UNIVERSIDAD AMERICANA DE ACAPULCO

EXCELENCIA PARA EL DESARROLLO

FACULTAD DE DERECHO
INCORPORADA A LA UNIVERSIDAD
NACIONAL AUTONOMA DE MEXICO

TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN MÉXICO

T E S I S

QUE PARA OBTENER EL TITULO DE LICENCIADO EN DERECHO

P R E S E N T A:

JESÚS AGUIRRE SALAS

DIRECTOR:
DR. JESÚS MARTÍNEZ GARNELO

ACAPULCO, GRO. FEBRERO DE 1999

PAGINACION

DESCONTINUA

Dedicatoria . . .

A Dios
Nuestro creador.

A mis Padres
Maximina y Jesús

A mi Abuelita
Engracia Vega García
Que en Paz Descanse

A mis Hermanos
Vicky y Jorge.

A mi Tía Josefina
Y demás Familiares

A la Universidad Americana de Acapulco
Nuestra Alma Mater.

A la Facultad de Derecho
Y sus Directores.

A mi Asesor de Tesis
Dr. Jesús Martínez Garnelo.

A nuestros Profesores.
A todos y cada uno de ellos.

A mis Compañeros de Generación
Con especial afecto a:
Flores Sánchez, Aquiles
Hernández Pérez, Giancarlo

INDICE

PAGS.

INTRODUCCIÓN.

CAPITULO I.
ANTECEDENTES HISTORICOS DE LAS COMPUTADORAS.

1.1. EVOLUCION DE LAS COMPUTADORAS. 01
1.2. GENERACIONES EN LAS COMPUTADORAS. 03
PRIMERA GENERACIÓN (1951-1958). 03
SEGUNDA GENERACIÓN (1959-1964). 04
TERCERA GENERACIÓN (1965-1970). 04
CUARTA GENERACIÓN (1971-1980). 04
QUINTA GENERACIÓN (1981-?). 05
1.3. COMPONENTES BÁSICOS DE LAS COMPUTADORAS. 06
PROGRAMACIÓN Y SOFTWARE. 08
1.4. CLASIFICACIÓN DE LAS COMPUTADORAS. 09

CAPITULO II
PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTO.

2.1. NOCIONES GENERALES. 11
2.2. PROTECCIÓN MEDIANTE LA VÍA CIVIL. 12
2.3. PROTECCIÓN MEDIANTE LA VÍA PENAL. 14
2.4. PROTECCIÓN MEDIANTE LA VÍA DE DERECHO DE AUTOR. 17

CAPÍTULO III
LOS DELITOS INFORMÁTICOS.

3.1. GENERALIDADES. 23
3.2. CONCEPTO DE DELITO INFORMÁTICO. 23
3.3. CARACTERÍSTICAS. 25
3.4. CLASIFICACIÓN. 26
3.5. ANÁLISIS DE LOS ELEMENTOS DEL DELITO INFORMÁTICO. 29
3.5.1. La conducta y su elemento negativo. 30
3.5.2. La tipicidad y su elemento negativo. 34
3.5.3. La antijuridicidad y su elemento negativo. 37
3.5.4. La culpabilidad y su elemento negativo. 39
3.5.5. La imputabilidad y su elemento negativo. 42
3.5.6. La punibilidad y su elemento negativo. 43
3.5.7. La condicionalidad objetiva y su elemento negativo 45

CAPITULO IV.
INTERNET Y EL DELINCUENTE INFORMATICO.

4.1. NOCIONES GENERALES 46
4.2. CARACTERISITICAS DEL DELINCUENTE INFORMATICO. 47
4.3. FORMA BASICA DE OPERAR DE UN DELINCUENTE INFORMATICO. 48
4.4. HACKING/ CRACKING/ PHREAKING EN EL CÓDIGO PENAL ESPAÑOL. 48
4.5. CASOS FAMOSOS DE ALGUNOS DELITOS INFORMATICOS Y SUS AUTORES 50
4.6. EL CRIMEN INFORMATICO. 51
4.7. RESUMEN DEL COMUNICADO DE LA COMISION AL PARLAMENTO EUROPEO. 52
4.7.1. Argumentos a favor de la regulación técnico-jurídica en Internet 53
4.7.2. Argumentos en contra de la regulación técnico-jurídica en Internet. 53
4.7.3. Autorregulación: códigos de conducta, sistemas de seguridad informática y los ciberpolicías. 54

CAPÍTULO V
LEGISLACIÓN EN MATERIA DE DELITOS INFORMÁTICOS.

5.1. LEGISLACIÓN NACIONAL. 55
5.1.1. MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA. 56
A). PRIMER EVENTO. CIUDAD DE VERACRUZ, VER., 18 DE SEPTIEMBRE DE 1996. 56
B). SEGUNDO EVENTO. CIUDAD DE GUADALAJARA, JAL., 20 DE SEPTIEMBRE DE 1996. 57
C). TERCER EVENTO. CIUDAD DE MONTERREY, N.L., 25 DE SEPTIEMBRE DE 1996. 57
D). CUARTO EVENTO. CIUDAD DE TIJUANA, B.C., 27 DE SEPTIEMBRE DE 1996. 58
E). QUINTO EVENTO. CIUDAD DE MÉXICO, D.F., 4 DE OCTUBRE DE 1996. 58
5.1.2. CODIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA. 59
5.2. LEGISLACIÓN INTERNACIONAL. 61
5.2.1. ORGANISMOS INTERNACIONALES.
A). LA ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE) 61
B). LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) 62
C). LA ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL. 63
5.2.2. LEGISLACIÓN EN PAISES EXTRANJEROS 63
A). ALEMANIA. 64

B). AUSTRIA. 65
C). FRANCIA. 65
D). ESTADOS UNIDOS. 66
5.2.3. TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE (TLC) 68
5.2.4. ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCIAS FALSIFICADAS. 72
5.2.5. EXTRACTO DE LA LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE DEL CÓDIGO PENAL DE ESPAÑA. 73

CAPITULO VI
PROCEDIMIENTO, JURISDICCIÓN Y COMPETENCIA.

6.1. EL PROCEDIMIENTO PENAL. 80
6.2. EL PROCESO PENAL. 81
6.3. LA PRUEBA. 83
A).- LAS PRUEBAS DIGITALES. 84
B).- LOS SISTEMAS DE IDENTIFICACIÓN. 84
C).- SNIFFERS. 85
D).- OBSTACULOS. 85
6.4. LA PERITACIÓN. 86
6.5. EL EXHORTO. 89
6.6. LEY DE EXTRADICIÓN INTERNACIONAL. 92
6.7. LA JURISDICCION. 95
6.8. COMPETENCIA JURISDICCIONAL EN INTERNET. 96
6.9. LOS JUECES FEDERALES PENALES 103
6.10. EL MINISTERIO PUBLICO FEDERAL. 106

PROPUESTA. 111

CONCLUSIONES. 113

SECCIÓN DE ANEXOS. . . . . I-XXXI

BIBLIOGRAFIA.

INTRODUCCIÓN

El amplio desarrollo tecnológico ofrece aspectos benéficos a la sociedad, a través de los medios de comunicación y el uso de las computadoras, cuya aplicación se canaliza a sectores académicos, científicos, médicos, en la economía, entre otros, sin embargo, también se generan las conductas delictivas derivadas de ese gran avance tecnológico, sobre todo en el campo de la informática. Por ello, es necesario que se atiendan y regulen jurídicamente, las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Podemos definir someramente al derecho informático como el conjunto de normas jurídicas tendientes a regular la propiedad, uso y abusos de los equipos de cómputo y de los datos transmisibles en forma electromagnética.

Los delitos informáticos (llamados también delitos cibernéticos) han sido definidos por la organización para la cooperación económica y el desarrollo, como: "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos". Ya en esta definición podemos encontrar elementos de valoración ética que son trascendentes para el derecho penal. Los países avanzados han estatuido ordenamientos jurídico-penales respecto a los delitos informáticos, e incluso han celebrado tratados internacionales para enfrentar a este tipo de delincuentes, llamados también delincuentes informáticos o cibernéticos.

Entre las conductas ilícitas, denominadas delitos informáticos podemos encontrar las siguientes:

- Acceso no autorizado a base de datos o información.
- Destrucción de datos.
- Infracción de los derechos de autor.
- Infracción del Copyright de bases de datos.
- Interceptación de e-mail.
- Estafas electrónicas.
- Transferencias de fondos.
- Espionaje.
- Espionaje industrial.
- Terrorismo.

- Narcotráfico.
- Tráfico de armas.
- Proselitismo de sectas.
- Propaganda de grupos extremistas.
- Correo electrónico.
- Difusión del material pornográfico.
- Pornografía infantil.
- Publicidad engañosa.
- Injurias y calumnias.
- Seguridad y ataques a sistemas informáticos.
- Estafas.
- Propiedad intelectual.
- Protección a la intimidad personal.

La presente investigación, la desarrollamos de acuerdo a los siguientes rubros y se obtuvo en gran parte a través de Internet, por haber pocos libros en México que estudian este tema.

En el capítulo primero, estudiaremos los antecedentes históricos relativos al nacimiento de los ordenadores, desde el ábaco hasta las modernas computadoras, sus generaciones, sus componentes básicos y su clasificación.

En el capítulo segundo, analizaremos un apartado especial, denominado protección jurídica de los programas de cómputo, en el cual veremos las diferentes vías de protección jurídica en México de los software (programas) a saber; la vía civil, penal y el derecho de autor.

En el capítulo tercero, entramos al desarrollo de los delitos informáticos, la dificultad y complejidad para conceptualizarlos, sus características, su clasificación y el análisis de sus elementos como delito.

El capítulo cuatro, trata del delincuente informático (o sujeto activo del delito) sus características (calidad de garante), las formas básicas de operar (comisión del delito), se incluye el tema de hacking/ cracking/ pheaking en el código penal español y algunos casos de gran importancia de delitos informáticos y sus autores.

En el capítulo cinco, analizamos las diferentes legislaciones en materia de delitos informáticos, comenzando por la nuestra, y después a nivel internacional, exponiendo las diversas y complejas leyes que han expedidos los países mas avanzados para contrarrestar las acciones ilícitas derivadas del mal uso o manejo de las computadoras.

En el capítulo sexto, estudiaremos algunos conceptos de gran relevancia relativos a los delitos informáticos y que han implicado gran complejidad en su estudio a nivel transnacional, iniciando con la jurisdicción para conocer tales delitos, que jueces tiene competencia, la intervención del ministerio público federal, disposiciones en materia de peritos, cuestiones relativas a los exhortos en tratándose de delincuentes informáticos hasta llegar a un somero análisis de la ley de extradición internacional.

Y para terminar, proponemos la estructura del tipo penal de los delitos informáticos a nivel federal, al igual que manifestamos nuestras conclusiones finales de la presente tesis.

CAPITULO I
ANTECEDENTES HISTORICOS DE LAS COMPUTADORAS.

SUMARIO: 1.1. EVOLUCION DE LAS COMPUTADORAS. 1.2. GENERACIONES EN LAS COMPUTADORAS. Primera Generación (1951-1958). Segunda Generación (1959-1964). Tercera Generación (1965-1970). Cuarta Generación (1971-1980). Quinta Generación (1981-?). 1.3. COMPONENTES BÁSICOS DE LAS COMPUTADORAS. Programación y Software. 1.4. CLASIFICACIÓN DE LAS COMPUTADORAS.

1.1. EVOLUCION DE LAS COMPUTADORAS.[1]

Es importante hacer una somera referencia histórica de las herramientas manuales y electrónicas conocidas como computadoras, a efecto de conocer a grandes rasgos su evolución y desarrollo, ya que en la actualidad son el instrumento de trabajo electrónico de mas importancia en el planeta, por lo que para conocer el progreso e impacto que tiene esta herramienta en el presente, es necesario analizar su proceso histórico.

Se puede afirmar que la historia de la computación inicia a partir de que el hombre se ve en la necesidad de ordenar numéricamente sus ideas; es decir, a partir del nacimiento de la contabilidad. Con el transcurso del tiempo, el ser humano tenía la problemática de plasmar en un determinado objeto, los conocimientos numéricos que *poseía*; y *es ahí donde empieza a utilizar* primeramente las piedras, papiro, papel etc., hasta llegar a perfeccionar la Ciencia de la Contabilidad.

El primer instrumento para ayudar a contar fue el ábaco. Se construyó en Babilonia hacia el 3000 a. de C. Aunque no existe evidencia que pueda asegurarlo, se dice que los conceptos más importantes en el funcionamiento de una computadora que consisten en repetir y programar, nacen en los instrumentos musicales conocidos como el organillo y la pianola, ya que se simplificaba el esfuerzo humano para realizar tareas repetitivas, en razón de que dichos instrumentos contaban con instrucciones detalladas en su procedimiento, a efecto de repetir de manera indefinida y automática un mismo proceso.

