando el dispositivo lógico (virus) que permitirá la finalidad planteada, donde se representa la posibilidad de resultados concomitantes, que puede ser el daño a la información o el riesgo de reproducirse en otros instrumentos informáticos y ya como tercera etapa, dar en marcha el curso de la casualidad, pero ésta ya está contemplada ex ante, de la posibilidad de su acontecer, que es el caso de que el daño programado representado en la mente del sujeto activo, es conveniente aclararlo, su curso causal es modificable en tiempo y no en la conducta.

3.11. TIPICIDAD

Como es sabido la tipicidad es la adecuación de la conducta al tipo, y según Zafaronni "...el tipo es predominantemente descriptivo, por que los elementos descriptivos son los más importantes para individualizar una conducta y entre ellos de especial significación es el verbo, que es precisamente la palabra que sirve gramaticalmente para cometer un acción".[64]

En otras palabras el tipo tiene como función la individualización de la conducta humana que son penalmente prohibidas. El tipo es la hipótesis que le pertenece a la ley, mientras que la tipicidad pertenece a la conducta.

En estos tipos de conductas que se estudian y que en la legislación internacional se le denominan delitos informáticos, y que en México aun no existen literalmente en la ley, generalmente los tipos que tratan de regular estas conductas son tipos abiertos, que el juez debe de complementar a base de otras legislaciones externas, en su caso, para comprobar el cuerpo del delito y la probable responsabilidad del sujeto que realiza la conducta ilícita, por lo que el

[64] ZAFFARONI, Op. Cit. p.392

Creando un tipo penal con una antinormatividad que regule conductas relacionadas con instrumentos informáticos, se llegará a una regulación eficaz, en estricto derecho, seleccionando a aquellas conductas ilícitas que afecten a la sociedad, dejando que las legislaciones secundarias como la Ley de Derecho de Autor u otras legislaciones se contemple preceptos que se enfoquen aquellas conductas que tengan como finalidad la sanción correspondiente de acuerdo a su fin de su existencia de dichas leyes, sin embargo aún se ha dejado al arbitrio dichas conductas en el ordenamiento penal, dejando en indefensión los sujetos que lo realicen, sin ningún sistema judicial penal imparcial.

Ahora bien los preceptos permisivos como lo menciona Zafanonni es la categoría de ejercicios de derechos lo cual se manifiesta de manera objetiva en permisos en el orden jurídico y en jerarquía superior (constitución).

Por lo que una vez analizado los preceptos permisivos (causas de justificación) con la conducta ilícita que se propone a legislar, y no existiendo en el orden jurídico un descripción legal que lo ampare será un injusto penal.

3.13. CULPABILIDAD

Retomando nuevamente a Zafaronni, lo define a la culpabilidad en su libro de derecho Penal como "el juicio que permite vincular el forma personalizada el injusto a su autor y de este modo operar como el principal indicador que desde la teoría del delito, condiciona la magnitud del poder punitivo que puede ejercer sobre este." [67] Mientras en su libro Manual de Derecho Penal lo define como "...la reprochabilidad del injusto al autor ¿Que se le reprocha? El injusto ¿Por que se le reprocha? Por que no se motivo en la norma ¿Por que se le reprocha no haberse motivado en la norma? Por que le era exigible que se motivase en ella. Un injusto, es decir, una conducta típica y antijurídica es culpable cuando el autor le es

[67] ZAFFARONI, Eugenio Raúl, et al, p. 620

Creando un tipo penal con una antinormatividad que regule conductas relacionadas con instrumentos informáticos, se llegará a una regulación eficaz, en estricto derecho, seleccionando a aquellas conductas ilícitas que afecten a la sociedad, dejando que las legislaciones secundarias como la Ley de Derecho de Autor u otras legislaciones se contemple preceptos que se enfoquen aquellas conductas que tengan como finalidad la sanción correspondiente de acuerdo a su fin de su existencia de dichas leyes, sin embargo aún se ha dejado al arbitrio dichas conductas en el ordenamiento penal, dejando en indefensión los sujetos que lo realicen, sin ningún sistema judicial penal imparcial.

Ahora bien los preceptos permisivos como lo menciona Zafanonni es la categoría de ejercicios de derechos lo cual se manifiesta de manera objetiva en permisos en el orden jurídico y en jerarquía superior (constitución).

Por lo que una vez analizado los preceptos permisivos (causas de justificación) con la conducta ilícita que se propone a legislar, y no existiendo en el orden jurídico un descripción legal que lo ampare será un injusto penal.

3.13. CULPABILIDAD

Retomando nuevamente a Zafaronni, lo define a la culpabilidad en su libro de derecho Penal como "el juicio que permite vincular el forma personalizada el injusto a su autor y de este modo operar como el principal indicador que desde la teoría del delito, condiciona la magnitud del poder punitivo que puede ejercer sobre este." [67] Mientras en su libro Manual de Derecho Penal lo define como "...la reprochabilidad del injusto al autor ¿Que se le reprocha? El injusto ¿Por que se le reprocha? Por que no se motivo en la norma ¿Por que se le reprocha no haberse motivado en la norma? Por que le era exigible que se motivase en ella. Un injusto, es decir, una conducta típica y antijurídica es culpable cuando el autor le es

[67] ZAFFARONI, Eugenio Raúl, et al, p. 620

reprochable la realización de esa conducta, por que no se motivo en la norma, siéndole exigible, en las circunstancias en ella...". [68]

Por lo que se refiere específicamente a la reprochabilidad, Enrique Bacigalupo lo clasifica a la culpabilidad en dos: La capacidad de la culpabilidad y la cognocibilidad de la antijuricidad. Esto para hacer el juicio valorativo en su actuar, es decir, si el sujeto al momento de actuar tenía la capacidad necesaria y libre en su acto para que pueda ser que una persona que tenga la finalidad de manipular un instrumento informático sea amenazada o presionado para cometer daños al sistema informático.

Por una pare, es importante analizarlas estos elementos a exponer ya que con estos estudios se dará un conocimiento mas eficaz y señalar que efectivamente es necesario regular y aplicar los elementos del delito, para conformarlos hacia las nuevas conductas que se relacionan a objetivos y medios de comisión de carácter intangible y de valor cuantificable.

Bacigalupo señala:

a) Capacidad de culpabilidad (imputabilidad). La capacidad de culpabilidad requiere que el actor haya podido, en el momento del hecho punible, comprender la criminalidad de su acto y comportarse de acuerdo a esa comprensión. Ejemplo: Insuficiencia en las facultades mentales, alteración morbosa en las mismas; y grave perturbación de la conciencia.

b) Conocimiento potencial de la antijuricidad: Zafaronni establece al respecto: como la posibilidad de conocimiento y comprensión del injusto (conocimiento potencial) se halla en la culpabilidad, permaneciendo ajeno al dolo, sea que este se halla en el tipo (finalista) o en la culpabilidad (causalista)

[68] Op Cit. P. 543.

La voluntad humana requiere capacidad psíquica para realizar cierta conducta requerida en su esfera material, el derecho penal sanciona aquellos sujetos que tiene dicha capacidad psíquica en función de una conducta prohibitiva.

La imputabilidad que es un presupuesto de la culpabilidad, requiere de la capacidad psíquica que abarca la voluntariedad del actor para responder a la exigencia de que comprenda la antijuricidad de su conducta, y de que adecue su conducta a esta comprensión, por que es factible de que exista perfecta capacidad de comprensión de la antijuricidad de su conducta – e incluso efectiva comprensión de ella -, y, no obstante, el agente no tiene capacidad psíquica para adaptar la conducta a esa comprensión, como sucede en los múltiples casos de fobias severas.

Por lo que Zafaronni lo define como "... la ausencia de impedimento de carácter psíquico para la comprensión de la antijuricidad y para la adecuación de la conducta conforme a esa comprensión...".[69]

Estudiosos del derecho asignan a la Imputabilidad como elemento de la culpabilidad, mientras que otros tratadistas lo adecuan como elemento del delito, y al respecto Zafaronni señala que la imputabilidad es la ausencia del impedimento psíquico para la comprensión de la antijuricidad y para la adecuación de la acción a esa comprensión, corresponde su ubicación sistemática en el mismo nivel analítico en que se haya la posibilidad exigible de comprensión de la antijuricidad por un lado, y de la ausencia de situación reductor o reductora por otro, esto es, en la culpabilidad.

Existen varias noticias que informan que agentes vulneran sistemas informáticos a través de virus transmitidos por Internet, y que estos agentes no rebasan la edad de 18 años, que dichos individuos manipulan de manera eficaz

[69] ZAFARONNI, Eugenio, et al, Op. Cit p. 664

los sistemas informáticos, en busca de información confidencial o como retos que se imponen, por lo cual es evidente la falta de seguridad que permiten ser vulnerados dichos sistemas, por tanto en necesario que en estos actos ilícitos se requiere un cuidado y protección jurídica para la seguridad del funcionamiento de los sistemas informáticos.

3.14. PUNIBILIDAD

El estado debe imponer medidas punibles como sanción a determinadas conductas ilícitas por la ley, por lo que es necesario antes de enfocarnos a la pubinilidad conocer el significado de la pena.

Existen, muchas definiciones sobre la pena, una de las importantes se encuentra en la obra de Castellanos Tena que expone el de C. Bernaldo de Quirós que lo define: "...es la reacción social jurídicamente organizada contra el delito..." así también el Mtro. Eugenio Cuello Calón la define como "...el sufrimiento impuesto por el Estado, en ejecución de una sentencia, al culpable de una infracción penal.", mientras que el autor lo define como: "...es el castigo impuesto por el estado al delincuente, para conservar el orden jurídico...".[70]

Ahora bien, la punibilidad consiste en el merecimiento de una pena en función de la realización de cierta conducta. Un comportamiento es punible cuando se hace acreedor a la pena; tal merecimiento acarrea la conminación legal de aplicación de esa sanción.

[70] Cfr. CASTELLANOS Tena, Fernando., "Lineamientos Elementales de Derecho Penal", Trigésima Octava Edición, Edit. Porrúa, México 1997, p.317, 318.

Es punible una conducta cuando por su naturaleza amerita ser penada; se engendra entonces la conminación estatal para los infractores de ciertas normas jurídicas (ejerciendo del jus puniendi).

La punibilidad es un: a) Merecimiento de penas; b) Conminación estatal de imposición de sanciones si le llenan los presupuestos legales; y c) Aplicación fáctica de las penas señaladas en la ley.