---

[1] Esta sección por tratarse de un recuento general, se basa en los siguientes trabajos: a). Fix Fierro, Héctor. Informática y documentación jurídica. 2da. Edición, UNAM, México, D.F. 1996. Pág. 44-45. b). IBM de México. Historia de la computación. IBM México, 1987, Pág. 114. c). Téllez Valdez, Julio. Derecho Informático. 2da. Edición. *Editorial McGraw-Hill. México 1996, Págs. 5-10.* d). H. Aiken, Ch. Babbage, J. Von Neumann, C.E. Shannon, A.M. Turing, W.G. Walter y otros. Perspectivas de la revolución de los computadores. Selección y comentarios de Zenon W. Pylyshyn. Editorial Alianza. 1994.

La primera computadora se invento en Francia en 1642 y la construyó el científico francés Blaise Pascal a los 19 años. La calculadora funcionaba bien, pero sólo podía sumar y restar. La primera máquina que pudo multiplicar y dividir la inventó el científico Alemán Gotteried Leibntz en 1694. Más sin embargo, desde el ábaco la humanidad tardó casi cinco milenios en pasar de este ingenioso y a la vez primitivo artefacto a lo que se considera el prototipo de las computadoras modernas.

El matemático e inventor Inglés Babbage, creó en 1834 los primeros diseños de la Calculadora Analítica que lleva su nombre. Sólo hasta 1854 George Pehr Schuetz llevó a la práctica un modelo de la máquina de diferencias. Las teorías de Babbage se utilizaron posteriormente por los ingenieros que construyeron las primeras computadoras. En 1842 se tradujo del italiano al inglés un artículo de L. F. Menabrea. que versaba sobre la máquina analítica.

En la década de 1880, el U.S. Census Bureau (departamento censal de E.U.) pidió a Herman Hollerith que desarrollara un método para obtener mayor velocidad en el procesamiento de los datos del Censo. Hollerith creó tarjetas perforadas que semejaban las tarjetas actuales de computadora, su código y el equipo de tabulación. En 1937, se desarrolló una computadora en la Harvard University por parte de H. H. Aiken, este aparato, el MARK I, fue un prototipo o antecesor de las computadoras actualmente utilizadas. Esta máquina electrónica fue desarrollada bajo la supervisión de John V. Atanasoff y constituyó las bases de ENIAC (electronic numerical integrator and calculator: integrador y calculador numérico electrónico), que hizo su aparición en 1946.

Durante la 2da. guerra mundial se empleó una computadora denominada "colossus" para descifrar las transmisiones alemanas, y ayudar a planear estrategias de los aliados. El matemático John Von Neumann elaboró varios comunicados sobre el concepto de programa almacenado. En 1949, este concepto se integró a la computadora EDSAC (electronic delay storage automatic computer: computadora automática de almacenamiento electrónico demorado), los avances en la tecnología de cómputo proliferaron durante la primera parte del decenio de 1950.

En 1951, el aparato UNIVAC 1 (universal automatic computer : computadora automática universal), se presentó y se constituyó en la primera computadora comercial disponible. El principio de la década de 1950 trajo también el desarrollo y la aceptación de las cintas magnéticas, un gran avance tecnológico.

La era posterior al lanzamiento del primer SPUTNIK, de 1959 a 1965, trajo consigo la segunda generación de computadoras. Utilizaban transistores y por lo tanto eran menos voluminosas y podían almacenar más información. Entre 1959 y1965, el disco magnético de alta velocidad se desarrolló y se lanzó al mercado.

A mediados de la década de 1960, la tercera generación de computadoras hizo su aparición y convirtió a la computadora en un auxiliar esencial para las empresas. En 1970, IBM lanzó su serie de computadoras 370. Utilizaban chips de silicio que tenían únicamente ocho centésimas de una pulgada cuadrada. La primera minicomputadora desarrollada por Digital Equipment Corporation, se puso en el mercado en 1965. El desarrollo del chip de las computadoras precedió el desarrollo de la microcomputadora.

Los avances tecnológicos permiten en la actualidad a las microcomputadoras la exhibición de datos a color, la fijación de datos en archivos de disco y el uso de sintetizadores de voz para "platicar" con sus usuarios. Las redes de computo distribuidas, se construyen en la actualidad con microcomputadoras y minicomputadoras, tan buenas como con sistemas convencionales de cómputo. Asimismo, la tecnología del LÁSER ha demostrado en forma experimental que es posible que una computadora mantenga trillones de caracteres de datos en un formato inmediatamente recuperable. Los nuevos sistemas de cómputo reflejan el deseo de las industrias de obtener equipos económicos y eficientes.

Como se puede observar, no es sino hasta la Segunda Guerra Mundial, cuando se presenta de manera significativa y apresurada el desarrollo de la informática, principalmente porque los científicos de la época tenían que invertir gran cantidad de tiempo para realizar sus investigaciones y estudios, a efecto de realizar cálculos matemáticos exactos y en el menor tiempo posible. A partir de aquí podemos hablar de las Generaciones de las computadoras.

1.2. GENERACIONES DE LAS COMPUTADORAS.[2]

PRIMERA GENERACION (1951-1958).

La primera generación de computadoras empleó tubos de vacío como elemento lógico principal. También se apoyó fuertemente en el uso de las tarjetas perforadas y el almacenamiento interno en tambor magnético. Posteriormente, los programas se escribían en lenguaje de máquina o en lenguaje ensamblador. La mayoría de las computadoras comerciales de la primera generación estaban limitadas a aplicaciones de tipo contable, debido a que éstas eran relativamente fáciles de "justificar" en términos de costos.

Entre sus principales características encontramos que estas computadoras trabajan mediante válvulas o bulbos al vacío (características que la diferencian de las demás

[2] Esta sección por tratarse de un recuento general, se basa en los siguientes trabajos: a). Mora Enzo Molino, José Luis. Introducción a la Informática. Editorial Trillas, México 1973. Pág. 117-121. b). Fix Fierro, Héctor. Informática y Documentación Jurídica. 2da. Edición 1996. UNAM, México D.F. c). Téllez Valdez, Julio. Derecho Informático. 2da. Edición. Editorial McGraw-Hill. México 1996, Págs. 9-10.

generaciones), no disponían de programas de apoyo y sus equipos periféricos eran lentos, por lo que sus costos eran muy elevados, con dificultad para su uso, alto consumo de energía y grandes probabilidades de fallas. Las computadoras de la Primera Generación fueron máquinas diseñadas para uso meramente científico.

SEGUNDA GENERACION (1959 - 1964).

Los transistores sustituyeron a los tubos de vacío como elemento lógico principal. Otros desarrollos notables fueron el surgimiento de las cintas y discos magnéticos para almacenamiento secundario, el almacenamiento interno en núcleo magnético, el diseño del hardware modular y los lenguajes de programación de alto nivel. Las características que encontramos en estas computadoras es el uso de transistores, cuentan con equipos periféricos más adecuados, son pequeñas, rápidas y empezaban a tener gran capacidad; disponen de lenguajes que facilitan su uso y su costo resulta más accesible. Estas computadoras a diferencia de las de la Primera Generación fueron diseñadas principalmente para el uso comercial, y no científico.

TERCERA GENERACION (1965-1970).

Los circuitos integrados (I.C.) reemplazaron a los transistores como elemento lógico principal. Otros avances importantes fueron el concepto de familias de computadoras, los sistemas operativos, adelantados en la aplicación del software de lenguaje y las microcomputadoras. En esta generación las computadoras se caracterizan principalmente en que trabajan con transistores microminiaturizados y circuitos integrales (interconexiones de cierto número de componentes electrónicos en una o más rutas conductoras para realizar una función eléctrica o electrónica); y circuitos monolíticos integrados (circuitos con miles de transistores encapsulados en una pequeña pieza de semiconductor); así como el nacimiento de redes de elaboración locales, nacionales e internacionales.

CUARTA GENERACION (1971- 1980)

Esta generación se resume en tres términos: "pequeño", "más pequeño" y "todavía más pequeño". Es un periodo de microminiaturización caracterizado por los microprocesadores y las memorias a base de semiconductores (memorias de un chip). La microminiaturización a reducido el costo de los productos de computación a un nivel que ha hecho que las computadoras se utilicen en casi todas partes. De este modo, la cuarta generación ha surgido como la era del usuario.

Los sistemas de administración de bases de datos han evolucionado de tal modo que facilitan a los usuarios, el reunir información relacionada que antes pudiera haberse guardado en cientos de diferentes archivos de computadora. Los lenguajes amigables para el usuario se están desarrollando para cubrir las necesidades del creciente número de usuarios que no son expertos en programación.

Las características principales de esta generación de computadoras son las siguientes: la velocidad de proceso se lleva a cabo en millones de operaciones por segundo, así como existen nuevos componentes de las mismas; los equipos periféricos se perfeccionan; se introduce lo que se conoce como circuitos a muy alta escala (VLSI); se producen nuevos y mejores lenguajes de programación y eficientes paquetes de aplicación de uso inmediato; surgen las microcomputadoras (para uso personal), en virtud del tamaño de los nuevos equipos; se introduce el empleo intensivo de minidiscos y cartuchos magnéticos, se desarrollan sistemas de impresión de alta calidad y velocidad; y empiezan a manejarse nuevos proyectos a efecto de ampliar el campo de la informática y computación para el próximo siglo.

QUINTA GENERACION (1981-¿?)

Generación en transición en donde los japoneses fueron los primeros en lanzar un desafío abierto al presentar, a principios de la década de los ochenta; computadoras realmente inteligentes, con sistemas que se puedan programar con lenguajes naturales mediante los cuales sea posible conversar.

De esta manera se ha observado a grandes rasgos el desarrollo y avance que han tenido las computadoras en los últimos años, lo cual ha traído como consecuencia nuevas formas de conductas delictivas que se les han denominado dentro del derecho como ``delitos informáticos´´, lo cual pone en peligro el adelanto tecnológico de las empresas que fabrican programas de computación, así como también a toda la sociedad; por lo tanto es necesario crear mecanismos de protección jurídica de la materia informática y computacional, mediante la revisión y reformas de nuestros textos legales, a efecto de dar una seguridad al desarrollo y crecimiento de la tecnología informática, ya que haciendo buen uso de estas máquinas, podemos obtener grandes aprovechamientos y beneficios.

1.3. COMPONENTES BASICOS DE LAS COMPUTADORA.[3]

Es importante mencionar, que para que una computadora produzca los resultados y beneficios que se persiguen, es necesaria la participación y dirección del ser humano; es decir, una computadora no opera por sí sola, el hombre es el que las crea, le señala instrucciones, mecanismos y programas. Las computadoras están programadas para realizar trabajos y tomar decisiones con una precisión exacta. Por ello se dice que las computadoras es la última y más moderna herramienta de trabajo que tiene el hombre para desempeñar sus funciones.

Una computadora consta de dos partes diferentes que trabajan al unísono : El equipo físico es la parte material de una computadora compuesta por: Equipo tangible (hardware), plástico, eléctrico y mecánico; y el equipo abstracto, que consiste en la programación y software.

HARDWARE: Parte dura de la computadora.

- Pantalla.
- Teclado.
- Mouse.
- Disco duro.
- Disco flexible.
- Impresora.
- CD. ROOM o multimedia.
- Escáner.
- V.R. (virtual reality)

Los dispositivos periféricos de entrada (locales o remotos) son los elementos que permiten la comunicación continua con la computadora. A través de estos dispositivos se le pueden proporcionar las instrucciones y los datos que, una vez procesados, arrojarán los resultados requeridos. Es importante distinguir los dos elementos que el hombre debe proporcionar a la computadora. Por un lado, los datos que la computadora procesará y por otro lado las instrucciones que la computadora seguirá una a una, las cuales a su vez, manipularan cada uno de los datos, y producirán los resultados previstos en dichas instrucciones.

Los dispositivos locales de entrada son aquellos que se encuentran conectados directamente a la unidad central de proceso (CPU). Los dispositivos remotos de entrada

[3] Véase a Joyanes Aguilar, Luis. Programación Basic para computadoras. 3era. Edición. Editorial McGraw-Hill, México 1992. Págs. 7-24. y a H. Sanders, Donald. Informática: Presente y Futuro. Editorial McGraw-Hill. México 1990. Págs. 19-23.

son aquellos que se encuentran conectados indirectamente a la unidad central de proceso mediante un conjunto adicional de elementos.

Una vez que el hombre sabe con precisión lo que desea obtener de la computadora y le proporciona los datos y las instrucciones a través de los dispositivos de entrada, la computadora es capaz de lograrlo, valiéndose de su unidad central de proceso, la cual realiza las siguientes funciones:

a). Almacena los datos e instrucciones en su memoria;
b). Sigue la secuencia de instrucciones en función de las condiciones en que debe procesar cada dato, tomando las decisiones predefinidas en las instrucciones, de acuerdo con las variantes de los datos.
c). Realiza todas las operaciones de cálculo establecidas en las instrucciones.

Unidad Central de Procesamiento (C.P.U.): Dirige todas las operaciones de la computadora. Contiene casi un millón de transistores en un oblea de silicio, por lo que puede ejecutar operaciones muy diversas; como sumar, multiplicar, leer la información enviada desde el teclado y enviar la información a la pantalla de visualización. Se controlan por programas almacenados en la memoria principal de la computadora.

Las funciones individuales que realiza la unidad central de proceso para operar los datos a través de las instrucciones son las siguientes:

a) Memoria.- Las instrucciones en conjunto que determinen el proceso que se efectuará con cada dato son recabadas y cargadas en la memoria de la computadora, así como cada dato que será procesado.

La memoria principal es contenida en muchos circuitos electrónicos. Almacena información, incluyendo las instrucciones que le indican a la CPU lo que debe de hacer, y los datos que debe procesar. Su tamaño se mide en bytes o kilobytes.

La memoria de acceso aleatorio (RAM) también conocido como disco virtual, proporciona otra forma de acelerar la operación con un costo menor al de un disco duro. Su memoria de trabajo se reduce de manera equivalente. Su información contenida se pierde cada vez que la computadora se apaga. Permite escribir, leer o modificar datos tantas veces como sea necesario. Las memorias de lectura y escritura, constituyen la parte medular del almacenamiento. Su bajo costo ha permitido que las computadoras actuales cuenten con memorias muy grandes, que pueden llegar a varias decenas de millones de caracteres.

La memoria de solo lectura (ROOM) constituyen una nueva concepción en la arquitectura de los equipos de cómputo. Normalmente se usan para guardar programas de

uso general en forma permanente, convirtiéndose así en un híbrido entre lo que tradicionalmente constituía el equipo y los sistemas y programas (hardware y software).

b) Unidad de Control.- En la memoria solo se guardan los datos y las instrucciones para que puedan ser recordados por la computadora, es decir, ahí no se efectúa el proceso. La unidad de control es la encargada de reconocer en que orden se le ha indicado que siga las instrucciones y, al encadenar una instrucción con otra, establece el camino a seguir; es decir, es una caja que contiene la mayor parte del equipo de la computadora. Tiene las unidades de disco, los puertos de entrada y salida (E/S) y elementos electrónicos como el CPU. y la memoria principal. Efectúa todos los cálculos y opera las otras partes de la computadora

c) Unidad Lógica y Aritmética.- Esta unidad es la encargada de efectuar las instrucciones aritméticas cargadas en la memoria, es decir, si la memoria dicta que se haga una suma, ésta unidad identifica los datos que componen la operación, y la realiza como lo hace cualquier calculadora electrónica, solo que guarda el resultado en su memoria donde se le haya indicado; ésta contiene: Circuitos, Registros, Unidad de control de proceso, Unidad de algoritmización.

Las operaciones de esta unidad se basan en la adicción. La resta se realiza por la adicción del complemento del número original. La división se logra por la sustracciones sucesivas y la multiplicación, por sumas progresivas.

En la unidad de aritmética lógica se usan dos clases de registros: acumuladores y sumadores. Los acumuladores constituyen registros especiales en los cuales se almacenan los resultados de operaciones aritméticas. El acumulador está formado, por lo general, de un par de registros combinados conjuntamente para manejar resultados de operaciones aritméticas. Todo proceso a realizar en una computadora arroja un resultado. Los dispositivos de salida son los que complementan el ciclo, ya que en ellos se obtienen dichos resultados. Y lo mismo que los dispositivos de entrada, los de salida pueden estar conectados cerca de la unidad central de proceso en forma local o en distancias remotas.

Los cálculos que se puedan realizar con una computadora alcanzan tales niveles de precisión que incluso a veces no los podemos concebir, como es el caso los puntos decimales. La capacidad de almacenamiento de datos que es posible mantener en los dispositivos de una computadora, también rebasa, por mucho, lo imaginable.

PROGRAMACION Y SOFTWARE

Un sistema computacional no hace nada hasta que se le ordena. Un programa, que consiste en instrucciones para la computadora es el medio por el cual le mandamos

ejecutar ciertas operaciones. Estas instrucciones son ordenadas y agrupadas en forma lógica mediante la etapa de programación, los programadores utilizan varios lenguajes de programación tales como COBOL Y BASIC, para comunicar instrucciones a la computadora.

Usamos el término "software" para referirnos a los programas que dirigen las actividades del sistema computacional. El software está dividido en dos categorías generales: aplicaciones y sistemas. El software de aplicaciones está diseñado y elaborado para realizar tareas específicas tanto administrativas y científicas, ejemplos de estos son: El procesamiento de nominas entrada de pedidos o análisis financiera. El software de sistemas es más general que el de aplicaciones generales, es independiente de cualquier área específica de aplicación.

1.4. CLASIFICACION DE LAS COMPUTADORAS.

El Lic. en Ciencias de la Comunicación, Alberto Montoya Martín del Campo, clasifica a las Computadoras de acuerdo a sus capacidades en: a). Recolectar datos. b). Almacenar información. c). Organizar información. d). Cálculos. e). Comunicaciones. f). Presentación de la información. g). Control. h). Diseño auxiliado por computadora y elaboración de modelos. Y de acuerdo a sus usos: a). Tecnología Militar. b). Tecnología Científica. c). Tecnología de producción. d). Microelectrónica integrada a los bienes de consumo. e). Tecnología de poder.[4]

Otra clasificación, considerada como Clásica es aquella que considera que existen diferentes tipos de computadoras y sus aplicaciones están en función de las operaciones que se pueden realizar con cada una de ellas. Es decir, que las computadoras, en función a su aplicación, y por el tipo de dato que procesan, se clasifican en las siguientes categorías:

a). Computadoras Digitales: Macrocomputadoras, minicomputadoras y microcomputadores.
b). Computadoras Analógicas.
c). Computadoras Híbridas.

Una computadora digital es un dispositivo de cálculo que procesa datos discretos. Trabaja directamente contando números o dígitos que representan cifras, letras u otros símbolos especiales. Los procesadores digitales cuentan valores discretos para alcanzar los resultados deseados. Los datos que se obtienen por conteo se llaman datos discretos y

[4] Montoya Martín del Campo, Alberto. México ante la revolución tecnológica. Asociación Mexicana de Investigadores de la comunicación. Editorial Diana. México 1993.

aquellos obtenidos indirectamente por mediación de alguna magnitud física en una escala, son datos continuos.

A diferencia con los procesadores digitales, hay también máquinas analógicas que no calculan directamente números y en cambio, lo hacen con variables que están medidas en una escala continua y son registradas con un determinado grado de precisión. Los sistemas de computación analógicos son frecuentemente usados para controlar procesos. Las computadoras analógicas pueden ser precisas hasta en un 0.1% del valor correcto. Pero las computadoras digitales pueden obtener cualquier grado de precisión que se requiera para los cálculos, añadiendo fracciones a la derecha del punto decimal.

Las características deseables de las máquinas analógicas y digitales son continuadas algunas veces para crear sistemas de computación híbridos. Los procesadores analógicos y los híbridos, realizan importantes tareas especializadas. Pero la abrumadora mayoría de las computadoras usadas en aplicaciones científicas y comerciales son dispositivos digitales.

Las computadoras digitales son fabricadas para usos especiales y para usos generales. Las especiales están diseñadas para realizar solo una tarea específica, los programas de instrucciones están alambrados en el interior o permanentemente almacenados a la máquina. Aunque esto reduce flexibilidad, hace la tarea rápida y eficiente; mientras que las de uso general son las que están diseñadas para almacenar diferentes programas y pueden ser usadas en incontables aplicaciones. La flexibilidad de un sistema de propósito general está limitada solo por la imaginación humana.

La principal característica de las Macrocomputadoras está dada por su gran velocidad de proceso y la enorme capacidad de almacenamiento de datos y producción de resultados; en tanto que las minicomputadoras son muy similares a las macrocomputadoras, solo que su capacidad de proceso y almacenamiento de datos está muy por debajo de éstas.

Las Microcomputadoras.- Son computadoras digitales de aplicación general, compuesta por elementos estándar, tienen su propio suministro de energía, y son utilizadas por propietarios de pequeños negocios, fabricantes, aficionados, educadores, científicos y niños para multitud de fines. Son una innovación en los últimos años, y la aceptación que han tenido llega a ser sorprendente, al grado de que se le han llamado también computadoras personales (PC).

CAPITULO II
PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTO.

SUMARIO: 2.1. NOCIONES GENERALES. 2.2. PROTECCIÓN MEDIANTE LA VÍA CIVIL. 2.3. PROTECCIÓN MEDIANTE LA VÍA PENAL. 2.4. PROTECCIÓN MEDIANTE LA VÍA DE DERECHO DE AUTOR.

2.1 NOCIONES GENERALES.

Antes de comenzar el análisis y desarrollo de la problemática que implican los Delitos Informáticos, es menester hacer un estudio breve, pero completo respecto a los aspectos y elementos que implica la Protección Jurídica de los Programas de Computo, el cual es un problema de actualidad en todo el mundo.

Por ello, es importante conocer qué régimen de derecho es el más adecuado para proteger jurídicamente a los programas de cómputo, ya sea como propiedad o derecho intelectual; así como también analizar todo lo relacionado con la tecnología e informática.

La Ciencia de la Informática y la Computación han sido vulneradas por un gran número de conductas ilícitas no tipificadas como delitos, en razón de los siguientes factores:

a) Por el gran número de personas que entran en contacto con las computadoras, algunos con conocimientos muy avanzados en estas ciencia, y carentes de ética en el momento de realizar un comportamiento indebido.

b) Por el bajo costo de los equipos de cómputo y el continuo desarrollo de la Tecnología computacional que permiten realizar operaciones inimaginables, y que ahora son tan factibles y reales.

c) Por la gran cantidad de información que se maneja, almacena y se procesa y se puede recuperar en un periodo corto, lo que la convierte en un blanco fácil para la delincuencia.

También es conveniente señalar que la protección de los programas de cómputo no es en sentido estricto un tema de índole jurídico, sino también son temas que pueden ser estudiados por otros medios de protección, principalmente el que nos proporciona la misma informática, el cual consiste en una protección de carácter técnica o tecnológica, como por ejemplo el método de la Criptografía (método que consiste en criptar los programas por un sistema de codificación sofisticado que emplea una o varias claves que

se convierten en un conjunto de caracteres que transforman los cálculos aritméticos y algebraicos en información codificada); y los Métodos de Borrado Interno (métodos que consiste en un conjunto de instrucciones por los cuales los programas de cómputo dejan de funcionar pasados ciertos días), los cuales, son métodos que impiden el copiado de programas a través de sus instrucciones, y que puede llegar en un momento dado a bloquear o destruir el mismo programa.

La desventajas que tienes dichos métodos son su alto costo, así como también su corta existencia, en razón de que como son creados por la técnica, es esta misma la que los supera con el paso del tiempo, por lo cual no garantiza en un cien por ciento la protección de los programas de cómputo de las conductas ilícitas.

Ahora bien, así como en la informática se pretende proteger a los programas de cómputo, en el ámbito jurídico se ha procurado dar soluciones al mismo problema. Se ha discutido mucho entre los doctrinarios de la materia cual sería la vía idónea para proteger jurídicamente los programas de cómputo, algunos autores sostienen que la más conveniente es la vía civil; otros señalan que debe de ser la vía penal; otros dicen que debe de ser la vía autoral (siendo ésta la utilizada en México); otros tantos señalan vías que a fin de cuentas resultan inapropiadas y poco eficaces (como por ejemplo la del enriquecimiento ilícito o sin causa).

Pero independientemente de la vía, veremos en el presente capitulo que todos ellas de forma directa e indirecta tienen aplicación y repercusiones jurídicas no solo dentro de nuestro sistema legal, sino en todos los sistemas legales del mundo.

2.2 PROTECCIÓN MEDIANTE LA VÍA CIVIL.[5]

Dentro de esta vía tenemos como fuente primordial a los convenios y los contratos, que según el Código Civil Para el Distrito Federal y Territorio Federales, nos señala en sus artículos 1792 que, Convenio es el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones; y el 1,793 estatuye que los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos, nos dan la pauta a efecto de entender el por qué de muchos autores señalan que la vía civil es la mas adecuada para proteger a los programas de cómputo.

[5] Esta sección se fundamenta en los siguientes trabajos: a). Ricardo A. Guibourg, Jorge O. Allende, Elena M. Campanella. Manual de Informática Jurídica. Editoreal Astrea. Buenos Aires, 1996. Pags. 253-262. b). Téllez Valdez, Julio. Derecho Informático. 2da. Edición. Editorial McGraw-Hill, México 1996. Págs. 85-94. c). Téllez Valdez, Julio. La Protección Jurídica de los Programas de Computación. UNAM, México 1989, 2da. Edición. Instituto de Investigaciones Jurídicas. Págs. 30-36.

La forma a través de convenios y contratos consisten en consagrar en los mismos, cláusulas que tiendan a la protección y seguridad de los programas de cómputo, estipulando en las cláusulas qué personas tienen acceso a los programas, su uso, función, utilización, modificación, etc., así como señalar que sanciones se impondrán a aquellas personas que destruyan información, utilicen un recurso de un sistema sin autorización, obtengan informes confidenciales o exploten un programa, o en el último de los casos, lo utilicen para fines ilícitos. Todo ello implica un régimen estricto de secreto entre las partes.