La finalidad de la pena es la de proteger a la sociedad, para eso debe ser intimidatoria para que la delincuencia presienta el temor al aplicarla; una pena ejemplar, es decir, la efectividad de la amenaza de la autoridad; correctiva, para una readaptación a la vida normal y reintegrarse nuevamente a la sociedad; Eliminatoria que puede ser temporal o definitivo para que el delincuente se adapte nuevamente a la vida normal o se trate de sujetos incorregibles; y una pena Justa donde se destaque la justicia, la seguridad y el bienestar social.

También las medidas de seguridad es una sanción que tiene como finalidad la evitación de nuevos delitos, es muy confundible con las penas, sin embargo las primeras tiene carácter aflictivo mientras las segundas tienen la idea de expiación, en cierta forma la retribución. También suele confundirse las medidas de seguridad con los medios de prevención estos últimos tiene como finalidad propio, ajeno al derecho penal, ya que se dirige a toda la población como son la educación pública, alumbrado nocturno de las calles etc., mientras que las primeras recaen sobre una persona por haber cometido una infracción típica.

Sobre la hipótesis que se señaló existe una punibilidad coherente y justa para estos delitos contra la informática, ya que debe equiparase al daño que se ocasionó con el delito de robo, es decir, así como se impone la pena dependiendo la cantidad de lo robado, así también debe cuantificarse la utilidad, el valor y la función del soporte lógico a través de peritajes y tomar en cuenta las reglas que se

aplican con el delito del robo para imponer la pena. Nuevamente se expone la hipótesis:

> "El que sin autorización y sin derecho altere, introduzca, programe, provoque la transmisión o ejecución de programas con el fin de modificar, destruir, o cause negación de servicio, por cualquier medio en contra de programas o sistemas de naturaleza informática, **se le impondrá de seis meses a dos años de prisión.**
>
> **Cuando es en contra de sistemas financieros de imposible reparación se le impondrá de dos a cinco años de prisión.**
>
> **Cuando es en contra de sistemas del Estado Federal y de imposible reparación se le impondrá de tres a siete años de prisión.**

Como se observa la penalidad es muy coherente, basándose en la necesidad y el valor que significa la función del soporte lógico y sus consecuencias que altera el valor que le da la nueva sociedad virtual. Por lo tanto se debe de prevalecer a través del derecho los valores fundamentales que nacieron con el Internet y los sistemas informáticos para que permanezca la seguridad, el anonimato y mas que nada la justicia dentro de la cibernética.

Es por ello que el Estado al valorar la conducta ilícita debe de considerar la utilidad en la función de los sistemas informáticos, es decir, el disvalor del acto, así como el disvalor del resultado y sus efectos concomitantes trascendentes para imponer una pena equilibrada y justa.

4. CAPÍTULO 4.

4. CAPÍTULO 4.

MEDIOS DE PRUEBA QUE PERMITEN ACREDITAR LA VULNERACIÓN ILÍCITA EN LOS SISTEMAS DE INFORMÁTICA

4. TEORÍA Y PRÁCTICA DE LA PRUEBA

De a Cruz Agüero señala: "...El término o palabra "prueba " deriva del latín, probo, bueno, honesto y, probandum, recomendar, aprobar, experimentar, patentizar, hacer fe, acción o efecto de probar, razón con que se demuestre una cosa indicio o señal de una cosa..."[71]

En la práctica, señala el citado autor "...entendemos por prueba en el procedimiento penal a todos los medios de convicción que en la actualidad contempla la ciencia y la tecnología, y aun cualquier hecho o fenómeno perceptible en el mundo circundante, capaces de materializar la verdad o falsedad que se busca y colocar al juzgador en un aptitud de pronunciar la sentencia que en derecho corresponda, con base también en los principios de valoración de la prueba...". [72]

"La sentencia que ha de verse sobre la verdad de los hechos de la acusación, tiene por base la prueba. Suministrar la prueba de los hechos del cargo, tal es la misión de la acusación; en cuanto al acusado, se esfuerza en hacer venir á tierra el aparato de las pruebas contrarias, y presenta las que le disculpan".[73]

Así mismo señala este último autor que los preceptos en materia de prueba se refieren también a los medios que se ponen a disposición del magistrado instructor para el descubrimiento de la verdades. Es así que los medios de prueba

[71] DE LA CRUZ Agüero, Leopoldo, "Procedimiento Penal Mexicano", Porrúa, tercera edición, 1998, p. 199.
[72] Ibidem p 200
[73] C. J. A. MITTERMAIER, "Tratado de la Prueba en Materia Criminal". Angel Editor, 1999, 17

es la forma o el acto en el cual se suministra conocimiento sobre algo que se debe determinar en el proceso.

Ahora bien, el órgano de la prueba, es la persona física portadora de un medio de prueba, es decir, la persona física que suministra en el proceso el conocimiento del objeto de la prueba.

Colín Sánchez, citado por De la Cruz Agüero, menciona que el órgano de la prueba es la persona que proporciona el conocimiento por cualquier medio factible y que los sujetos que intervienen en la relación procesal son órganos de prueba: el probable actor del delito, el ofendido, el legitimo representante, el defensor y los testigos

Mientras que el objeto de la prueba es buscar la verdad, demostrar la verdad y que el juzgador, una vez concluida la secuela procedimental, contando con el acervo probatorio aportado por las partes, esté en aptitud de hacer uso del árbitro judicial que la ley otorga y pronunciar la sentencia que en derecho corresponda.

Leopoldo Silva, establece que el objeto de la prueba abarca los elementos objetivos y subjetivos del delito, es decir, la comprobación de los elementos del cuerpo del delito, la conducta del sujeto activo, el resultado del hecho criminoso y el nexo causal que debe unir la conducta con el resultado.

Dentro del sistema penal mexicano contempla los siguientes probatorios:

a) Libre b) Tasado c) Mixto

Dentro del sistema Libre se tiene como ejemplo el artículo 206 del Código Federal de Procedimientos Penales dispone: se admitirá como prueba en los términos del artículo 20 fracción V de la Constitución Política de los Estados

Unidos Mexicanos, todo aquello que se ofrezca como tal, siempre que pueda ser conducente y no vaya contra el derecho, a juicio del Juez o Tribunal, cuando la autoridad judicial lo estime necesario, podrá por algún otro medio de prueba, establecer su autenticidad.

Así mismo la fracción V del artículo 20 en su apartado A, así como en su apartado B en su fracción II de la Constitución, en relación con el diverso 206 del Código Federal de Procedimientos Penales, tanto el Ministerio Público, en su calidad de autoridad de la investigación de los delitos y persecución de sus autores, ya convertidos en parte en el proceso, y el acusado y defensor, gozan de plena libertad para hacer uso de los medios probatorios conducentes y permitidos por el derecho, con objeto de afirmar sus pretensiones y aportar una convicción constitucional de un sistema libre de pruebas en el procedimiento penal mexicano.

b) Por lo que hace al sistema tasado, este se encuentra en la verdad formal, basándose exclusivamente en los medios probatorios establecidos por la ley y para cuya valoración el juez debe sujetarse a las reglas fijadas para tal efecto y que constituyan una necesidad de prevenir arbitrariamente a ignorancia del juez, es decir, que en este caso el órgano jurisdiccional debe sujetarse a alas pruebas señaladas en el Código Procesal Penal en que se trate, como son la confesión, inspección, peritos, testigos, careos y documento.

c) Se estima mixto a la combinación que surge entre el libre y tasado, o sea, que además de que las partes deben sujetarse a las pruebas que señala la fracción V del artículo 20 Constitucional y el 206 del Código Federal de Procedimientos Penales, así como la obligación del juzgador de observar las reglas para su valoración, las partes pueden ofrecer y desahogar todo elemento de prueba no especificado por la ley procesal, siempre y cuando no sea contra derecho y vayan contra la moral y las buenas costumbres.

La carga de la prueba recae comúnmente quien afirma un hecho o derecho que le asiste, sin embargo en materia penal la carga de la prueba incumbe al Ministerio Público como el acusado, e incluso al órgano juzgador en los casos que la ley procesal señale.

En nuestro sistema judicial y administrativo, y mas que nada el Código Federal de Procedimientos Penales se contempla:

I. La Confesión
II. La Inspección
III. La Pericial
IV. La confrontación
V. Los careos
VI. La Documental

En consideración de lo anterior, la prueba en México a tomado varios criterios para su valoración, sin embargo es menester tomar como instrumento de prueba a valorar a los elementos telemáticos o el mismo soporte lógico, al respecto menciona Garrido "Es muy importante que nuestras leyes procesales actualicen sus elementos de prueba con el desarrollo tecnológico, toda vez que esto proporcionará que tanto los usuarios como el proveedor de acceso a Internet logren un grado considerable de confianza en las transacciones en línea"

La volatilidad de los datos en lo que la prueba informática se refiere exige las máxima precauciones a la hora de obtener el *corpus instrumentorum*. Dicha actividad comienza desde el momento del allanamiento mismo. Los métodos tradicionales de búsqueda y el hallazgo de la prueba en todas las investigaciones, no resultan suficiente para el éxito en los procedimientos por delitos informáticos. Aquello que se halló en el lugar del hecho, debe ser exactamente lo que llegue al ámbito del perito, para su análisis y dictamen.

No escapa a la lógica más simple suponer que, al procederse el diligenciamiento de una orden de allanamiento, quienes resultan afectados y, de alguna manera se saben partícipes de una actividad delictual, intentarán por todos los medios evitar que los funcionarios intervinientes obtengan elementos probatorios que pudieren incriminarlos. Partiendo de esta natural reticencia a que prospere la medida judicial, debe tenerse en cuenta que, cuando aquello que resulta de interés .se haya almacenado en computadoras, por lo general, sus operadores conocen las rutinas que deben llevarse a cabo rápidamente para eliminar los registros comprometedores o bien inutilizar completamente los sistemas.

Atento a ello, a fin de no echar por tierra la labor investigativa previa es menester como primera medida disponer el alejamiento de toda persona que se halle en presencia de los computadores, servidores o tableros de suministro eléctrico, para proceder, inmediatamente a desconectar la totalidad de los teclados hasta que cada uno de los terminales sea examinados por los expertos.

4.1. PRUEBAS EN PARTICULAR

LA CONFESIÓN.