Asimismo, esta forma de protección puede presentar dos variantes: la primera consiste en la firma de un contrato privado entre la empresa distribuidora del software y el usuario del programa; y la segunda consiste en la protección extracontractual, la cual consiste en el deber a que se obligan las dos partes (la empresa distribuidora y el usuario), de poder explotar un programa de cómputo, sin que exista la formalidad de un contrato.

En la actualidad, en nuestro país y casi todas partes del mundo, las empresas distribuidoras de Hardware así como de Software, recurren a esta vía del recurso contractual, creyendo con ello que se encuentran amparados legalmente, mas sin embargo, esta forma de protección es incompleta, en razón de que en primer lugar, se tendría que elaborar y estipular en el contrato un sin número de cláusulas para poder englobar todas las conductas que puedan llegar a darse, lo cual sería casi imposible, además de la dificultad de ambas partes para acreditar, según el caso si se ha o no se ha cometido una infracción al contrato sería muy difícil, toda vez que los medios de pruebas en estos casos requieren gran conocimiento de la informática, además de que entre ambas partes siempre existe desequilibrio en el mismo contrato, teniendo el usuario, una gran variedad de formas para poder quebrantarlo.

Todos estos motivos son los que nos hacen pensar que esta vía no es la más idónea para poder proteger a los programas de cómputo en una forma total.

Como referencia, es bueno apuntar, que otra de las formas con la que se pretende proteger mediante esta vía a los programas de cómputo es el Enriquecimiento ilegítimo o sin causa, siguiendo el principio de que nadie puede enriquecerse en detrimento de otro. Así nos señala el Código Civil para el Distrito Federal y Territorios Federales, en su Art. 1882 "El que sin causa se enriquece en detrimento de otro, está obligado a indemnizarlo de su empobrecimiento en la medida que él se ha enriquecido".

El problema que se encuentra en esta acción consiste en acreditar mediante pruebas fehacientes dicho enriquecimiento de una persona en detrimento de otra, es decir, comprobar verdaderamente que se presentó la figura del enriquecimiento ilegítimo o sin causa, y más aún, podría utilizarse dicha figura en sentido inverso, es decir, aparentar un empobrecimiento tanto por parte de la empresas o del usuario en su caso, y ahí estaría un

problema mucho mayor. Motivos por los que se considera muy difícil que se consagre como la mejor esta forma de protección para los programas de cómputo.

2.3. PROTECCION MEDIANTE LA VIA PENAL.

Encontramos en esta vía, la forma más adecuada dentro de la esfera jurídica para proteger a los programas de cómputo, la cual consiste en la triplicación de las conductas ilícitas que tengan los sujetos, que hasta el momento doctrinalmente se les conoce como Delitos Informáticos o Computaciones, (y que en los países de habla inglesa se les denomina Computer Crimen), como la forma de solución más viable para la protección y resguardo de los programas de cómputo.

En la actualidad, los países mas avanzados en materia informática tales como Estados Unidos, Francia, Japón, España por mencionar algunos, tienen una legislación amplia en materia penal respecto a los llamados delitos informáticos o computacionales, siendo dichos países los precursores en esta disciplina.

El Código Penal para el Distrito Federal en materia de fuero común, y para toda la república en materia de fuero Federal, estatuye figuras jurídico-penales que no podrían aplicarse a los Delitos Informáticos, toda vez que estos implican sujetos distintos, acciones y modalidades de diferente índole, aunado a los efectos transfronterizos que acarrean los mismos. Es menester, ante el desarrollo tecnológico venidero, que nuestra legislación penal, se reforme adoptando esta nueva figura jurídica a nivel federal y celebrando Tratados Internacionales con otros países respecto al tema, para con ello, poder hacer frente a tales actividades ilícitas, que actualmente son de gran peligrosidad para los países avanzados y para el nuestro también, por sus efectos transfronterizos o Internacionales.

El Código Penal Federal de 1931, en su Título Vigésimo segundo y bajo el rubro de "Delitos en contra de las personas en su patrimonio", consigna los siguientes delitos:

- Robo (Capítulo I, artículos 367-381 bis),
- Abuso de confianza (Capítulo II, artículos 382-385);
- Fraude (Capítulo III, artículos 386-389 bis);
- Extorsión (Capítulos III bis artículo 390);
- Daño en propiedad ajena (Capítulo VI, artículos 397-399 bis).

Además, en su Titulo Noveno, establece El delito de Revelación de Secretos, en los artículos 210 y 211.

Tales delitos, no deben equiparase o tratar de adecuar a los Delitos Informáticos, toda vez que estos últimos son de diferente índole y tienen características muy especiales, las cuales los hacen distintos a los delitos actualmente estatuidos en el código penal federal.

A continuación, analizaremos las discrepancias entre los delitos indicados y el porque no deben identificarse con los delitos informáticos.

DISCREPANCIA CON EL DELITO DE ROBO

ARTICULO 367. "Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley".

La discrepancia esencial entre el delito de Robo y los Delitos Informáticos estriba en que en él primero debe haber una cosa ajena mueble y en los segundos no se da tal condición, ya que la información se considera un bien intangible o inmaterial .

DISCREPANCIA CON EL DELITO DE ABUSO DE CONFIANZA

ARTICULO 382. "Al que con perjuicio de alguien, disponga para si o para otro de cualquier cosa ajena mueble, de la que se haya transmitido la tenencia y no el dominio, se le sancionará con prisión hasta de un año y multa hasta de 100 veces el salario, cuando el monto del abuso no exceda de 200 veces el salario."

De igual forma qué en delito de robo, en el abuso de confianza debe haber una cosa ajena mueble, y por ello el delito informático no puede configurase.

DISCREPANCIA CON EL DELITO DE FRAUDE

ARTICULO 386. "Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido".

La diferencia medular con el delito informático, es que en este delito no se requiere necesariamente de engaño, ni de aprovecharse del error para hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido, ya que por la naturaleza de este nuevo tipo penal, este se puede presentar, por diversas formas de acción u omisión.

Ahora bien, no obstante lo anterior, en algunos casos puede mediar el engaño, por ejemplo en el comercio electrónico o en los famosos casinos virtuales. O también aprovecharse del error de una persona, sin embargo tal condición no es básica para la ejecución o manipulación de acciones ilícitas a través de la computadora o vía Internet.

DISCREPANCIA CON EL DELITO DE EXTORSIÓN.

ARTICULO 390. "Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa".

Por cuanto hace a este delito, tales acciones o condiciones pueden ser dadas en el delito informático, sin embargo, estaríamos en presencia de dos delitos diferentes, ya que en estos últimos, el medio comisivo sería sin lugar a duda la computadora a través de Internet u otro sistema de red, o telecomunicaciones y estas serían las características singulares o especiales que harían diferente a los delitos Informáticos con el de Extorsión.

DISCREPANCIA CON EL DELITO DE DAÑO EN PROPIEDAD AJENA

ARTICULO 399. Comete el delito de Daño en propiedad ajena: "Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones de robo simple".

Volvemos a recalcar que en los Delitos Informáticos, no se maneja el concepto de cosa mueble, ya que por la naturaleza de estos ilícitos, siempre media la información, la cual es considerada como inmaterial o intangible, ya que se encuentra almacenada en un soporte de almacenamiento magnético.

Por otro lado, dadas las características especiales de este nuevo tipo penal, no se dan únicamente el daño, la destrucción o deterioro en la cosa ajena o propia, sino también dado el carácter transfronterizo de la información, se dan en contra de la nación, otros países, la humanidad, contra la seguridad pública, las telecomunicaciones, la salud mundial, la economía tanto nacional como extranjera, etc.

DISCREPANCIA CON EL DELITO DE REVELACIÓN DE SECRETOS

ARTICULO 210. "Se impondrán de treinta a doscientas jornadas de trabajo a favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que puede resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto".

ARTICULO 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 preste servicios profesionales o técnicos o por funcionario o empleado público, cuando el secreto revelado o publicado sea de carácter industrial".

Este tipo penal, quedaría restringido y sería insuficiente para poder abarcar la complejidad que implican los delitos informáticos, ya que estos manejan múltiples conductas, las cuales no se limitarían a la revelación del secreto o comunicación reservada, puesto que las mismas van desde acceder ilícitamente a esta información, modificarla, destruirla parcial o totalmente, revelarla a un determinado grupo o al público en general, etc.

Además de que el artículo 210, establece la condición de ". . . que conoce o ha recibido con motivo de su empleo, cargo o puesto", y en los delitos informáticos "el cracker" accede a esa información ilícitamente, desconociéndola concreta y específicamente al principio.

Como resumen de lo analizado, los Delitos Informáticos no deben equipararse o identificarse con los delitos de robo, fraude, abuso de confianza, daño en propiedad ajena, revelación de secretos u otro delito ya que este Nuevo Tipo Penal (en otros países), tiene sus propias características, las cuales son diferentes y con carácter especial a los delitos indicados. Además de la cualidad de la información que es intangible o material.

2.4 PROTECCION MEDIANTE LA VIA DE DERECHO DE AUTOR.

Esta vía se ha presentado en la actualidad como la de mejor regulación y aplicación dentro del ámbito del derecho, como medio de protección jurídica de los programas de cómputo. En algunos países del mundo tales como Alemania, Australia, Brasil, Corea del sur, Chile, China, España, Estados Unidos, Francia, Japón, México,

entre otros, han incorporado en sus legislaciones de Propiedad Intelectual, Patentes, Marcas o Derecho de Autor, la solución más viable al conflicto de la protección jurídica de los programas de cómputo. Otros países, como es el caso de Argentina, Uruguay y Colombia, han dictado normas administrativas reglamentarias vinculadas a la creación de un Registro Nacional de Programas de Cómputo.

Existe además, en el ámbito internacional, la Organización Mundial de la Propiedad Intelectual (de la cual México es parte), la cual ha recomendado a sus países miembros, que los programas de computación se registren y se protejan como obras científicas, técnicas y literarias.

Hay que tener presente que el derecho de autor, es una rama del Derecho de Propiedad Intelectual, y que tiene las siguientes características::

- Es una creación original y novedosa producto del intelecto humano. (Principio de originalidad y novedad).
- Es un derecho exclusivo de explotación o de autorización para el titular de la obra. (Derecho Patrimonial).
- Es un derecho único, primigenio y perpetuo para el titular de la obra. (Derecho Moral).
- Están protegidos por un tiempo determinado.

En nuestro país, la Ley Federal del Derecho de Autor, contiene un capítulo especial que habla de la forma de regulación jurídica de los programas de cómputo y las bases de datos, además de señalar de manera clara en su Artículo 13 fracción XI lo siguiente:

> **Art. 13.- "Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:**
>
> **XI.- Programas de cómputo".**

Así también en su Artículo 101 nos define lo que para esta Ley un programa de cómputo: "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".

Sigue diciendo dicha ley:

> *"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 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o
II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

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 adaptación, 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 desensamblaje.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
II. Su traducción, adaptación, reordenación y cualquier otra modificación;
III. La distribución del original o copias de la base de datos;
IV. La comunicación al público, y
V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia".

Pese al gran esfuerzo que han puesto nuestros legisladores en materia de derechos de autor respecto de los programas de cómputos, existen[6] diversos supuestos que todavía no cubren las necesidades para satisfacer en una forma aceptable la protección jurídica de los programas de cómputo, ya que si bien es cierto la Ley Federal de Derechos de Autor protege a dichos programas, existe una insuficiencia para la debida protección de los programas de cómputo, las cuales consisten en los siguientes razonamientos:

a) Los derechos de autor protegen la divulgación, publicación, comunicación pública, ejecución o representación pública, distribución al público y la reproducción de uno obra artística, técnica o científica (entre ellos están comprendidos los programas de cómputo), pero debe de entenderse que un programa de cómputo es mucho más complejo que solo estas medidas de protección, es decir, un programa de cómputo no es algo concreto o material, sino algo abstracto e inmaterial, no se regula como una obra literaria o artística, ya que pese a estar regulado esta materia en derechos de autor, pueden provocarse a un programa de cómputo una alteración sin que con ello se entre en los supuestos que señala la Ley Federal de los Derechos de Autor, tales como su modificación, corrección o inclusive su mejoramiento para una mejor eficacia, no siguiendo los mismos lenguajes o códigos o el conjunto de instrucciones que hizo el autor original para crear su programa, y que otra persona astuta puede mejorar ese programa y dejarlo mejor que el original.

Además de que un programa de cómputo es muy fácil de reproducir como se puede comprobar en cualquier escuela o empresa, en comparación con las demás formas protegidas por el derecho de autor, tales como un libro, una canción, un videocassette etc., los cuales son profesionales los que se encargan de ello. Es por eso que los programas de cómputo pueden provocar un sin número de conductas ilícitas, por lo que es necesario de manera urgente la tipificación de los delitos informáticos o computacionales.

b) Los Derechos de autor quedan protegidos por un tiempo determinado. Este principio es muy relativo en los programas de cómputo, ya que es precisamente la Ciencia de la Informática la que está avanzando a pasos enormes dentro de nuestra época, lo cual provoca que lo que es novedoso en mes determinado mes o día, a los dos o tres meses o días ya es obsoleto, provocando así una gran confusión este principio dentro de la gama de los derechos de autor respecto de los programas de cómputo.

c) Al igual que el principio de tiempo determinado, el principio de originalidad no está de todo claro en el derecho de autor al grado de que se podría considerar insuficiente, en razón de que se puede afirmar que solamente los programas de cómputo que se crearon en el nacimiento de la ciencia computacional, son los únicos originales, ya

[6] Véase la Ley publicada en el Diario Oficial de la Federación el lunes 24 de diciembre de 1996)

que todos los demás que se han venido creando o inventando, tienden a realizar las mismas funciones y poseen las mismas características que los anteriores, solamente que estos realizan dicha función de una manera mucho mas avanzada y menos complicada para el usuario de una computadora.

Por estos razonamientos y otros de carácter técnico, en materia de la informática y computación, es muy difícil afirmar que los programas de cómputo se encuentren protegidos mediante los derechos de autor de manera total. Es por ello la necesidad de legislar en materia de los denominados "delitos informáticos."

Ya por último es importante señalar que muchos han pretendido proteger jurídicamente a los programas de cómputo mediante el sistema de patentes, lo cual es un completo error, ya que sería precisamente el sistema de patentes el que provocaría aún más un sin número de conductas ilícitas en esta materia, en razón de su principio de divulgación pública, porque facilitaría tener acceso total a un programa de cómputo y permitiría de manera ilimitada la utilización, reproducción, modificación y hasta la destrucción de los mismos, por ello no es conveniente utilizar este sistema, además que en nuestro país, la Ley de Fomento y Protección de la Propiedad Industrial es tajante al señalar en su artículo 19 fracción IV lo siguiente:

> ***"Artículo 19.- No se considerarán invenciones para los efectos de esta Ley:***
>
> ***IV.- Los programas de computación."***[7].

[7] Véase la Ley publicada en el Diario Oficial de la Federación el jueves 27 de junio de 1991.

CAPÍTULO III
LOS DELITOS INFORMÁTICOS.

SUMARIO: 3.1. GENERALIDADES. 3.2. CONCEPTO DE DELITO INFORMÁTICO. 3.3. CARACTERÍSTICAS. 3.4. CLASIFICACIÓN. 3.5. ANÁLISIS DE LOS ELEMENTOS DEL DELITO INFORMÁTICO. 3.5.1. La conducta y su elemento negativo. 3.5.2. La Tipicidad y su elemento negativo. 3.5.3. La antijuridicidad y su elemento negativo. 3.5.4. La culpabilidad y su elemento negativo. 3.5.5. La imputabilidad y su elemento negativo. 3.5.6. La punibilidad y su elemento negativo. 3.5.7. La condicionalidad objetiva y su elemento negativo.

3.1. GENERALIDADES.

La aparición en la sociedad actual de las nuevas formas de conductas ilícitas no reconocidas o tipificadas en los textos penales, implica el riesgo de caer en el elemento negativo de la Tipicidad: la atipicidad; problema que el Derecho ha tratado de solucionar mediante la regulación específica de dichas formas de conductas, en un marco legal adecuado. Por lo tanto, es necesario introducir nuevas figuras delictivas para dar respuestas a las exigencias de la sociedad actual, provocando, la desaparición o modificación de aquellas figuras ya superadas, que han perdido su razón de ser.

Los delitos informáticos implican actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho y ya no es válido el criterio de encuadrarlos conforme a los delitos llamados "clásicos", por las razones expuestas en el capítulo anterior.

En el presente capítulo, se analizarán a los delitos informáticos en su aspecto doctrinal y práctico, en tanto suponen un nuevo grupo de comportamientos surgidos como consecuencia del avanzado desarrollo de la tecnología en la sociedad y el uso indebido de las misma, con el objeto de perjudicar a los habitantes de dicha sociedad.

3.2. CONCEPTO DE DELITO INFORMATICO.

"La palabra delito, deriva de verbo latino delinquere, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. El delito, está íntimamente ligado a la manera de ser de cada pueblo y a las necesidades de cada época,

los hechos que en determinado momento han tenido ese carácter, lo han perdido en función de situaciones diversas y, al contrario, acciones no delictuosas, han sido erigidas en delitos."[8]

Para **Francisco Carrara**, principal exponente de la escuela Clásica, el delito "es la infracción de la ley del estado promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso."[9]

Por su parte, **Rafael Garófalo**, representante del Positivismo, lo define de la siguiente manera: "Es la violación de los sentimientos altruistas de probidad y de piedad en la medida media indispensable para la adaptación del individuo a la colectividad."[10]

El Código Penal para el Distrito y Territorios Federales en materia del fuero común y para toda la República en materia del fuero federal, en su artículo 7 define al delito de la siguiente manera: "Es el acto u omisión que sancionan las leyes penales." Por último el artículo 11 del Código penal para el Estado de Guerrero, nos señala lo siguiente: "El delito es la conducta típica, antijurídica e imputable".

Por otro lado, etimológicamente la palabra Informática surge de la fusión de los términos información y automatización. Los Franceses son los creadores de esta palabra, en virtud de que unieron las dos primeras sílabas de **Infor**mación y las tres últimas de auto**mática** ; por lo tanto en sentido amplio informática significa "tratamiento automático de los datos que constituyen una información".

> **La Informática se define como: "Conjunto de técnicas en que se basan los procesos de tratamiento automático de la información mediante computadoras u ordenadores electrónicos." O como "El conjunto de ciencias, técnicas y actividades relacionadas con los ordenadores y con todas sus aplicaciones posibles."[11]**

A nivel internacional se considera que no existe una definición propia de los delitos informáticos, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. Así por ejemplo Carlos Sarzana define a los delitos electrónicos de la siguiente manera:

---

[8] Castellanos Tena, Fernando. Lineamientos elementales de Derecho Penal. Edit. Porrúa, S.A. México 1984. Vigésima Edición. pág. 125.
[9] Ibidem, págs. 125 y 126.
[10] Ibidem, pág. 126.
[11] Nuevo Diccionario Enciclopédico Universal y de México. 1996 Ediciones Trébol. S.L. Barcelona España.

"Cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo." [12]

Julio Téllez Valdés nos dice que para hablar de delito informático, por lo menos en México, es necesario que las conductas que se describen estén contempladas en textos jurídico-penales y en nuestro país no han sido tipificados. Por ello da su conceptualización del delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin."[13]

Para **Carlos M. Correa**, tratadista argentino, el delito informático consiste en "Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y la transmisión de datos." [14]

Por otro lado, **Klaus Tiedemann** expresa lo siguiente: "Son los delitos que protegen cualquier acción ilegal en el que la computadora es el instrumento o el objeto del delito." [15]

Podemos definir a los delitos informáticos como: "La realización de una conducta que, reuniendo los elementos que integran el concepto del delito, es llevada a cabo utilizando y vulnerando el componente informático ya sea como instrumento, medio o fin, en el hardware o en el software".

3.3. CARACTERISTICAS.

a). Los Delitos Informáticos representan una nueva forma de Delito de Cuello Blanco.
b). Los métodos de comisión son únicos. (Es necesario el conocimiento de la Informática).
c). El perfil del delincuente informático es muy original, es decir, el sujeto activo requiere reunir cierto tipo de características que no se presentan en los demás ilícitos.
d). El tiempo de ejecución es mínimo a comparación de cualquier otro medio de delito, es decir, la velocidad para cometer este tipo de ilícitos es impresionante.
e). El bien jurídico tutelado es el derecho a la intimidad y la información
f). Los daños económicos y morales que generan este tipo de delitos son extremadamente

[12] Citado por Téllez Valdez, Julio. Derecho Informático, México, Universidad Nacional autónoma de México, 1987, p. 105.
[13] Ibidem, p. 105.
[14] Correa M. Carlos. Derecho Informático, Buenos aires, Ed. Depalma, 1987, pp. 125 y 296.
[15] Citado por Rojas Pérez, Palacios Alfonso. Delitos de Cuello Blanco, México. Joaquín Porrúa, S.A., 1986, pág. 78.

considerables.

g). La distancia tampoco es una limitante en razón de que si el criminal posee una terminal de computadora, vía telefónica puede perpetrar su crimen hasta el otro extremo del mundo (Delitos por Internet).

h). Presenta grandes dificultades para su comprobación.

i). En este tipo de delitos no existe violencia como en otros.

j). Normalmente se cometen en el ejercicio empresarial o gestión económica. Pero sus objetivos suelen ser muy variados, desde atentar contra un particular, hasta perjudicar al mismo Estado.

3.4. CLASIFICACION.

Existe un sin número de formas de clasificación de los delitos, ya que estos tienen una subdivisión atendiendo a diversos factores como lo son:

1.- **La conducta:** Delitos de acción (aquellos que se consuman a través de un comportamiento positivo, es decir, en una conducta de hacer); y de omisión (Aquellos que para que tenga lugar la consumación del delito se requiere una conducta de abstención). Estos últimos a su vez se subclasifican en delitos de simple omisión y delitos de Comisión por omisión

2.- **Los sujetos que participan:** Delitos unisubjetivos (Solo requieren un individuo para su ejecución) y plurisubjetivos (Es necesaria la participación de dos o mas individuos para su ejecución).

3.- **El resultado:** Delitos formales (cuando existe una acción o una omisión pero no se manifiesta un resultado externo, lo que se castiga es la conducta en sí); y delitos materiales (Son los que si provocan un resultado externo).

4.- **Su culpabilidad:** Delitos Dolosos (Se presentan cuando existe la voluntad del sujeto activo de realizar el daño); delitos culposos (Es aquel que se produce cuando el sujeto activo no desea el resultado típico y antijurídico, sin embargo este se presenta por la falta de atención y cuidado del mismo); y preteritencionales (Se presentan cuando el resultado va más allá de la intención del sujeto activo).

5.- **Su duración:** Delitos instantáneos (Aquel que se produce en un solo momento o instante); delitos permanentes (aquellos que requieren una continuidad tanto en la conciencia del sujeto activo como en su ejecución); y delitos continuados (aquellos en el que se producen varias acciones y una sola lesión jurídica).

6.- **El daño que producen:** Delitos de Lesión (provocan un daño directo a los bienes jurídicamente tutelados); y delitos de peligro (aquellos que solo ponen en peligro los bienes jurídicamente protegidos por la ley penal, es decir, que no sufren un daño directo).

7.- **Forma de persecución:** delitos por querella (aquellos que son perseguibles por la autoridad solamente por que la ley disponga que así lo manifieste la parte agraviada); y de oficio (Cuando la autoridad está obligada por mandato de ley a perseguir y castigar a los responsables del delito).

8.-.- **Su gravedad**: faltas, delitos y crímenes.

Ahora bien, entrando de lleno a la clasificación de los Delitos Informáticos, Julio Téllez Valdés clasifica a éstos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

> 1.- "**Como instrumento o medio**: Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.
> 2.- **Como fin u objetivo**: En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Destrucción de un programa, dañar una memoria y quemar la computadora."[16].

La Dra. Lima los clasifica de la siguiente manera:

> 1.- "**Como Método**: Para llegar al resultado ilícito usan algún método electrónico. La máquina o instrumento mismo realiza la infracción penal dirigido por su autor como: a) Falsificar una tarjeta de crédito. b)Defraudar a una compañía alterando sus activos, pasivos, etc. c) Fraude con técnica Salami que consiste en extraer pequeñas cantidades de dinero de miles de cuentas bancarias; los afectados generalmente no lo perciben o se conforman con hacer una recomendación intranscendente.
> 2.- **Como Medio**: Son las conductas criminógenas que para realizar un delito se valen de un objeto electrónico como medio o símbolo, como los siguientes: a). Lectura de información confidencial para

[16] Téllez Valdez, Julio, Op. cit. pág. 106 y 107.

bloquear la capacidad operativa de la víctima y cometer sabotaje industrial. b). Lectura de ficheros judiciales para extorsionar. c). Lectura de datos confidenciales para chantajear"[17].

La clasificación que se propone es la siguiente, atendiendo al papel que juega la computadora en la comisión de los delitos:

a) Como objetivo o Fin.- Se presentan cuando la conducta del agente va encaminada primeramente a la destrucción de los componentes de una computadora, o de sus programas. (ejemplo: La destrucción de Software en una red).
b) Como medio o Instrumento.- Se presenta cuando la computadora es utilizada como la herramienta o el instrumento para la comisión de la conducta ilícita. (El fraude con la técnica Salami).
c) Como un Método.- se presenta cuando el aparato de cómputo es el encargado por sus características propias de cometer un ilícito, es decir, programar una computadora para que cometa un delito. (ejemplo: La detonación de una bomba, la falsificación de tarjetas de crédito, etc.).

Existen otros tipos de clasificaciones atendiendo a los enfoques que se presentan:

1.- Por el tipo de delito:
a). Fraude;
b). Robo;
c). Abuso de confianza;
d). Daños en propiedad ajena;
e). Extorsión;
f). Sabotaje;
g). Espionaje y Sabotaje.

2.- Por el tipo de conducta:
a). De destrucción;
b). De modificación;
c). De alteración;
d). De creación;
e). De diseño;
f). De ejecución;
g). De uso;

[17] Lima, Ma. de la Luz. Delitos Electrónicos, México, revista Criminalia No. 50, 1984, pág. 29.