Lo establece el artículo 207 del Código Federal de Procedimientos Penales, que estipula: es la declaración voluntaria hecha por persona no menor de dieciocho años, en pleno uso de sus facultades mentales, rendida ante el Ministerio Público, el Juez o Tribunal de la causa, sobre hechos constitutivos del tipo delictivo materia de imputación, emitida con las formalidades señaladas por el artículo 20 de la Constitución Política de los Estados Unidos Mexicanos.

El Maestro Marco Antonio Díaz de León, citado por De la Cruz Agüero, define a la prueba Confesional como "...una manifestación que hace el inculpado sobre la

participación activa que hubiera tenido en los hechos delictivos, que dicha manifestación debe ser libre, con toda la voluntad del acusado, es decir, sin presión externa ajena, sea hecha ante el Ministerio Público o ante el Juez...".[74]

Esta prueba servirá para comprobar, si existiera, personas ajenas al hecho que aportara elementos que percibieron a través de sus sentidos, necesarios, para tener indicios sobre el acto delictivo con relación a la vulneración a un soporte lógico, esto es así por ejemplo, en un Ciber café que puede ser el encargado del mismo, su hora de entrada y salida, el posible nombre, y el equipo informático utilizado; otro ejemplo sería personas cercanas al sujeto que participó en la creación del instrumento lógico que vulnero el programa o el que introdujo dicho instrumento lógico para la vulneración.

LA INSPECCIÓN.

Lo establece el artículo 208 del Código Federal del Procedimientos Penales, que describe: Que es materia de inspección todo aquello que puede ser directamente apreciable por la autoridad que conozca del asunto... .

El Diccionario Jurídico Temático, señala que "...en un sentido lato, es la admisión que se hace en un juicio (sinónimo de procedimiento judicial) o fuera de él de la "verdad" (coincidente o no con la verdad histórica) de un hecho o de un acto, que produce consecuencias desfavorables para el confesante...". [75]

Nuevamente Diaz de León, puntualiza que la palabra inspección se deriva del latín *inspectio- tiones*, que significa "acción y efecto de inspeccionar y ésta a su vez equivale a examinar, reconocer una cosa con detenimiento... que procesalmente la inspección es un medio de prueba, real, directo, por medio del cual el juzgador observa o comprueba personalmente sobre la cosa, no solo su

[74] DE LA CRUZ Agüero, Leopoldo, Op. Cit. p. 224
[75] "Diccionario Jurídico Temático", Dir. Leonel Pereznieto Castro, V.6, México, 2000, 98 pp

existencia o realidad, sino alguna de sus características, condiciones o efectos de interés por la solución del asunto sometido a su decisión..".[76]

La inspección es la prueba que nos permite identificar el objeto material o los medios comisivos físicos y posibles lógicos que se utilizaron como instrumento para realizar la vulneración contra el soporte lógico, claro es cierto que si el acto se realizo fuera del Estado Mexicano se tendría que actuar conforme a los tratados internacionales y los lineamientos establecidos, como aprecia en este aspecto es mas tardado y poco eficiente en estos actos, por lo tanto es conveniente utilizar otros medios probatorios como es la pericial, obteniendo resultados mas eficaces.

PERICIAL

El artículo 220 del citado ordenamiento procesal, estipula "siempre que para el examen de personas, hecho y objeto se requieran conocimientos especiales, se procederá con la intervención de peritos.

José Alberto Silva Silva, citado por De la Cruz Agüero, lo define como " ... el peritaje consiste en el informe o declaración de experto en una rama del saber, en el que previa aplicación del método científico, expresa a su juicio, opinión o resultado en torno a una cuestión científica (científica, técnica o artística) que se le ha planteado...".[77]

Mientras que para Colín Sánchez, manifiesta que la peritación, en el Derecho de Procedimientos Penales, es el acto procedimental o ciencia (perito), previo examen de una persona, de una conducta o hecho, o cosa, emite un dictamen conteniendo su parecer y los razonamientos técnicos sobre la materia en la que se ha pedido su intervención.

[76] Cfr. DE LA CRUZ Agüero, Op. Cit. 275
[77] Idem p.303

Es la prueba de mas importancia en la materia de actos ilícitos en contra de la informática, ya que nos permite conocer e identificar al sujeto activo, así como su actuar y los medios utilizados que se utilizaron, el nexo causal que se desprendió de la conducta del sujeto al introducir el instrumento lógico causando en el tiempo el resultado y como se dijo el desarrollo del nexo causal no depende de la conducta del sujeto sino del programa ya configurado, es así que con base a los peritajes de la informática forense, instrumentación electrónica, y una reconstrucción mediante modelización y animación se tendrá plenos indicios que nos permitiría identificar al sujeto y la comprobación del hecho que se le puede imputar.

TESTIMONIAL

El Código Federal de Procedimientos Penales, en su artículo 242 dispone que toda persona que sea testigo está obligada a declarar con respecto a los hechos investigados, las preguntas que formulen las partes deberán guardar relacion con los hechos.

El multicitado Maestro De la Cruz Agüero, señala que "... por testigo debe entenderse a la persona física, sin impedimento legal alguno y con capacidad de discernir, que participó directa o indirectamente, o que presencia casualmente, o tuvo conocimiento de una conducta o hecho estimado como criminal por la ley penal, y que tiene la obligación ineludible de comparecer ante los autoridades judiciales o administrativas, a narra, informar o explicar esa experiencia o conocimiento, con objeto de que la autoridad establezca la verdad en favor o en contra del o los autores de tal hecho
ilícito...".[78]

Es una prueba que aportaría muy pocos elementos para la comprobación de la conducta y del hecho delictivo, por que generalmente el sujeto actúa

[78] DE LA CRUZ Agüero, Op. Cit., p.360

solitariamente sin necesidad de otro en el acto mismo, realizándolo en su propio computador, en un Ciber Café, en su oficina, sin embargo es posible encontrar ciertos testigos en este último, ya que en algunos sitios te registran y te asignan el número de máquina, por lo tanto es posible que una vez ya identificado el lugar y el cumputador utilizado, aportaría las caracteristicas físicas del sujeto y el posible nombre, sin calificarlas como indicios.

CAREOS

Rafael de Pina, establece que careo "...es la diligencia personal en virtud de la cual son enfrentadas dos personas que han formulado declaraciones contradictorias con ocasión de un proceso, dando a cada una de ellas la oportunidad de afirmar la sinceridad de la propia y su conformidad con la verdad." Mientras que Guillermo Colín Sánchez, lo define " como un acto procesal cuyo objeto es aclarar los aspectos contradictorios de las declaraciones del procesado o procesados, del ofendido y los testigos, o de estos entre sí, para, con ello, estar en posibilidad de valorar esos medios de prueba y alcanzar el conocimiento de la verdad."[79]

El careo es otra prueba que no aportaría ningún elemento para la comprobación del cuerpo del delito y la probable responsabilidad, es claro que su ofrecimiento no permite acreditar ningún acto o hecho, por lo tanto es innecesario para estos actos ilícitos su utilidad.

DOCUMENTAL

La prueba documental, es el medio que se hace uso en un procedimiento de escritos públicos o privados o por algún otro elemento material susceptible de facilitar la comprensión o sentido de algún hecho o acto.

[79] Cfr. DE LA CRUZ Agüero. Op. Cit. p. 409

Mientras que Sergio García Ramírez, citado nuevamente por De la Cruz Agüero, puntualiza que "...documento es el concepto genérico de que el instrumento constituye una especie, es la materialización de una pensamiento, mismo que al adquirir una forma objetiva, se transforma y concreta en una documento..."[80]

La documental es una prueba que se tiene que tomar en cuenta en su forma electrónica que lo legisla el Código de Procedimientos Civiles Federal en su Capitulo de Pruebas que le da valor probatorio teniendo algunos requisitos fundamentales para su autenticidad, ya que permitiría en los hechos ilícitos en la informática acreditar ciertos factores en su análisis, por ejemplo aportar documentación en su naturaleza informática información en lenguas de programación, los mecanismos de seguridad, su autenticidad, y su almacenamiento de la información en el disco duro así como otros elementos.

4.2. NUEVAS TECNOLOGÍAS Y SU PROBLEMÁTICA JUDICIAL

Por los grandes avances de la ciencia y la técnica, el Derecho Informático, es decir, aquella rama del Derecho que permite plantear las soluciones jurídicas a los problemas generados por la aplicación de la informática en la sociedad, se ve afectado por la aplicación de las Nuevas Tecnologías de la Información en la realidad circundante. Como podemos apreciar diariamente dichas tecnologías evolucionan constantemente, siendo una situación innegable que plantean nuevos retos a los profesionales de las diversas disciplinas, en el ámbito nacional y mundial

Por los grandes avances de la ciencia y la técnica, el Derecho Informático, es decir, aquella rama del Derecho que permite plantear las soluciones jurídicas a los problemas generados por la aplicación de la informática en la sociedad, se ve

[80] Op Cit 436

afectado por la aplicación de las Nuevas Tecnologías de la Información en la realidad circundante. Como podemos apreciar diariamente dichas tecnologías evolucionan constantemente, siendo una situación innegable que plantean nuevos retos a los profesionales de las diversas disciplinas, en el ámbito nacional y mundial

Las nuevas tecnologías son aquel conjunto de medios, procedimientos y conocimientos técnicos que permiten generar una serie nuevas perspectivas de desarrollo para el ser humano y la sociedad en general, permitiendo generar un mayor grado de eficiencia, efectividad y cumplimiento de las obligaciones en el tiempo oportuno, con lo cual, el beneficio general de usar las nuevas tecnologías se ve incrementado en bien del ser humano.

Es así, que las nuevas tecnologías vienen transformando el mundo diario de los profesionales por cuanto tienen mayor efectividad para acceder, utilizar, producir y generar nuevos datos e información. En un sentido general permiten que sus potencialidades puedan ser incrementadas al extremo de alcanzar altos estándares de calidad. Asimismo, las nuevas tecnologías permiten alcanzar la democratización de la información y el conocimiento.

El gran dilema que plantea la irrupción de las nuevas tecnologías, especialmente la informática en el campo de las comunicaciones, es que pone en crisis la vigencia de la imperatividad de las normas locales, al desarrollarse cada día más relaciones (negociables, sociales, culturales, etc.) en una dimensión espacial que no es "territorial". Son relaciones "sin rostro", que ocurren en un lugar "virtual", y al que cada día accedemos con más frecuencia e intensidad, pero con menos conocimiento de los presupuestos que permiten su funcionamiento, la posibilidad de vulnerar nuestra privacidad, honor o aún en los negocios. La informática en tanto es la tecnología que posibilita el almacenamiento, procesamiento y recuperación de información en volúmenes y a velocidades hasta hace poco desconocidas, y la telemática, que ha incrementado las posibilidades

de comunicación y ha dado lugar a novedosas relaciones contractuales, nos obligan a pensar nuestros paradigmas tradicionales, en particular el de la igualdad. El desarrollo incontenible y aún no regulado o irregulable de Internet, los problemas del comercio electrónico, el documento y la firma digital, el derecho a la información y una adecuada protección de los derechos personales, demandan respuestas también novedosas y originales.