3.- Por la forma de operar:
a). En ataque físico;
b). Técnica Salami;
c). Virus Informático
d). Manipulación de datos falsos.
e). Por el uso de símbolos o códigos secretos.

4.- Por el resultado obtenido:
a). Afectación a la propiedad intelectual;
b). Daño físico y destrucción;
c). La ganancia o el lucro indebido;

3.5. ANALISIS DE LOS ELEMENTOS DEL DELITO INFORMATICO.

Es preciso mencionar que en el presente tema los autores y doctrinarios de la materia penal no han llegado a un acuerdo sobre los elementos del delito, ya que para algunos éste es indivisible, es decir, es un todo (Corriente Unitaria), y para otros, el delito está constituido por varios elementos (Corriente Totalizadora).

Ahora bien, independientemente de esta discrepancia doctrinal, se estudiará en el presente capítulo al delito informático siguiendo la postura de la Corriente atomizadora, por lo cual el Maestro Jiménez de Azúa ha definido doctrinalmente al delito como "el acto típicamente antijurídico culpable, sometido a una sanción penal."[18] Y a su vez el maestro Raúl Carranca y Trujillo nos señala: "Delito es el acto típicamente antijurídico, culpable, sometidos a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal."[19]

Como se puede apreciar de estas dos definiciones, encontramos en ellas los elementos positivos y negativos del delito que podemos enunciar de la siguientes manera:

* Conducta humana.	* Ausencia de Conducta.
* Tipicidad.	* Atipicidad.
* Antijuridicidad.	* Causas de Justificación.
* Culpabilidad.	* Inculpablidad.
* Imputabilidad.	* Inimputabilidad.
* Punibilidad	* Excusas absolutorias.
* Condiciones objetivas de punibilidad.	* Ausencia de condiciones objetivas de punibilidad.

[18] Jimenez de Azua, Luis, Principios del Derecho Penal, la Ley y el Delito. Edit. Sudamericana Abelardo Perrot, Buenos Aires 1990, pág. 207.
[19] Carranca y Trujillo, Raúl, Der. Penal Mexicano, Méx. Edit. porrúa, quinceava Edic. P.223.

Someramente podemos conceptualizarlos de la siguiente manera:

- La conducta es todo hecho humano ya sea mediante una acción u omisión capaz de modificar el mundo exterior (El elemento físico del delito).
- La Tipicidad es el encuadramiento de una conducta con la descripción hecha en la ley.
- La antijuridicidad es la violación u oposición del valor o bien protegido por la ley.
- La culpabilidad es el nexo emocional e intelectual que une al sujeto con su acto.
- La imputabilidad es la facultad de atribuirle a un sujeto su conducta culpable.
- La punibilidad es la sanción que establece la Ley Penal al infractor de una norma.
- Las condiciones objetivas de punibilidad son las exigencias ocasionalmente establecidas por el legislador para que la pena tenga aplicación.
- Los elementos negativos constituyen la ausencia o negación de los ya descritos elementos positivos.

Una vez descritos los elementos indicados, se entrará al estudio y análisis de los mismos, como se le ha denominado por todos los conocedores como la "Teoría del Delito". Más adelante se hará el estudio a fondo de dichos elementos y la forma de manifestación en los delitos informáticos.

3.5.1. LA CONDUCTA HUMANA Y SU ELEMENTO NEGATIVO.

"La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito."[20] Por lo tanto podemos afirmar que solo el ser humano tiene relevancia para el ámbito de aplicación del derecho penal. Por lo que respecta a las personas morales, éstas no se consideran sujetos activos de los delitos por carecer de voluntad propia; mas sin embargo, pueden considerarse pasivos, especialmente cuando se presentan infracciones patrimoniales en su contra.

A) LA ACCION.- El vocablo acción proviene de la voz latina "actio", que significa movimiento. Se entiende como todo hecho humano capaz de modificar el mundo exterior. "La acción consiste en la conducta positiva, expresada mediante un hacer, una actividad, un movimiento corporal voluntario con violación a una norma prohibitiva".[21] De lo anterior podemos obtener los tres elementos de la acción los cuales son los siguientes:

[20] Castellanos Tena, Fernando. Op. cit. p. 149.
[21] Pavon Vasconselos, op. cit. pág. 186.

a). La manifestación de voluntad.- "Consiste en el peculiar comportamiento de un hombre que se traduce exteriormente en una actividad o inactividad voluntaria; es decir, la conducta consiste exclusivamente en una actividad o movimiento corporal, o bien una inactividad, una abstención, un no hacer.[22]

b). El resultado.- Comprende "tanto las modificaciones de orden físico, como las del orden jurídico y ético, tanto las cosas materiales como los estados de ánimo del sujeto pasivo y de la sociedad" (Maggiore); es "no sólo el cambio en el mundo material sino también mutación en el mundo psíquico y aun el riesgo o peligro (Jiménez de Asúa)."[23]

c). El nexo de causalidad.- "Entre la acción y el resultado debe de haber una relación de causa a efecto; y es causa tanto la actividad que produce inmediatamente el resultado como la que lo origina inmediatamente, o sea por elementos penalmente inoperantes per sé, pero cuya eficacia dañosa es aprovechada."[24]

B) LA OMISION.- Consiste en dejar de hacer lo que se debe de realizar, es decir, se deja de hacer algo que se encuentra ordenado por la ley; es una inactividad, una abstención. "La omisión es conducta negativa, es inactividad voluntaria de una norma preceptiva (omisión simple, o de esta)."[25] Se clasifica en dos tipos:

a) Omisión simple.- Es el hacer culposo o involuntario en el que se viola una ley preceptiva y se produce un resultado jurídico no material.

b) Comisión por omisión.- Consiste en una doble violación a una ley prohibitiva y a otra preceptiva, es decir, se presentan dos tipos de conducta, por un lado el hacer y por el otro un no hacer, produciendo con esto un resultado jurídico y otro material, existiendo entre ambos una relación causal.

C) LA AUSENCIA DE CONDUCTA (*nullum crimen sine actione*).- Consiste en el aspecto negativo del primer elemento del delito, para la ejecución de un delito es necesaria la presencia de una conducta humana, y si ésta faltara, no se configuraría el delito.

"Es unánime el pensamiento, en el sentido de considerar como factores eliminatorios de la conducta a la *vis maior* (fuerza mayor) y a los *movimientos reflejos*.

---

[22] González Quintanilla, José Arturo, Derecho penal Mexicano, parte general, Edit. Porrúa, México. 1991 pág. 182.
[23] Carranca y Trujillo, Raúl, op. cit. p. 263.
[24] Ibidem, p. 263.
[25] Ibidem, p. 187.

Entre nosotros estas causan adquieren carácter supra legal, por no estar expresamente detectadas en la ley, pero pueden operar, porque su presencia demuestra la falta del elemento volitivo, indispensable para la aparición de la conducta que, como hemos dicho, es siempre un comportamiento humano voluntario. Solo resta añadir que las *vis absoluta* y la *vis maior* difieren por razón de su procedencia; la primera deriva del hombre y la segunda de la naturaleza, es decir, es energía no humana. Los actos reflejos son movimientos corporales involuntarios (si el sujeto puede controlarlos o por lo menos retardarlos, ya no funcionan como factores negativos del delito)."[26]

Ahora bien, una vez analizado lo anterior, podemos afirmar que dentro de los llamados "delitos informáticos", la conducta siempre va a estar manifestada mediante una acción, y nunca por omisión, en razón de que forzosamente para el funcionamiento de una computadora, es indispensable que el hombre haga uso de ella (desde encenderla hasta apagarla), le señale una serie de instrucciones y ordenamientos técnicos y lógicos a través de los comandos, y una vez realizado esto, obtendrá el resultado físico deseado que sería el "delito informático" por el operador de la máquina. Se puede observar que la relación de causalidad o el nexo causal si se presenta en los delitos informáticos, porque existe una conducta de hacer, y un resultado físico u objetivo.

En ese orden de ideas, la ausencia de la conducta en los delitos informáticos solo opera cuando *existe vis absoluta*, en razón de que para cometer un delito informático es sumamente necesario los conocimientos técnicos sobre la ciencia informática y computacional, y por lo tanto puede presentarse la hipótesis en que un usuario tenga que realizar cierto tipo de conducta por causa de *vis absoluta*, y si somos extremistas, en el caso de que una persona en estado de hipnótico lleve a cabo una conducta delictiva, existe también una ausencia de conducta. Por lo tanto este elemento negativo si se presentan en los delitos informáticos. recordar el principio de "*nullum crimen sine actione*".

SUJETOS DEL DELITO:

El sujeto activo: "Sólo el hombre es sujeto activo del delito, porque únicamente el se encuentra provisto de capacidad y voluntad y puede, con su acción u omisión, infringir el ordenamiento jurídico penal. Se dice que una persona es sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible, ya sea como autor intelectual, material, partícipe, cómplice o encubridor."[27]

---

[26] Castellanos Tena, Fernando. Op. cit. p. 164.

[27] Pavon Vasconcelos, Francisco, Derecho Penal Mexicano, Décima Edición, S.A., Edit. Porrúa. México, 1991 pág. 17.

Dentro de los llamados "delitos informáticos", el sujeto activo de la conducta no es un sujeto de rasgos comunes, sino de un especialista que tiene conocimientos amplios de la ciencia informática y computacional.

El sujeto pasivo: "Por tal se conoce al titular del derecho o interés lesionado o puesto en peligro por el delito."[28] Es el titular del derecho violado en su contra y que jurídicamente ese derecho está protegido por la norma. Por lo tanto es importante señalar en primer lugar, que debemos hacer una distinción sujeto pasivo ó víctima del delito, que es la persona sobre la cual recae la conducta de acción u omisión que realiza el sujeto activo.

Por lo tanto, en los denominados "delitos informáticos", es procedente afirmar que las víctimas pueden ser cualquier persona física como usuario de una computadora, las personas morales o jurídicas como las empresas creadoras de programas, distribuidoras de hardware y software, instituciones crédito, el Estado, los gobiernos, y en general la sociedad y cualquier persona que en sus labores usen sistemas automatizados de información, generalmente conectados a otros, y que resienta el daño en la comisión de un delito informático .

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen estos tipos de infractores, con el objeto de prever las acciones de prevención para el control de estos ilícitos.

EL BIEN U OBJETO DEL DELITO.

El Objeto material de un delito lo constituye la persona o cosa sobre quien recae el peligro o el daño, es decir, sobre la persona o cosa sobre quien recae de manera directa el acto o evento delictuoso. Dentro del mundo de la informática podemos señalar que son las computadoras, los usuarios y las empresas generadoras del Hardware y Software las que se pueden considerar como objeto material del delito.

El objeto jurídico protegido es la el bien salvaguardado por el Estado mediante la creación de la ley penal, con el propósito de resguardarlo y protegerlo de las conductas ilícitas. En el campo de los delitos informáticos existe una gran confusión de que si solamente es el patrimonio el único bien jurídico protegido, con lo cual se afirma de que no es solamente el patrimonio, sino también lo es el derecho a la intimidad y a la información confidencial.

---

[28] Cuello Calon, Eugenio. Derecho Penal I, 14a. Edición Barcelona, 1964 pág. 315.

3.5.2. LA TIPICIDAD Y SU ELEMENTO NEGATIVO.

Primeramente es importante analizar lo que dispone la Constitución Política de los estados Unidos Mexicanos en su artículo 14, que a la letra nos dice:

> **Art. 14.- "... En los juicios de orden criminal queda prohibido imponer por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trate..."**

Del análisis que se efectúa de ésta disposición constitucional, se puede deducir que si no existe el elemento de la Tipicidad, no puede considerarse una conducta aún siendo ilícita como delito; por lo tanto este es uno de los elementos indispensables para configurar un delito. En este orden de ideas es necesario hacer una distinción de lo que se conoce como Tipicidad y el Tipo.

A). TIPICIDAD.- Raúl Carranca y Trujillo nos define a la tipicidad como "la conformidad de una conducta con la hipótesis delictiva consignada en la ley penal."[29] Para el Doctor Jesús Martínez Garnelo, prominente jurista mexicano que se ha preocupado por este tema, nos define a la tipicidad de la siguiente manera: "Es el encuadramiento de una conducta con la descripción hecha en la ley, la adecuación de una conducta concreta con la descripción legal formulada en abstracto."[30] En otras palabras, tipicidad es el encuadramiento de una conducta en la descripción hecha por la Ley.

B). TIPO.- "Es la descripción legal de una conducta estimada como delito, que lesiona o hace peligrar bienes jurídicos protegidos por la norma penal; es una concepción legislativa, es la descripción de una conducta dentro de los preceptos penales."[31] En otras palabras, es la descripción que el Estado por medio de sus órganos realiza que una conducta sea prohibida en la Ley Penal.

A su vez, los tipos penales se clasifican atendiendo a su composición (normales y anormales); por su ordenación metodológica (Fundamentales o básicos, especiales y complementados); y en función de su autonomía o independencia (autónomos o independientes y subordinados).[32]

---

[29] Carranca y Trujillo, Raúl, op. cit. p. 171.
[30] Martínez Garnelo, Jesús. La Investigación Ministerial Previa. Primera edición. Edit. OGS Editores S.A. de C.V. pág. 15.
[31] Martínez Garnelo, Jesús. Op. cit. p. 15.
[32] Castellanos Tena, Fernando. Op. cit. pág.. 170-173.

Normales: Son aquellos que se limitan a hacer una descripción objetiva. (Como ejemplo encontramos el tipo penal de homicidio).

Anormales: Son aquellos que además de contener factores objetivos, contienen elementos subjetivos o normativos. (Como ejemplo encontramos al estupro).

Fundamentales: Son aquellos que constituyen la esencia o fundamento de otros tipos. (Ejemplo: homicidio).

Especiales: Se forman agregando otros requisitos a tipo fundamental, al cual subsumen. (Ejemplo: parricidio).

Complementados: Se constituyen al lado de un tipo básico y una circunstancia o peculiaridad distinta (ejemplo: Homicidio calificado).

Autónomos: Tienen vida por sí mismo (Robo simple)

Subordinados: Dependen de otro tipo (homicidio en riña).

C). AUSENCIA DE TIPICIDAD (ATIPICIDAD) Y DE TIPO.- Esta figura se presenta cuando no se reúnen todos y cada uno de los elementos del tipo penal, siendo ésta, el aspecto negativo del delito (atipicidad).

El Doctor Martínez Garnelo hace la distinción entre atipicidad y ausencia del tipo de la siguiente manera:

a) "Atipicidad: Supone una conducta que no llega a ser típica por falta de alguno o algunos de los elementos descriptivos del tipo, ya con referencia a calidades en los sujetos, de referencia temporales o espaciales, de elementos subjetivos, etc.
b) Ausencia de tipo: (Inexistencia del presupuesto general del delito). Esto presupone la ausencia total de la descripción. Se maneja cuando unánimemente se establece que no hay delito sin tipo legal, cuando el legislador no describe una conducta dentro de

> las leyes penales, tal conducta no es delito; hay ausencia del tipo, ya que no existe descripción legal de una conducta considerada como delictiva"[33].

Ahora bien, es precisamente el tema de la tipicidad de los delitos informáticos, el que nos hace reflexionar sobre la necesidad que existe no nada más en México, sino en todos los países del mundo, de la creación de normas jurídicas penales para la debida protección de los programas de cómputo; ya que hasta la fecha solo existe en algunos países la sanción por la **reproducción indebida de un programa de cómputo**, a través de las Leyes concernientes al régimen autoral o propiedad intelectual, dejando al margen de ello, todas las diversas conductas delictivas que pueden generarse con motivo de los conocimientos de la ciencia informática y computacional.

En nuestro país, desafortunadamente solo el Código Penal para el Estado de Sinaloa tipifica el delito informático en su artículo 217 que a la letra dice:

> "**Art. 217.-** Comete el delito informático, la persona que dolosamente y sin derecho:
>
> I.- Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el propósito de defraudar, obtener dinero, bienes informáticos; o
> II.- Intercepte, interfiera, reciba, use, altere, dañe, o destruya un soporte lógico o programa de computadora o los datos contenidos en las misma, en la base , sistema o red.
>
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa"[34].

De ésta disposición legal vigente, podemos señalar que los elementos del tipo penal son los siguientes:

a) La acción dolosa y sin derecho de una persona
b) Que tenga por objeto entrar, diseñar, ejecutar, alterar, defraudar, obtener dinero o bienes informáticos, interceptar, interferir, recibir, usar, dañar y destruir una base de datos, un sistema de computadoras o red de computadoras o cualquier parte de la misma.
c) Que realice todas esas conductas sin la autorización debida.
d) Que las conductas ilícitas las realizara por medio de una computadora o herramienta similar.

---

[33] Martínez Garnelo, Jesús. Op. cit. pág. 15.
[34] Código Penal Para el estado de Sinaloa, edit. Porrúa, Tercera edición. pag. 68.

Por cuanto hace a su clasificación, este delito se encuentra comprendido en la categoría de Normal (porque se limita a hace únicamente una descripción objetiva); Especial (porque se forman agregando otros requisitos al tipo fundamental, al cual subsumen, ya que casi todos los delitos informáticos tienden a lastimar el patrimonio ajeno, por lo cual se agregan ciertos requisitos como por ejemplo al fraude informático, al robo informático, a la destrucción o daño informático, etc.); y por último sería autónomo (ya que este tipo penal tiene vida por sí solo, no requiere de factores externos para su nacimiento).

Ya para finalizar el análisis de este elemento del delito, se puede afirmar que es precisamente la atipicidad y la ausencia del tipo lo que mas ha prevalecido y perjudicado a muchos países, especialmente donde se encuentran las grandes empresas creadoras de hardware y Software, ya que siempre será difícil encuadrar una conducta ilícita de la materia informática a un tipo penal descrito en las normas jurídicas penales vigentes.

3.5.3. LA ANTIJURIDICIDAD Y SU ELEMENTO NEGATIVO.

A) ANTIJURIDICIDAD.- Para el Maestro Pavón Vasconcelos la antijuridicidad "es un desvalor jurídico, una contradicción o desacuerdo entre el hecho del hombre y las normas del Derecho."[35] Por su parte Raúl Carranca y Trujillo nos define la antijuridicidad como: "la oposición a las normas de cultura, reconocidas por el estado."[36]

En otras palabras, la antijuridicidad es la incompatibilidad de una conducta hacia el orden jurídico establecido. Atento a lo anterior, "una acción es antijurídica cuando constituye un ataque a un bien jurídico (menoscabándolo, poniéndolo en peligro) protegido por el mandato, no se adecua a una finalidad admitida o impuesta por el derecho; en otras palabras: es antijurídico el ataque a un bien jurídico protegido, no admitido por el derecho."[37]

Algunos doctrinarios como Franz Von Lisz y Cuello Calón han manifestado que la antijuridicidad maneja dos aspectos:

- **Formal:** Consiste en que la conducta ilícita transgreda a una norma establecida por el Estado; o en otras palabras, es la rebeldía contra la norma jurídica.
- **Material:** Se presenta cuando la conducta ilícita signifique contradicción a los intereses colectivos; o en otras palabras, que dicha conducta ha causado un daño o perjuicio social por esa rebeldía.[38]

---

[35] Pavon Vasconselos, op. cit. pág. 295.
[36] Carranca y Trujillo, Raúl, op. cit. pág. 337.
[37] Martínez Garnelo, Jesús. Op. cit. p. 22.
[38] Citados por Castellanos Tena, Fernando. Op. cit. p. 180.

B) AUSENCIA DE ANTIJURIDICIDAD (causas de justificación).- Cuando se presenta alguna causa o circunstancia en una conducta típica, imputable, punible pero exista ausencia de antijuridicidad o alguna causa de justificación, no se configura el delito por faltar este elemento imprescindible.

Enrique Bacigalupo, nos señala en forma clara que las causas de justificación son "la autorización para la realización de un comportamiento típico. Decir que un comportamiento está justificado, equivale a afirmar que el autor de la acción típica dispuso de un permiso del orden jurídico para obrar como obró."[39]

Dentro del Régimen penal mexicano, son causas de justificación las siguientes:

a). Legítima defensa.- "Es la repulsa de una agresión antijurídica y actual por el atacado o por terceras personas contra el agresor, sin traspasar la medida necesaria para la protección."[40]

b). Estado de necesidad.- "Es la situación en que se encuentra un sujeto en la que como medio necesario para evitar la pérdida de bienes jurídicos propios (o de un tercero en determinados casos), ataca a un bien jurídico extraño de menor cantidad que el que trata de salvar".[41]

c). Legítimo ejercicio de un derecho.- "Son aquellos casos en que media una prohibición porque en las restantes basta con el propósito de reserva de la ley penal o de la Constitución. Son causas de justificación que emergen de cualquier otra parte del orden jurídico."[42]

d). Cumplimiento de un deber.- Se presenta cuando las personas en ejercicio de su función cumplen con la obligación que se encuentra consagrada en la ley, pero realizan un menoscabo en una esfera jurídica ajena.

e). Impedimento Legítimo.- Se presenta cuando una persona realiza una conducta omisiva por atender a un interés preponderantemente superior, y que ese interés se encuentre protegido por la Ley.

Una vez analizado lo anterior, y al igual que lo estudiado y expresado en el tema de la tipicidad, podemos encontrar que el elemento antijurídico del delito, todavía no reúne los requisitos básicos para la debida protección de los programas de cómputo y de

[39] Citado por González Quintanilla, José Arturo, p. 271.
[40] Ibidem, p. 192.
[41] Martínez Garnelo, Jesús. Op. cit. p. 22.
[42] Ibidem, p. 27.

los ya muy mencionados delitos informáticos, en virtud de que no existe disposición legal en México(salvo en el estado de Sinaloa como ya ha quedado expresado), que señale las conductas ilícitas de los delincuentes informáticos, y dichas conductas consideradas como antijurídicas, motivo por el cual existe una gran problemática en el ámbito del derecho penal al querer encuadrar la conducta referida en los llamados "delitos clásicos", tales como el robo, fraude etc., lo que genera una gran confusión y una gran dificultad al momento de pretender acreditar la antijuridicidad del acto realizado por un delincuente informático.

No obstante lo anterior, también es procedente señalar que una vez que sean debidamente tipificados los delitos informáticos, en ellos se puede presentar la causa de justificación que se hizo referencia como el ejercicio de un derecho, en razón de que puede presentarse la hipótesis de que una persona ejerciendo un derecho legítimo, realice actos de reproducción de un programa de cómputo que el mismo haya creado y que dicha creación se encuentre protegida por el derecho de autor. Así también puede presentarse la causa de justificación del estado de necesidad, cuando se encuentre amenazado de muerte un usuario y lo obligan a realizar una conducta ilícita como ingresar sin autorización a una red de una determinada empresa.

3.5.4. LA CULPABILIDAD Y SU ELEMENTO NEGATIVO.

Una conducta no solo será delictuosa cuando sea típica y antijurídica, sino además debe existir una reprochabilidad hacia un sujeto por haber cometido un delito o haberse conducido contrario a la norma penal previamente establecida.

A). LA CULPABILIDAD.- Para Francisco Pavón Vasconcelos, la culpabilidad es "el reproche hecho al autor sobre su conducta antijurídica."[43] Por su parte, Castellano Tena nos señala que la culpabilidad es "el nexo intelectual y emocional que liga al sujeto con su acto"[44]

El elemento de la culpabilidad se manifiesta de las siguientes formas:

a). El dolo.- Esta forma de culpabilidad se presenta cuando el sujeto activo realiza una conducta voluntaria con el propósito de realizar un daño o cometer un delito, es decir: "el sujeto activo ha representado en su mente la conducta que va a realizar y el resultado de esa conducta y decide en su acto la voluntad de llevar a cabo lo que en su mente representa."[45] Por lo tanto sus elementos consisten en:

[43] Pavon Vasconselos, Francisco, op. cit. p. 359.
[44] Castellanos Tena, Fernando. Op. cit. p. 234.
[45] Martínez Garnelo, Jesús. Op. cit. p. 31.

- Elemento moral o cognoscitivo.
- Elemento volitivo o psicológico.

A su vez, en dolo se clasifica en:

1.- Dolo directo: El resultado es el mismo a aquel que hubiera previsto y deseado el sujeto activo de la conducta. Ejemplo: Un sujeto desea cometer un homicidio a determinada persona y lo realiza tal como lo había planeado.
2.- Dolo indirecto: Este se presenta cuando el sujeto activo desea una conducta delictiva, la lleva a cabo y prevé que el resultado de su conducta va a ir más allá de lo que el está deseando. Ejemplo: Cuando una persona quiere matar a otra, y utiliza una bomba en el cine donde está esta persona, si bien es cierto sabe que se va a cometer el homicidio, también lo es que está consciente de cuantas personas van a morir en la explosión de dicho artefacto.
3.- Dolo indeterminado.- Es la voluntad de delinquir sin fijarse en el resultado o daño que se realizará. Ejemplo: las personas que quieren delinquir sin importar que tipo de delito y que daño realizarán, lanzar una bomba a la intemperie.
4.- Dolo eventual.- Se presenta cuando el sujeto desea cometer un delito, pero no prevé la posibilidad de que nazcan a la vida jurídica otros delitos, pero en caso de que se presentara este supuesto, acepta que los mismos ocurran.

b). La culpa.- Cuando el activo no desea realizar una conducta que lleve a un resultado delictivo, pero por un actuar imprudente, negligente, carente de atención, cuidados y reflexión, verifica una conducta que produce un resultado previsible o no intencional.[46] . Los elementos de la culpa son los siguientes:

- Acción u Omisión,
- Incumplimiento o determinación de un deber de cuidado,
- Resultado típico, previsible y evitable,
- Ausencia de voluntad de causar daño,
- Nexo causal entre la conducta y el resultado,
- Principio de confianza.

A su vez, la culpa se clasifica en:

- Culpa consciente, con previsión o representación: Existe cuando el agente ha previsto el resultado típico como posible, pero no solamente no lo quiere, sino que abriga la esperanza de que no ocurrirá.[47] Ejemplo: La persona que maneja un automóvil con alguna falla mecánica.