Por esto, "... una visión de la Justicia para el futuro nos conduce inevitablemente a un sistema de resolución de conflictos que integre el sistema clásico tradicional que privilegia el poder y los derechos conjuntamente con los sistemas alternativos que tienen prioridad los intereses de las partes en disputa. Esto no implica menoscabar la jurisdicción judicial, sino arbitrar medios alternativos y complementarios cuya finalidad no sea sólo descongestionar los Tribunales y proveer soluciones nuevas a los diversos conflictos en el menor tiempo posible, sino también paliar la insatisfacción que muchos sectores de la sociedad exponen al decir que no encuentran acceso a una solución justa de sus disputas..."[81]

4.2.1 TELEMÁTICA E INTERNET

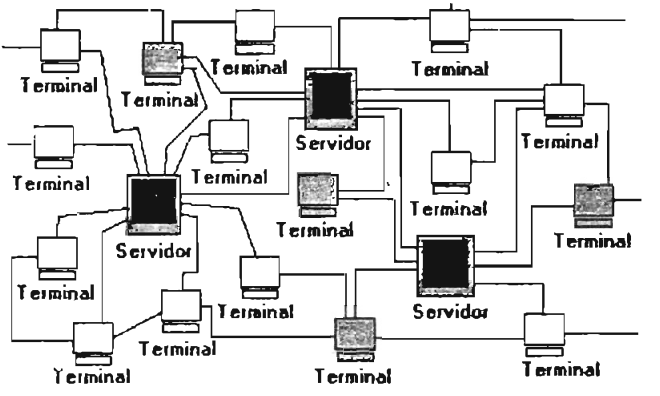
La ***red telmática o de telecomunicaciones*** es el concepto mediante el cual se nombra al conjunto de computadoras que se comunican o se conectan entre sí para transferir o intercambiar la información que se encuentra guardada en los discos duros de las computadoras.

Además de la información, con una ***red telemática*** se puede hacer uso de servicios o de programas que se encuentran disponibles en determinadas computadoras de la red, a las cuales se les llama ***servidores***, a las que se

[8] http://www.seei.org/Anuncios/amaya.htm. Consultado en fecha 15 de Septiembre de 2004

conectan otras computadoras, llamadas ***terminales,*** desde las que se solicita la información, los servicios o los programas.

Los servidores también sirven para conectar a las terminales a otras computadoras o a otros servidores. De esta manera es posible que se pueda formar una conexión con todas las computadoras existentes en el mundo. Una red telemática permite ofrecer o disponer información a distancia, igualmente propicia y hace posible la comunicación de una máquina con otra máquina, de un ser humano con la máquina o de un ser humano con otro ser humano a la distancia, por ello se le conoce también como ***red de telecomunicaciones.***



R E D T E L E M Á T I C A

La conexión imaginaria de las computadoras (entre terminales y servidores) forma en sentido figurado una red o una telaraña. ***Internet*** es una red de telecomunicaciones. "Antes que ***Internet*** se usó de manera muy difundida la red llamado ***Bitnet (Because It's Time NETwork, 1981).*** Antes que ***Bitnet*** e **Internet,** hubo otra red que fue el órigen de ésta última llamada ***ARPANET (1969).*** En los inicios de las redes telemáticas era necesario saber comandos de programación para hacer uso de las redes de telecomunicación. Actualmente, ***Internet*** se usa a través de un mecanismo formado por un sistema de información

creado por los archivos que están en las computadoras y un sistema de hipertexto y símbolos visuales, que sirve para lograr la conexión con las computadoras y con los archivos de éstas..."[82]

El sistema de información es una *interfaz gráfica de Internet*, porque no requiere del uso de comandos de programación para activar los programas y la conexión con las computadoras.

La red que forma esta interfaz gráfica con los archivos que guardan información multimedia recibe el nombre de ***Word Wide Web (1993).*** Se ha popularizado con el nombre simple de ***Web***. Simbólicamente se le representa con la triple w ***(www)*** .

Además de la información, con una *red telemática* se puede hacer uso de servicios o de programas que se encuentran disponibles en determinadas computadoras de la red, a las cuales se les llama *servidores,* a las que se conectan otras computadoras, llamadas *terminales,* desde las que se solicita la información, los servicios o los programas.

Actualmente, *Internet* se usa a través de un mecanismo formado por un sistema de información creado por los archivos que están en las computadoras y un sistema de hipertexto y símbolos visuales, que sirve para lograr la conexión con las computadoras y con los archivos de éstas.

Es así que la red de redes es un medio para hacer efectivo el prefacio de que el conocimiento es poder, hace que sea un instrumento real para la creación de la sociedad del saber, para poder afrontar los riesgos económicos de la aldea global económica y para sobrevivir en ese mundo de feroz competencia que es la informática asociada a las comunicaciones, lo que se ha dado en llamarse telemática.

[82] http://iteso.mx/~qcorona/red_telematica.htm. Consultado en fecha 21 de Abril de 2005

4.2.2. INSTRUMENTACIÓN ELECTRÓNICA

La electrónica se encuentra integrada en la mayoría de las actividades de la sociedad moderna: contribuye a mantener y optimizar los procesos industriales, proporciona enlaces de comunicación y permite un mejor nivel de vida mediante sus aplicaciones en la medicina, el hogar y el esparcimiento.

La Instrumentación Electrónica es una de las áreas de conocimiento de mayor importancia, desarrollo y avance en la industria electrónica de nuestros días, y ha venido creciendo a pasos acelerados, con gran repercusión en otras, tales como las comunicaciones, las mediciones y el control automático y convirtiéndose cada vez con mayor claridad en un área de especialización de los Ingenieros en Sistemas Electrónicos y de Comunicaciones.

Los temas tratados en esta materia son entre otros:

a)Principios básicos de un sistema de Instrumentación Electrónica,
b) Sensores y Transductores,
c) Acondicionamiento de las Señales,
d) Acoplamiento y Ruido,
e) Interfaces de Potencia,
f) Confiabilidad y Características Mecánicas y Eléctricas de los Instrumentos,
g) Seguridad Eléctrica, entre otros.

A su vez la instrumentación electrónica se fundamenta en el estudio de los sistemas de medida electrónicos, analizando múltiples configuraciones de los sistemas y elementos integrantes de los mismos sensores y acondicionadores.

La carrera de ingeniero en electrónica y comunicaciones se apoya en:

1. El electromagnetismo, para entender los mecanismos de manipulación y radiación de señales en los sistemas de comunicaciones, así como para analizar los procesos de conversión de energía en las máquinas eléctricas.

2. La teoría de circuitos eléctricos, para entender, analizar y manipular las señales electrónicas en sistemas de control, de computación y de comunicaciones.

3. La computación, para modelar, analizar, programar y diseñar sistemas electrónicos con características complejas.

El ingeniero en electrónica y comunicaciones tiene como áreas de especialidad el diseño electrónico, la automatización y control, y las comunicaciones eléctricas

En el área de diseño electrónico se dedica, primordialmente, al análisis, diseño e implantación de sistemas analógicos y digitales usando circuitos integrados, microcontroladores, microprocesadores y dispositivos electrónicos de potencia, aplicando sus conocimientos a la producción industrial, y las telecomunicaciones y la medicina.

En el área de comunicaciones, se dedica al análisis, diseño e integración de sistemas de comunicación de audio, vídeo y usando tecnologías de microcontroladores de uso especifico, enlaces ópticos y satelitales.

De esta forma, la instrumentación electrónica con sus respectivas especialidades, permiten investigar de manera mas a fondo las comunicaciones conectados a los sistemas informáticos, en el momento del envío de la información hasta el receptor del mismo, conociendo a base de dicha instrumentación la forma o el medio utilizado y su forma de transmisión, logrando que los peritos en la materia den dictámenes del proceso realizado en las señales de comunicación acerca de que, un instrumento lógico dañino ataque al fin programado.

4.2.3. RECONSTRUCCIÓN MEDIANTE MODELIZACIÓN Y ANIMACIÓN

La reconstrucción mediante modernización consiste en reconstruir sobre la base de imágenes virtuales y en tercera dimensión hechos o actos en el mundo fáctico representándolo a partir de programas que permiten la forma en que se desarrollo dichos hechos o actos y que facilitan, en materia penal, el *modus operandi* del agente, de tal forma que se representa como el virus informático entra a la red de redes y vulnera un sistema informático, desde el origen hasta el objetivo previsto.

Este tipo de Reconstrucción es manejado por estudiosos de desastres naturales, recreando la forma de la afectación de los fenómenos de la naturaleza y prever situaciones de emergencia y daños irreparables, ya sea humana o material.

Por una parte, los peritos han ido desarrollando su metodología, y por otra, la informática, como ciencia de la computación e inteligencia artificial, ha puesto a su disposición avanzadas herramientas infográficas para la modelización y animación virtual con las que simular la realidad y la temporalidad de casi cualquier accidente o crimen.

El daño corporal que se produce en los accidentes o en los delitos violentos es casi siempre extraordinariamente sensible a pequeñas variaciones de las distancias o de los ángulos con los que se produce una contusión. Por este motivo la reconstrucción infográfica de los siniestros tiene para el médico un carácter mucho más ilustrativo que analítico y pericial, sirviendo para representar con precisión pérdidas de movilidad en articulaciones o cualquier tipo de lesión mediante modelizaciones y simulaciones anatómicas y fisiológicas. [83]

[83] Cfr. http://www.iua.upf.es/~jblat/3d_esp.html. Consultado en fecha 20 de Mayo de 2004.

Por este motivo, consideramos útil e interesante el describir razonadamente aquí los recursos tecnológicos y científicos con los que está avanzando la peritología moderna.

La descripción de dichos imágenes sobre la base de la modelización y animación consiste en programas de reconstrucción 3D a partir de múltiples imágenes y calibración, en la perspectiva de potenciar una línea de investigación sobre estas cuestiones delictivas.

Este método es muy usual también en la reconstrucción de organismos vivos sobre la base de imágenes virtuales utilizando la informática, es decir, aprovechamiento de las herramientas avanzadas, modelización y visualización 3D para la simulación y generación de mundos virtuales relacionados con la industria (Se trata concretamente de los caracteres (biológicos) de síntesis y la "ecoinfografía".

La "*ecoinfografía*" es un concepto menos conocido. Se agrupan bajo esa denominación un conjunto, cada vez más numeroso, de técnicas de informática gráfica orientadas a la representación y simulación de los principales elementos de la naturaleza: animales (solos o en agrupaciones), plantas, elementos geológicos, condiciones meteorológicas o fluidos, por citar algunos ejemplos. Estas herramientas permiten reconstruir un hábitat o ecosistema completo, existente o desaparecido, con grado máximo de detalle.

El uso de nuevas tecnologías digitales, especialmente en el terreno de la producción audiovisual, es un complemento imprescindible en la industria del ocio moderna.

Por todo lo expuesto, es evidente que existe una convergencia de dos líneas de actuacion con experiencia complementaria; por un lado, está el interés por difundir una actividad ilícita penalmente relevante realizado a través de

instrumentos electrónicos y por otro, la capacidad para llevarlo a cabo empleando los recursos digitales avanzados e innovadores, favoreciendo la investigación aplicada a un sector estratégico en expansión: el de las tecnologías audiovisuales **mediante** imagen de síntesis digital.

4.2.4. INFORMÁTICA FORENSE

El desarrollo de las nuevas tecnologías informáticas ha cambiado los medios de registro de la actividad intelectual humana. Los computadores son los cuadernos y blocks de esta nueva era de la información. Gran cantidad de documentos son elaborados digitalmente en computadores para ser posteriormente impresos. El correo de cartas en papel fue sustituido prácticamente por el correo electrónico. Las redes de informática permiten nuevos tipos de publicaciones virtuales sin tinta.

Todo lo antes expuesto hace ver que los hechos jurídicos pueden ser claramente ubicados en estos nuevos soportes electrónicos digitales. La experticia grafotécnica o documentológica ha afrontado las necesidades del esclarecimiento de la autenticidad, origen y otros datos de producción de documentos convencionales en papel pero ella se encuentra limitada a los análisis sobre la escritura convencional firmas, tinta y papel.

Es posible investigar quien es el dueño de páginas o sitios en Internet, quienes son los autores de artículos y otros documentos enviados a través de redes o publicados en la misma. Es posible rastrear atacantes exteriores de sistemas e incluso se conocen casos donde se ha determinado la autoría de virus. Son igualmente investigables las modificaciones, lteraciones y otros manejos dolosos de bases de datos de redes internas o externas, y cualquier sistemas de redes, ataques internos. La destrucción de datos y la manipulación de los mismos también pueden ser rastreados. Los hábitos de los

usuarios de los computadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, siendo posible saber de todas las actividades realizadas en un computador determinado.

Los archivos informáticos pueden guardar información sobre su autor, la compañía y otros datos de interés jurídico. Esta información es almacenada a espaldas del usuario pudiendo determinarse en algunos casos en que computador fue redactado el archivo.

Las imágenes digitales y otros medios audiovisuales pueden estar protegidos no solo por derechos de autor sino por las llamadas marcas de agua digitales que servirían para determinar su origen del archivo aunque hayan sido modificados para disfrazarlos y darle una apariencia distinta.

La promoción, evacuación y control de estas experticias informáticas es especial y bajo las normas de naciente, pero desarrollada **informática forense** que se pone al servicio inmediato del derecho para afrontar nuevas tareas probatorias.

La Informática Forense se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial. Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes.

Ahora bien, por **'investigación forense en computación'** se conoce al "...conjunto de herramientas y técnicas que son necesarias para encontrar, preservar y analizar pruebas digitales frágiles, que son susceptibles de ser borradas o sufrir alteración de muchos niveles. Quienes la practican reúnen esos datos y crean una llamada prueba de auditoría para juicios penales. Buscan información que puede estar almacenada en registros de acceso, registros

específicos, modificación de archivos intencionalmente, eliminación de archivos y otras pistas que puede dejar un atacante a su paso...".[84]

En la recuperación de información nos enfrentamos con información que no es accesible por medios convencionales, ya sea por problemas de funcionamiento del dispositivo que lo contiene, ya sea porque se borraron o corrompieron las estructuras administrativas de software del sistema de archivos. La información se perdió por un problema de fallo de la tecnología de hard y/o soft o bien por un error humano. El sujeto pasivo indica su versión de los hechos y a menudo se encuentra la falla original otras que el usuario o sus prestadores técnicos agregaron en un intento de recuperación. Así es que debemos figurarnos a partir del análisis del medio qué ocurrió desde el momento en que todo funcionaba bien y la información era accesible.

En informática forense hablamos ya no sólo de recuperación de información sino de **descubrimiento** de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia para borrar, adulterar u ocultar información. Es por lo tanto esperarse que el mismo hecho de esta adulteración pase desapercibido.

La evidencia informática es frágil por definición y puede fácilmente ser alterada o modificada y así perder autenticidad frente a una corte. Se deben por lo tanto establecer rígidas normas de preservación y cadena de custodia de la misma.
Algunos rastros más evidentes que permanecen en las máquinas son los caché del browser (navegador), las copias de los correos electrónicos, las cookies almacenadas en la navegación, los archivos borrados que aun pueden ser recuperados, los registros de conexión del módem, entre otros.

Algunos programas utilizados son conocidos como la suite de Norton Utilities y demás aplicaciones de uso generalizado para recuperación de archivos,

[84] http://www.internet-solutions.com.co/forense.html. Consultado en fecha 25 de Agosto de 2004.

directorios y datos en disco duros y disquetes. De otra parte, existen aplicaciones más sofisticadas para encontrar, identificar, analizar y preservar evidencia digital que requieren entrenamiento y preparación en diferentes ambientes operacionales como UNIX, MAC, WINDOWS NT.

Básicamente los investigadores forenses en informática, independiente de las plataforma o sistema operacional donde estén efectuando sus actividades, deben procurar cumplir tres requisitos con la información o evidencia identificada o recolectada:

- Se deben utilizar medios forenses estériles (para las copias de la información).
- Mantener la integridad del medio original.
- Etiquetar, controlar y transmitir adecuadamente las copias de los datos, impresiones y resultado de la investigación.

Las metodologías utilizadas pueden ser diversas, pero lo importante es asegurar estos tres requisitos, dado que si no se aseguran, la evidencia puede ser rebatida y descartada como medio probatorio.

El servicio de peritaje tiene por objeto certificar y dar fe del contenido o de la ausencia de contenido de un disco, y precisar la naturaleza y motivo de la pérdida de información.

4.3. LA PRESUNCIÓN DE LA PRUEBA VITUAL Y SU VALOR PROBATORIO

La prueba virtual es un medio para lograr acreditar la comisión de algún delito informático, "...ya que en la práctica se cometen en este ámbitos errores frecuentes. dejando de transcurrir, por ejemplo, los plazos de denuncias, no prohibiendo inmediatamente al supuesto autor la entrada de la empresa sino permitiéndole que continúe ocupando su lugar de trabajo y de esta forma tenga la

oportunidad de destruir medios de prueba...".[85], esto es así por que el autor aprovechando de su conocimiento puede en cualquier momento, sin ninguna seguridad previa, destruir archivos o información que involucre la comisión del delito realizado, y es a base de la prueba virtual , que es una prueba intangible, poder acreditar el delito; es por eso que existe una tarea de importancia, y mas por los tiempos actuales, legislar sobre su aplicación y valoración en materia penal.

La apreciación o valoración de la prueba es el mérito que le otorga el Juez a la forma como las partes intentan demostrar los hechos, conforme a los medios permitidos en la Ley. La Doctrina señala que la valoración de la prueba proviene de los conocimientos del Juez, y que estos le llevan a precisar el mérito de la prueba, es decir, en la eficacia de la misma. El Juez emitirá su decisión conforme a la convicción que obtenga de las pruebas dadas por las partes, luego de analizar cada una de ellas siguiendo las normas relativas a la manera de valorarlas.

Se reconoció en el **Código Federal de Procedimientos Civiles** como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: **La fiabilidad del método para generar, comunicar, recibir o archivar la información** (que pueda conservarse sin cambio), **su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas.** Asimismo y para que la información generada, comunicada, recibida o archivada por medios electrónicos se considere como original (para su conservación o presentación) deberá acreditarse que dicha información se ha mantenido **íntegra e inalterada** a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

[85] MIR, Puig Santiago, Op Cit, p.37

En el **Código de Comercio** se definió el concepto "Mensaje de Datos" como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

Y se reconoce como prueba a los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la **fiabilidad del método** en que haya sido generada, archivada, comunicada o conservada

Para un mensaje de datos en el que se consigne contratos, pueda considerarse legalmente válido, es necesario asegurar que la información en él contenido reúna las siguientes características.

Integridad:

Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada. Al respecto la Secretaría de Economía elaboró una Norma Oficial Mexicana que establece los requisitos que deben observarse para la conservación de mensajes de datos, con fundamento en lo dispuesto por el artículo 49 segundo párrafo del Código de Comercio. El martes 19 de marzo del 2002 se firmó el texto final de la NOM, el cual fue publicado el DOF el día 4 de junio del 2002, para su entrada en vigor se requiere de existencia de infraestructura y publicación de aviso en el Diario Oficial de la federación.

Atribución:

Es la forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios.

Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es mas que una "firma electrónica" la cual puede ser de dos tipos:

Simple definida como los datos en forma electrónica consignados en un mensaje de datos, o adjuntos o lógicamente asociados al mismo, que puedan ser utilizados para identificar al afirmante en relación con el mensaje de datos (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes)

Avanzada que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste (entendida como proceso electrónico que permite al receptor de un mensaje de datos únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

Para esto se hizo necesaria la legislación federal relativa a la firma electrónica "avanzada" en la que se regule la actividad de los prestadores de servicios de admisibilidad y forma de presentar como prueba en juicio a los mensajes de datos, procurando preservar la independencia tecnológica

Accesibilidad:

Se refiere a que el contenido de un mensaje de datos en el que se consignen contratos, pueda estar disponible al usuario (emisor, receptor, juez, auditor,

autoridades, etc.) para ulterior consulta, siempre y cuando reúna las dos características anteriormente anotadas. Para ello será necesario establecer, en la legislación federal que al efecto deberá emitirse, la forma de presentar a "los usuarios" estos mensajes de datos, la cual podría hacerse previa certificación de atribución e integridad por parte del prestador de servicios de certificación.

Ahora bien, es importante recalcar que el medio físico a través del cual el contenido de un mensaje de datos se pone a disposición del usuario puede ser diferente de aquél en que se creó, ya que se debe garantizar la integridad del mensaje de datos, no del medio físico que lo contiene. Esto es, que el mensaje puede estar contenido en el disco duro de una computadora y ponerse a disposición del usuario en un diskette, el copiarse a ese medio físico distinto al en que fue creado no lo hace de ninguna manera perder integridad.

Mediante Reformas de fecha 17 de mayo del 2000 publicadas en el Diario Oficial de la Federación, se crearon en la especie, los artículos 211 bis 1 al 211 bis 7 al Código Penal Federal, que en lo medular, tipifican comportamientos -de los llamados *hackers* o *crackers*- que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. En este cuerpo normativo federal se sancionan el que un sujeto tenga acceso ilegal a dichos sistemas y los altere, dañe, modifique o provoque pérdida de información contenida en tales sistemas.

Se trata de formas que establecen aspectos de forma y no de fondo, estos es, no se abordan o innovan cuestiones de procedimientos, formalidad o pruebas en materia de delitos informáticos.

La complejidad de la "prueba en informática" requerirá de un alto grado de conocimientos técnicos, por lo que - previa motivación y fundamentación - el abogado de la parte ofendida o el C. Agente del Ministerio Público, seguramente tendrá que apoyarse en un ingeniero en informática para que este realice las

técnicas necesarias para robustecer e impulsar las evidencias identificado en un sistema de informática, con el fin de acreditar plenamente el cuerpo del delito probable.

En el mejor de los casos, asegurar ante Notario Público o mediante decomiso debidamente autorizado, la computadora y memorias externas (DVD, compact disck, etc.) que utilizó el sujeto activo, para:

- Poder garantizar que su contenido, no sea alterado o modificado para la investigación forense;
- Que la parte ofendida o la autoridad ministerial con el auxilio de perito especializado rastreé en el CPU, en el *floppy disk*, en el disco duro o en la memoria RAM de la computadora, alguna señal sobre las operaciones realizadas por el *hacker o cracker*;
- Que la parte ofendida o la autoridad ministerial con el auxilio de perito especializado rastreé algún vestigio (cookies) sobre los hábitos de navegación en Internet del delincuente, realizadas por el *hacker o cracker*;
- Que tales evidencias sean acreditables objetivamente, por lo que será necesario el practicar un inventario informático de las mismas, ordenar un respaldo (back up) y dar fe pública de estos.
- Tal vez, se estará ante una prueba colegiada porque seguramente deberán robustecerse los elementos de convicción obtenidos, con la credibilidad y veracidad de la probanza que por su parte, practiquen los peritos autorizados y certificados por el Tribunal Superior de Justicia del Distrito Federal o el Poder Judicial Federal. [86]

Que de no existir las herramientas legales adecuadas para que ante la autoridad competente, la parte ofendida denuncie y acredite con pruebas tales

[5] Cfr. www.delitosinformaticos.com. Consultado en fecha 10 de Diciembre de 2004

hechos o para que las autoridades penales los sancionen, entonces se facilita en gran medida la labor de los abogados defensores o bien, se favorece la impunidad.

Este es tan sólo un ejemplo hipotético de lo que hoy en día, con fines enunciativos y no limitativos, puede tener lugar en el escenario virtual del Internet.

Efectivamente, al día de hoy se está dando un enfrentamiento intelectual de épocas, en el que los estudiosos de los delitos informáticos que pertenecen a nuevas generaciones de abogados, pugnan por darles un tratamiento doctrinal especializado, con criterios recogidos del mundo del Internet y que por su alcance técnico, no resultan familiares a los Jueces Penales.

Las reformas penales del 17 de mayo del 2000 publicadas en el Diario Oficial de la Federación, con las que se crearon los artículos 211 bis 1 al 211 bis 7 al Código Penal Federal, son plausibles pero insuficientes. Es necesario el crear nuevos tipos penales en los que se describan la variedad de comportamientos ilícitos que hoy en día, se ejecutan en el escenario virtual del Internet, es decir, el establecer ¿el que?.

Es apremiante el establecer en ley, las normas procesales que permitan: la solicitud, la práctica, la preparación, el tratamiento, el aseguramiento y el desahogo (¿el cómo?) de las "pruebas en informática", a fin de que en el momento oportuno sean practicadas conforme a Derecho.

4.4. DILIGENCIAS INVESTIGATIVAS

El especial modus operandi de esta clase de conductas, es lo que las hace particularmente difíciles de pesquisar. Es por éstas consideraciones que para su esclarecimiento, no bastan los métodos clásicos de criminalística sino que se

requiere el manejo de conocimientos en el área informática, y la colaboración de unidades especializadas en el tema.

No obstante es posible dar ciertas orientaciones generales, que podríamos denominar de primeras diligencias ante un delito informático:

a) Ordenar expresamente la incautación del ordenador atacado a fin de evitar toda intervención de personas extrañas en el o los sistemas automatizados de tratamiento de información afectados por el ataque, puesto que los referidos sistemas son el eslabón de inicio en la investigación ya que de ellos se pueden obtener datos relevantes tales como hora de ingreso al sistema, fecha, número de IP, etc.

b) Luego de identificado el número de IP del atacante se puede determinar el ISP al cual pertenece dicho número. Acto seguido se debe requerir los registros que lleva el ISP en cuanto a los usuarios que se conectaron a la fecha y hora del ataque, y a través de la correspondencia entre el número de IP, nombre usuario, y número de teléfono, requerir los datos personales del usuario.

c) El problema se puede dar respecto de los ataques que se realizan en lugares de 'tránsito' tales como los conocidos como café Internet, sitios en los cuales se puede arrendar por un cierto número de horas un ordenador, conectarse a la red y llevar a cabo el designio criminal. La dificultad radica en la identificación del agente, pues ella será más difícil. Por tanto en aquellos casos se deben utilizar técnicas de investigación pura tales como: perfiles de los hackers, descripción de posibles sospechosos, averiguar si se observó a alguien en conductas sospechosas como toma de datos, modus operandi, largas horas frente al ordenador, etc., pues se debe recalcar que los actos preparatorios para vulnerar un sistema de seguridad (paso previo para un ataque) requieren de horas. Es por esta razón que sería recomendable la manutención de un registro de las personas que hacen uso de dichos servicios.

d) Respecto de ataques que se efectúan a ciertos organismos, instituciones, o, empresas de importancia económica, estratégica, pública, etc., resulta útil averiguar la historia de empleados que hayan trabajado con anterioridad en tales organismos, circunscribiéndolo hacia aquellos en que pueda haber sospechas que hayan tenido motivos suficientes para atentar contra la institución en la que se empleó, pudiendo deberse, lo anterior, a diversas circunstancias siendo la principal: el término disconforme de su relación laboral. Así por ejemplo es común que empleados disgustados dejen insertas bombas lógicas para que se activen cuando sean borrados de la planilla de trabajadores, acarreando con ello la destrucción de la información contenida en su ordenador o de toda la red. No debe olvidarse, que las anteriores diligencias son meramente enunciativas pues la rapidez con que avanza el área de la informática, genera nuevas formas de comisión y, por ende, se hace necesario recurrir a maneras más novedosas de investigación.

Así como también, la colaboración judicial y policial en materia de cibercrimen (instrumentos internacionales factibles, dificultades derivadas del principio de territorialidad, las necesidades surgidas en relación con la extradición... con atención particularizada al ordenamiento comunitario). La conservación de datos de las telecomunicaciones a efectos de su utilización en la investigación penal.

La adaptación de medidas de investigación clásicas (registro, incautación, etc.) al ámbito específico de las telecomunicaciones; La participación de terceros privados en la investigación del cibercrimen (el papel de los proveedores de telecomunicaciones y de expertos en la materia, la posibilidad de compulsión a la colaboración, etc.)

El aseguramiento de la prueba electrónica (las dificultades de reproducción del material informático, el tratamiento de las copias de archivos informáticos, la supervisión judicial de la recogida de pruebas, la reproducción en el juicio oral).

La garantía de los derechos del inculpado al secreto de las comunicaciones y a la intimidad en el tratamiento procesal del cibercrimen.

4.5. LA INVESTIGACIÓN Y PERSECUCIÓN DEL DELITO

Nos dice Ulrich Sieber que "Las mayores dificultades de averiguación se encuentra en las manipulaciones del programa. Y es así por que la completa comprobación de un programa ajeno y la búsqueda de rutinas ilícitas que puedan hallarse escondidas en él, comporta una enorme cantidad de trabajo que desde el punto de vista económico generalmente es insostenible..."[87], lo anterior describe que la investigación es muy compleja y costosa, sin embrago existe una variedad de formas para su persecución y que el gobierno federal ha implantado organismos para la búsqueda de hechos informáticos ilícitos.

Por lo tanto, el gobierno mexicano ha formado en Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos formado por: la Procuraduría General de la República, la Procuraduría General de Justicia del Distrito Federal, la Policía Federal Preventiva, el Centro de Investigación y Seguridad Nacional, la Asociación Mexicana de Internet, la Secretaría del Trabajo y Previsión Social, la Secretaría de la Defensa y de la Marina, la Presidencia de la República, E-México, la Universidad Nacional Autónoma de México, Teléfonos de México, Avantel, Alestra y la Alianza Mexicana de Cybercafés, A.C..[88]

Dichas dependencias coordinadas unifican esfuerzos para la investigación y persecución de los actos ilícitos contra los sistemas informáticos, actuando con rapidez y precaución ante el desvanecimiento de datos necesarios para la localización del sujeto activo.

[87] MIR, Puig Santiago, Op Cit. p.33

[88] Cfr."EL REFORMA, Diario". Sección Interf@se. Accesando a la red. México, Distrito Federal. 2003

Una de las formas eficaces para la persecución de estos actos ilícitos es necesario el fomentar: programas de capacitación especializados en el tema, para los CC. Agentes del Ministerio Público y Jueces, impulsar la creación de plazas para los peritos en informática como auxiliares de las Procuradurías de Justicia Federal o Estatales, autorizaciones y certificaciones especiales para los Ingenieros en Informática o en Sistemas para que como peritos autorizados, auxilien a los abogados postulantes independientes y Jueces, así como procurar la celebración de tratados internacionales mediante los cuales, entre países, se convenga el auxilio mutuo para combatir y sancionar los comportamientos ilícitos por el ilegal aprovechamiento del Internet y sus herramientas virtuales.

4.5.1 LA POLICÍA CIBERNÉTICA

Ejerciendo sus atribuciones legales y para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Los crimenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de computo, el hackeo, la venta de armas y drogas por Internet y el ciberterrorismo las cuales son amenazas para la sociedad.

Tiene como misión:

- La identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.
- Realización de operaciones de patrullaje anti-hacker, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.
- Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Funciones de la Policía cibernética:

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos utilizando computadoras.

- Realización de operaciones de patrullaje anti-hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve:

- Integrar un equipo especializado en delitos cibernéticos a fin de hacer este medio electrónico un lugar seguro para el intercambio de información. Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciber espacio, así como su modus operandi.
- Utilizar Internet como un instrumento para identificar a los delincuentes que cometen este tipo de delitos.
- Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.
- Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.
- Ofrecer seguridad en la navegación en la Internet para los menores, ya que existen peligros en ella.
- Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.
- Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.
- Identificar y combatir el crimen organizado dedicado al tráfico de menores
- Establecer técnicas adecuadas para la búsqueda y localización oportuna de niños extraviados, perdidos y/o robados.
- Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.

4.6. AUDITORÍA INFORMÁTICA COMO MEDIO DE PRUEBA

En México existe una serie de auditorias fiscales realizadas a domicilio, auditando diversos documentos, archiveros y programas, por tal motivo y conforme a la actividad que realizan los auditores fiscales, es preciso realizar por parte del gobierno federal a sus dependencias de gran interés público, una auditoria informática, como prevención a hechos delictivos irreparables, evitando así una serie de sucesos ocasionados por agentes informáticos, así como también dar una seguridad jurídica informática a las funciones gubernamentales en sistemas de informática.

Con la auditoria de cuentas tradicional se podía conocer cómo se abastece la información del sistema informático y cual es el resultado del tratamiento dentro del mismo pero no lo que sucede entre esa entrada y salida de información, conocemos los "imputs" y los "outputs" pero no cómo se han generado estos últimos y si han sido objeto de alguna manipulación antes de hacerse visibles
El examen de lo que acontece en esas "cajas negras", que es lo que en realidad son los sistemas informáticos, se pueden lograr gracias a la Auditoria Informática.

Pero veamos que se entiende por Auditoria Informática, se define como: "...una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía, y la adecuación de la infraestructura informática de la empresa...".[89]

Ahora bien la Auditoria Jurídica de los entornos informáticos, significa una importante colaboración en la persecución del delito informático, en sus diferentes

[89] DEL PESO, Navarro Emilio, "Auditoria Jurídica de los entornos informáticos", informática y derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, No. 24-28, Abril 1995

modalidades, algo difícilmente de conseguir y asimismo puede servir de herramienta a la hora de obtener la prueba del fraude detectado.

Siguiendo a Del peso Navarro manifiesta que " las principales áreas en que puede trabajar este último de auditoria (Auditoría jurídica de los entornos informáticos), por supuesto en íntima relación con el que figura en el apartado b) – Auditoria de los propios sistemas informáticos -, son los correspondientes a : los datos de carácter personal, los programas de ordenador, las bases de datos y multimedia, los fraudes y delitos informáticos, los contratos informáticos y electrónicos, el intercambio electrónico de datos, la trasferencia electrónica de fondos, el documento electrónico, la red Internet, los seguros informáticos y dictámenes y peritajes informáticos.

1. La protección Jurídica de los programas de ordenador.

Un programa de ordenador se puede considerar cono un conjunto de materiales elaborados conceptualmente para la solución de un problema automatizado de datos.

Un programa de ordenador, como una creación de la mente que es, no un bien corporales o incorporales, ya que no puede ser incluido en ninguna de estas dos categorías, por que hay que acudir a una nueva, la de los bienes inmateriales, y que este se define de acuerdo a Del Peso Navarro: "...fruto de la mente para que se haga perceptible para el mundo exterior es necesario plasmarla en un soporte puede ser disfrutado simultáneamente por una pluralidad de personas...".[90]

Por tal motivo la realización de dichas auditorias, tiene como efecto si se realiza por parte del gobierno federal, la protección jurídica del funcionamiento de un sistema informático, y que a la vez puede ser utilizada en un proceso penal

[90] DEL PESO Navarro, Op. Cit. 617

como fuerza probatorio, expedida dicho auditoria por un organismo público, que le da autenticidad al momento de valorar la prueba de la Auditoria informática.

Ahora bien, la auditoria informática debe comprender ciertas áreas para verificar anomalías que perjudiquen o prevengan hechos delictivos a los órganos del Estado, dichas áreas pueden ser: Equipos, sistemas operativos y paquetes, aplicaciones y el proceso de su desarrollo, organización y funciones, las comunicaciones, la propia gestión de los recursos informáticos, la calidad de procesos y productos.

Estas áreas, o pueden ser más, son las que implican la organización y función de una institución del estado, por lo que una vez hecha la revisión debe emitirse un informa detallado por escrito que resuma la situación desde un punto de vista independiente y objetivo, y, en su caso dicho informe ha de incluir deficiencias o indicaciones de mejoras. Esto con la finalidad de garantizar un funcionamiento eficaz y una seguridad en el mismo, obteniendo un impacto favorable en la imagen de las entidades.

Así, el informe debe ser escrito en todos los casos, y debe ir firmado, así como:

- "En el debe constar los antecedentes, el objetivo del proceso de auditoría, los agradecimientos (si proceden), las posibles limitaciones, y un resumen ara la Dirección, en términos no técnicos.
- En cada punto que se incluya debe explicarse, siempre que sea posible, por qué es un incumplimiento o una debilidad, y alguna recomendación, a veces abarcando varios puntos.
- La entidad decide qué acciones tomar, y en el caso de los internos suele hacer también un seguimiento de las implantaciones".[91]

[91] RAMOS González Miguel Angel, "Auditoria Informática", Informática y Derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, No. 24-28, España, Abril 1995. P.676

Este tipo de auditoria ha sido hasta el momento actual ignorado en parte por intereses consolidados y en parte de su ausencia de los textos legales, pero a pesar de ello esta emergiendo con gran potencia.

CONCLUSIONES

CONCLUSIONES

PRIMERA.- El origen así como su desarrollo de la informática ha permitido la adquisición y transmisión de la información de manera eficaz y sencilla a base de la telemática, provocando que la misma información sea un bien activa, consumible; Teniendo una utilidad funcional en el manejo de la misma; entrando así a la era de la información y creando así una nueva sociedad informática, en el cual la información es poder.

SEGUNDA.- El Derecho mexicano no a contemplado, pero si considerado un derecho informático, en donde el derecho entra de igual manera a las tecnologías de la información, creando normas para el uso de la información y en el funcionamiento de un soporte informático, dando seguridad jurídica a los activos que utilizan dichos servicios.

TERCERA.- Los delitos informáticos, que en sí no han sido tipificados y por lo tanto aún no existe en la ley penal mexicano, por lo tanto es menester entrar a un estudio profundo en donde se reconozca tal denominación, para una identificación plena y no dando interpretaciones ambiguas que provoque la violación de garantías individuales de los gobernados, por tanto los delitos informáticos es ya una realidad que debe el derecho tomarlo en cuenta.

CUARTA.- La red de redes, es la forma de comunicación y obtención de la información, en donde viaja éste en todos sus formatos, sin embargo esta misma red global, existe individuos que vulneran sistemas informáticos a base de instrumentos de la misma naturaleza, provocando perjuicios trascendentes a los usuarios, por lo cual esta delincuencia, debe el derecho de penalizarlo, creando una cuerpo punitivo de estricto derecho y conforme a su naturaleza.

QUINTA.- Los tratados internacionales en relación a los delitos comunes, pero aún no contemplado aquellos delitos informáticos, es el caso del Tratado de libre

Comercio, que no reconoce estos delitos, sin embargo es necesario mas acuerdos externos que permitan dar un seguimiento jurídico para la aplicación de la ley en estos hechos ilícitos.

SEXTA.- En la Constitución de los Estado Unidos Mexicanos, existe la seguridad jurídica para todo gobernado en la aplicación de la ley penal, en donde es de estricto derecho, por lo tanto la aplicación de una ley a conductas que intervienen en un sistema informático es interpretada por analogía, vulnerando los derechos constitucionales.

SEPTIMA.- El Código Penal Federal describe ciertas conductas relacionadas a los sistemas informáticos, y estas conductas prohibitivas se enfocan al daño de la información, dejando al arbitrio al mismo soporte informático que es un bien funcional para que la primera funcione de manera eficaz; así mismo tipificar otras conductas innovadoras en relación a esta nueva delincuencia informática.

OCTAVA.- En las leyes comparadas, existen los delitos informáticos, en otros contempla conductas prohibidas a estos delitos, pero en sí estas leyes identifican los bienes mas vulnerados, como son la misma información y los soportes lógicos, a si como su forma de comisión, en tanto no se actualice la ley mexicana existirá arbitrariedades constitucionales.

NOVENA.- Para una identificación plena en la conducta de la vulneración ilícita contra el funcionamiento en los sistemas de informática a través de Internet, se desarrolla el cuerpo del delito, en su caso para su tipificación, desarrollando cada uno de sus elementos del hecho ilícito, dando un esquema para que este forma comisión llegue a estar en una ley penal.

DECIMA.- La conducta de este hecho ilícito, es a base de la utilización de instrumentos informáticos, en el cual, su forma de comisión es sola una, la introducción de estos a las redes informáticas, provocando serios pérdidas a los

sujetos pasivos; Otra característica de estas conductas es la forma de intervención en el sentido subjetivo, en cual el dolo, es también la única forma en el actuar, por lo tanto esta conducta, es ilícito cuando su cumpla estos dos elementos.

DÉCIMA PRIMERA.- El bien jurídico protegido, en relación a este delitos que se estudio, es el patrimonio, sin embargo como se dijo, también se puede considerar como la seguridad jurídica en el funcionamiento informático, ya que la información en sí entra a otra gama de supuestos ilícitos, que es necesario un cuerpo normativo especial, en donde la información, no es un bien económico adquisitivo sino un bien funcional adquisitivo.

DÉCIMA SEGUNDA.- La punibilidad de la comisión de estos hechos ilícitos, debe ser basándose en la infuncionalidad del sistema informático o de la misma red, o también sobre la base del sujeto pasivo, como son las instituciones del estado, o instituciones externos federales, por su forma de comisión, así como la seguridad que tiene para su inalterabilidad.

DÉCIMA TERCERA.- La acreditación del cuerpo del delito es a base de la prueba, que en México aun no se ha desarrollado abiertamente el uso de la prueba informática, en el cual ya ha sido regulado en materia civil, pero aún no en materia penal, ya que e existen dos problemas, su valoración jurídica y su ofrecimiento por parte de los litigantes que desconoce que peritos son los que pueden auxiliar para la identificación del delincuente.

DÉCIMA CUARTA.- Los tratadistas penalistas se han preocupado por la prueba informática, por la necesidad de dar soluciones a lo generados por la misma tecnología informática, tratando de crear procedimientos en su valoración y su aplicación, de las diversas pruebas que puedan ser utilizables, pero mas que nada se basa en el peritaje, que permite identificar la verdad histórica del hecho ilícito.

DÉCIMA QUINTA.- Existe una gama de peritajes, como se observo en el contenido del trabajo, que pueden ser la reconstrucción y modelización, instrumentación electrónica, informática forense, para la investigación de estos hechos ilícitos y localización de los sujetos, pero a su vez la forma de investigación y persecución del delito es más compleja que la misma prueba, pero como va avanzando la tecnología para su identificación del delincuente, la prueba informática será de gran valor o mejor dicho, la prueba mas eficiente.

DÉCIMA SEXTA.- Los peritos especializados con las nuevas tecnologías y que sirven de base para la investigación de los hechos ilícitos descritos y localización de los sujetos activos, suelen ser los licenciados en informática, ingenieros en computación, instrumentación electrónica y telecomunicaciones, diseño electrónico y programadores; pueden ser localizados en la Universidad Nacional Autónoma de México, Instituto Politécnico Nacional, Universidad autónoma de México, Instituto Tecnológico de Monterrey, etc.

DÉCIMA SÉPTIMA.- Es por todo lo anterior que la hipótesis planteada ha sido comprobada, es decir, que la vulnerabilidad en los sistemas de informática a través de Internet es trascendente en la esfera jurídica, y por lo tanto el derecho penal mexicano debe de tipificarlo dando seguridad jurídica a los usuarios, logrando disminuir daños irreparables a bienes aún no considerados en el Código Penal como son los sistemas lógicos; así mismo se cuenta con peritos capacitados que pueden ser considerados sus dictámenes como prueba.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

AZPILCUETA, Tomás Emilio, "Derecho Informático", Mac Graw- Hill. Buenos Aires, 137 pp

BARRIO, Garrido, Gabriela, "Internet y Derecho en México", Mac Graw – Hill, México, 180 pp

CASTELLANOS, Tena, Fernando., "Lineamientos Elementales de Derecho Penal", trigésima octava edición , Editorial Porrua, México 1997, 353 pp.

CERVANTES, Martínez, Jaime Daniel, "Justicia Cibernética como Alternativa ante el nuevo Milenio", Cárdenas, México, 598 pp

C. J. A. MITTERMAIER, "Tratado de la Prueba en Materia Criminal", Angel Editor, México, 1999, 573 pp.

DAVARA, Rodríguez Miguel Angel, "De las Autopistas de la Información a la Sociedad Virtual", Aranzandi 1996, Pamplona España, 191 pp

DAVARA, Rodríguez Miguel Angel, "Manual de Derecho Informático", Cuarta edición, Aranzandi 2002, Pamplona España, 480 pp.

DE LA CRUZ, Agüero, Leopoldo, "Procedimiento Penal Mexicano", Porrúa, tercera edición, 1998, México, 199 pp.

DIAZ, Aranda Enrique, "DOLO Causalismo-Finalismo-funcionalismo y la reforma penal en México", Editorial Porrua, Tercera Edición, México 2001, 264 pp.

HUERTA, Miranda Marcelo, *et al*, "Delitos Informáticos", segunda edición, Jurídica Conosur Ltda, 1998, Santiago de Chile, 361 pp.

LAGARES, Garcia Diego, Internet y Derecho ; Tecnología y Jurisprudencia: Dos Conceptos Obligados a Entenderse, Careria, 145 pp

LIANEZA, González Paloma, "Internet y Comunicación digitales; Regimen legal de las Tecnologías de la Información y la Comunicación", Bosh 2000, Barcelona España., 450 pp

MIR, Puig Santiago, "Delincuencia Informática", Promociones y publicaciones universitarias, 1992, Barcelona España, 182 pp

ORTS, Berenguer Enrique y Roig Torrez Margarita, "Delitos Informáticos y Delitos Comunes cometidos a través de la Informática", Tirant Lo Blanch 2001, España, 195 pp.

RIESTRA, Gaytan, Emma, "Curso Introductorio a los Delitos Informáticos", Impacto Tecnológica en la sociedad, Cuaderno de la PGR, 180 pp.

SANDER, H. Donald. "Informática: Presente y Futuro. México", Edit. MacGraw-Hill, 1987, 210 pp.

SANCHEZ, Crespo Carolina, "La Prueba por Soportes Informáticos", Tiran Lo Blanch. 176 pp.

TÉLLEZ Valdés, Julio, "Derecho Informático", México, Edit.McGraw-Hill, México 1998. 120 pp.

ZAFFARONI, Eugenio Raúl, et al, "Derecho Penal", parte general. Porrúa, México 2001, 1017 pp.

ZAFFARONI, Eugenio Raúl, "Manual de Derecho Penal", parte general. Segunda edición, México, Cárdenas, 1988, 825 pp.

DICCIONARIOS

Diccionario de la Lengua Española Larousse, Primera Edición, México, 1994. P. 176.

Diccionario de la Lengua Española, Real Academia Española, Vigésima segunda edición, 2001.

Gran Diccionario Enciclopédico Asuri. Dir. Lorenzo Portillo Sisiniega, v.4, España, 1989, 1497 pp.

Diccionario Jurídico Temático", Dir. Leonel Pereznieto Castro, V.6, México, 2000, 98 pp.

HEMEROGRAFÍA

HEMEROGRAFÍA

CARRASCOSA, López Valentin, "Regulación Jurídica del Fenómeno Informático", Informática y Derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, Abril 1998

Corport: México Academia Mexicana de Ciencias, México Frente a la Era de la Información, Academia Mexicana de Ciencias, México, 59 pp

DEL PESO, Navarro Emilio, "Auditoria Jurídica de los entornos informáticos", informática y derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, No. 24-28, Abril 1995

GOMEZ, Sánchez Navarro, "Nueva Legislación sobre delitos Informáticos", Revista Mexicana de Justicia, Nueva Época, No. 8, 1999, México, D.F.

NIELSON R. Daniel, "Los casos mas usuales de Criminalidad Informática y Cibernética", Catalana de Seguritat, Barcelona España., Num. 3, Diciembre 1998,

ROMEO Casabona Carlos, "Llamados Delitos Informáticos", Informática y Derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, No. 24-28, Abril 1995.

RAMOS González Miguel Angel, "Auditoria Informática", Informática y Derecho, Universidad Nacional de Educación a Distancia, Centro Regional de Mérida, No. 24-28, España, Abril 1995.

ROSA, Pacheco Guillermo, "Derecho a la Informática Jurídica", Estudios Jurídicos, Universidad Intercontinental, México, D.F., Año 1, No. 1, Enero 1991, 75-87 pp

SALT Marcos, "Delitos Informáticos", Justicia Penal y Sociedad, Revista Guatemalteca de Ciencias Penales, Año 4, No. 6, Abril de 1997, 49-69 p.

TAMBURRINI, Pietro, "Computer Crimes en Italia", Derecho de la Alta Tecnología, Italia, Año VIII, No. 88-89, Diciembre 95 / Enero 96

ORILLA Bueno Rocio, "Internet y Derecho de la Realidad Virtual a la Realidad Jurídica", Boletin Mexicano de Derecho Comparado, V.31, No. 92, Mayo- Agosto 1998, 421-438.pp

ZEDILLO Ernesto, "Las tecnologías de la información son un instrumento de la mayor importancia para la superación productiva de nuestro país y el bienestar de sus habitantes", (Discurso del Presidente de la República durante la ceremonia de instalación de la Comisión Nacional de Conversión Informática Año 2000), Los Pinos, México D.F., 3 junio 1998, Edit. Presidencia de la República, 10 p.

PAGINAS DE INTERNET

http://iteso.mx/~gcorona/red_telematica.htm. Consultado en fecha 21 de Abril de 2005.

http://www.iua.upf.es/~jblat/3d_esp.html. Consultado en fecha 20 de Mayo de 2004.

http://www.internet-solutions.com.co/forense.html. Consultado en fecha 25 de Agosto de 2004.

http://www.seei.org/Anuncios/amaya.htm. Consultado en fecha 15 de Septiembre de 2004.

http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node275.html. Consultado el 18 de Septiembre de 2004.

http://buscon.rae.es/diccionario/drae.htm Consultado en fecha 24 de Septiembre de 2004.

http://www.delitosinformaticos.com. Consultado en fecha 10 de Diciembre de 2004.

LEGISLACIÒN

LEGISLACIÓN

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

Constitución de los Estados Unidos Mexicanos, 3 Leyes para el Distrito Federal, Sista, 2003, 100 p.

Código Penal Federal, Edit. ISEF, 2003. 129.pp

Ley Federal de Telecomunicaciones, Ediciones Delma, 455-479 pp.

Reglamento de Telecuminicaciones, Ediciones Delma 481-537 pp.

Ley de Información Estadística y Geografía, RIESTRA, Gaytan, Emma, "Curso Introductorio a los Delitos Informáticos", Impacto Tecnológica en la sociedad, Cuaderno de la PGR, 180 pp.

Código Penal del Distrito Federal, Edit. Sista, 2005. 3 Leyes para el Distrito Federal, Sista, 2003, 100 p.

Código Penal de Sinaloa, Edit Anaya, 1996

Exposición de Motivos de la Comisión de Justicia de la Cámara de Diputados, para reformar el Código Penal Federal, en el que se agregan los artículos 211 bis 1 hasta artículo 211 bis 7, en materia de Delitos al Acceso Ilícito a Sistemas y Equipos de Informática, Publicado en el Diario Oficial de la Federación el 17 de Mayo de 1999.