[46] Martínez Garnelo, Jesús. Op. cit. p. 33.
[47] Castellanos Tena, Fernando. Op. cit. pág. 247.

- Culpa inconsciente, sin previsión o sin representación: se presenta cuando no se prevé un resultado previsible. Existe voluntariedad de la conducta causal, pero no hay representación del resultado de naturaleza previsible.[48] Ejemplo: el caso de que una persona limpie su pistola en presencia de otras.

c). La preterintención.- Es una suma de dolo y culpa, una conducta que tiene un inicio doloso o intencional y una culminación culposa o imprudencial.[49]

Por último es importante anotar lo que nos dice el Código Penal para el Distrito y Territorios Federales en Materia de Fuero Común, y para toda la República en Materia del Fuero Federal en su artículo noveno, que a la letra dice:

> **"ARTICULO 9o.**- Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley, y
>
> Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales."

B). LA INCULPABILIDAD.- Esta figura se presenta como el aspecto negativo de la culpabilidad. Se presenta cuando una persona actúa en forma aparentemente delictuosa pero no se le puede reprochar su conducta por existir una causa de culpabilidad que se refiere a la voluntad en la realización de la conducta como el caso del error de hecho y en términos generales la reacción sobre la voluntad.[50]

Las causas de inculpabilidad mas frecuentes en el ámbito jurídico son las siguientes:

a) El error: "Es un vicio psicológico consistente en la falta de conformidad entre el sujeto cognoscente y el objeto conocido, tal como este es en la realidad. El error es un falso conocimiento de la verdad, un conocimiento incorrecto; se conoce, pero se conoce equivocadamente."[51] El error se subdivide a su vez en error de derecho (cuando el sujeto activo actúa de manera antijurídica creyendo que lo hace lícitamente), y el error de hecho (este se presenta cuando el sujeto activo confunde la finalidad de su conducta, o el objeto jurídico protegido no es el mismo que pretende quebrantar el sujeto activo).

---

[48] Ibidem, pág. 247.
[49] Martínez Garnelo, Jesús. Op. cit. pág. 36.
[50] Martínez Garnelo, Jesús. Op. cit. p. 30.
[51] Castellanos Tena, Fernando. Op. cit. p. 259.

b) Coacción sobre la voluntad.- Esta se presenta cuando el sujeto activo actúa bajo una presión física o moral, ejecutando una conducta delictiva. Si bien la conducta es culpable existen estas circunstancias que la colocan en los elementos de la inculpabilidad (ejemplo: la obediencia jerárquica, legitima defensa putativa, el estado de necesidad de bienes de igual jerarquía, el temor fundado).

Como ha quedado manifestado en la presente tesis, son poco los países que tienen tipificado el "delito informático", y es por ello que muchas de las conductas ilícitas realizadas por los conocedores de la materia pasan inadvertidas dentro del ámbito jurídico, y consecuentemente, esas conductas no son consideradas como culpables. Y más aún, en aquellos países como Francia, Estados Unidos, Japón y España, países que van a la vanguardia en este tema, representa una gran dificultad demostrar la conducta culpable de un usuario que mediante un equipo de cómputo, realice alguna acción informática en perjuicio del patrimonio de otra persona.

Ahora bien, una vez analizado el elemento de la culpabilidad, es pertinente señalar que para que exista la conducta culpable, es necesaria la acción dolosa en su máximo esplendor, debe de existir una voluntad manifiesta por parte del infractor para cometer este tipo de delitos, en resumen, debe de ser un dolo directo, toda vez que la persona que ejecuta el acto es un conocedor de la materia y sabe muy bien que es lo que está realizando, por lo que no hay lugar para una forma de conducta como la culpa o preterintención.

El sujeto activo de este delito como se ha venido manifestando, es un conocedor de la materia, cuenta con una habilidad insuperable, y sabe muy bien específicamente la conducta que esta realizando, ya sea una alteración a una red informática de una empresa, así como la reproducción indebida de programas de cómputo etc., por lo que se afirma que debe de ser una conducta dolosa directa en la comisión de este tipo de delitos.

Así también, las causas de inculpabilidad se presentan en los delitos informáticos, específicamente con el error de hecho, ya que es muy frecuente que una persona esté utilizando programas de cómputo reproducidos de manera clandestina, lo cual no es conocimiento de un usuario que ejecuta este programa en una computadora.

3.5.5. LA IMPUTABILIDAD Y SU ELEMENTO NEGATIVO.

A). LA IMPUTABILIDAD. El Maestro **Castellanos Tena,** define la Imputabilidad como la posibilidad condicionada por la salud mental y por el desarrollo del autor, para obrar según el justo conocimiento del deber existente. En otras palabras, podemos definir la imputabilidad como la capacidad de entender y de querer en el campo

del derecho penal.[52]

Por otro lado, el Maestro **Jiménez de Asúa** explica qué "Imputar un hecho a un individuo es atribuírselo para hacerle sufrir las consecuencias, es decir, para hacerle responsable de el, puesto que de tal hecho es culpable".[53]

Por ello, la noción de Imputabilidad requiere no solo el querer del sujeto, sino además su capacidad de entendimiento, pues únicamente quien por su desarrollo y salud mental es capaz de representar el hecho, conocer su significación y mover su voluntad al fin concreto de violación de la norma, puede ser reprochado en el juicio integrante de la culpabilidad.

B). LA INIMPUTABILIDAD. El Maestro **Pavon Vasconcelos**, define a la inimputabilidad, como la incapacidad para conocer la ilicitud del hecho o bien para determinarse en forma espontánea conforme a esa comprensión.[54]

Las causas de Inimputabilidad son las siguientes:

- Minoría de edad.
- Trastorno mental.
- Desarrollo intelectual retardado.
- Miedo grave.[55]

3.5.6. LA PUNIBILIDAD Y SU ELEMENTO NEGATIVO.

Frecuentemente se confunden las nociones que en seguida se distinguirán, toda vez que, a pesar de emplearse indiscriminadamente como voces sinónimas, cada una de ellas tiene un significado propio. Tal distinción servirá para manejar de manera adecuada la terminología respectiva.

> **"Noción de Punibilidad.** Es la amenaza de una pena que contempla la ley para aplicarse cuando se viole la norma.
> **Punición.** Consiste en determinar la pena exacta al sujeto que ha resultado responsable de un delito concreto.
> **Pena.** Es la restricción o privación de derechos que se impone al autor de un delito. Implica el castigo para el delincuente y una

[52] Castellanos Tena, Fernando. Op. cit. Pág. 218.
[53] Jimenez de Asua, Op. cit. Pág. 325.
[54] Pavon Vasconcelos, Op. cit. Pág. 375.
[55] Osorio y Nieto, Op.cit. Pág. 63.

protección para la sociedad.

Sanción. De manera genérica, el término sanción se usa como sinónimo de pena, pero propiamente, aquel corresponde a otras ramas del derecho y llega a ser un castigo o carga a que se hace merecedor, quien quebranta una disposición no penal. La sanción es propiamente impuesta por una autoridad administrativa, por ejemplo, multa, clausura, etc. Debe tenerse presente que no se podrá imponer una pena si previamente no existe una ley que la establezca"[56].

A). 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".[57]

B). LAS EXCUSAS ABSOLUTORIAS. Constituyen la razón o fundamento que el legislador considero para que un delito a pesar de haberse integrado en su totalidad, carezca de punibilidad.[58]

Raúl Carranca y Trujillo las define así: "Son las circunstancias en las que, a pesar de subsistir la antijuridicidad y la culpabilidad, queda excluida desde el primer momento la posibilidad de imponer la pena al autor."[59]

El maestro **Pavón Vasconcelos**, explica que "las causas de impunidad de la conducta o del hecho típico, antijurídico y culpable denominado excusas absolutorias, constituyen el aspecto negativo de la punibilidad y originan la inexistencia del delito.[60]

Por ejemplo, en el artículo 73 del Código Penal Federal, establece que no se impondrá sanción alguna, lo cual procede en razón del arrepentimiento del sujeto activo y de su mínima temibilidad; "cuando el valor de lo robado no pase de 10 veces el salario, y sea restituido por el infractor espontáneamente y pague éste todos los daños y perjuicios antes de que la autoridad tome conocimientos del delito, no se impondrá sanción alguna si no se ha ejecutado el robo por medio de la violencia". Además de los artículos 55, 333, 334, 375, 379 y 400 del Código Penal Federal.

---

[56] Amuchategui Requena, Irma G. Derecho Penal. Curso 1ero. y 2do. Colección de textos jurídicos universitarios Editorial Harla, Págs. 90-91.
[57] Castellanos Tena, Op. cit. Pág. 267.
[58] Amuchategui Requena, Irma G. Págs. 92.
[59] Carranca y Trujillo, Raúl. Op.cit. Pág. 651.
[60] Pavón Vasconcelos. Op. cit. Pág. 459.

3.5.7. LA CONDICIONALIDAD OBJETIVA Y SU ELEMENTO NEGATIVO.

El maestro **Castellanos Tena,** define a las condiciones objetivas de punibilidad "como aquellas exigencias ocasionalmente establecidas por el legislador para que la pena tenga aplicación".[61]

A). LAS CONDICIONES OBJETIVAS DE PUNIBILIDAD. No son elementos esenciales del delito, sino son una circunstancia, un dato, que debe darse para que opere la punibilidad, pero sin que sea elemento del delito. La condicionalidad objetiva esta constituida por requisitos que la ley señala eventualmente para que se pueda perseguir el delito. Algunos autores dicen que son requisitos de procedibilidad o perseguibilidad, mientras que para otros son simples circunstancias o hechos adicionales, exigibles, y para otros más constituyen un auténtico elemento del delito.

Jiménez de Asúa, quien los denomina condiciones objetivas de punibilidad, afirma: ". . . son presupuestos procesales a los que a menudo se subordinan la persecución de ciertas figuras de delito . . . ".[62]

B). AUSENCIA DE CONDICIONALIDAD OBJETIVA. La ausencia de condicionalidad objetiva llega a ser el aspecto negativo de las condiciones objetivas de punibilidad. La carencia de ellas hace que el delito no se castigue.

Cuando en la conducta concreta falta la condición objetiva de punibilidad, es obvio que no puede castigarse; pero así como la carencia de acto, la atipicidad, la justificación, la inimputabilidad, la inculpabilidad y las excusas absolutorias hacen para siempre imposible perseguir el hecho.[63]

---

[61] Castellanos Tena. Op.cit. Pág. 271.
[62] Jiménez de Asúa. La ley y el delito. 10 ed. Sudamericana, Buenos Aires. 1980. Pág. 425.
[63] Ibidem. Op. cit. Pág. 425.

CAPITULO IV.
INTERNET Y EL DELINCUENTE INFORMATICO.

SUMARIO: 4.1. NOCIONES GENERALES. 4.2. CARACTERISTICAS DEL DELINCUENTE INFORMATICO. 4.3. FORMA BASICA DE OPERAR DE UN DELINCUENTE INFORMATICO. 4.4. HACKING/ CRACKING/ PHREAKING EN EL CÓDIGO PENAL ESPAÑOL. 4.5. CASOS FAMOSOS DE ALGUNOS DELITOS INFORMATICOS Y SUS AUTORES. 4.6. EL CRIMEN INFORMATICO. 4.7. RESUMEN DEL COMUNICADO DE LA COMISION AL PARLAMENTO EUROPEO. 4.7.1. Argumentos a favor de la regulación técnico-jurídica en Internet. 4.7.2. Argumentos en contra de la regulación técnico-jurídica en Internet. 4.7.3. Autorregulación: Códigos de conducta, sistemas de seguridad informática y los ciberpolicías.

4.1. NOCIONES GENERALES.

El delincuente informático (hackers y crackers, denominación que se les otorga en el ámbito internacional), es uno de los temas mas candentes dentro de los denominados "delitos informáticos", ya que mientras existen criterios de especialistas de la Ciencia informática y computacional que los protegen, en el área jurídica, específicamente en la propiedad intelectual y derechos de autor, existe la postura de deben ser castigados severamente por el gran número de ilícitos que cometen a diario mediante la utilización de sus conocimientos computacionales.

Desde finales de la década de los 70s, cuando se introdujo al mercado la computadora personal (PC), la acción de estos sujetos ha crecido en proporciones asombrosas y, en una proporción semejante, también han crecido quienes los catalogan de tecno-criminales, así como también aquellos que los consideran rebeldes positivos, que luchan para que los adelantos tecnológicos en materia de la informática y computación lleguen a las manos no solo de los poderosos, sino también a cualquier tipo de usuario de una computadora.

Diversos especialistas de la informática señalan que a pesar de las actividades clandestinas de los hackers, éstos representan una subcultura revolucionaria que juega un papel muy importante para el desarrollo tecnológico. Y así, uno de los lemas principales de este tipo de personas es el siguiente: El conocimiento y la información son poder, por lo tanto deben utilizarse abiertamente por todos, de manera que la creatividad e ingeniosidad deben ser venerados para alcanzar el ideal de una sociedad electrónica donde la información será libre e incontrolada.

Existe una distinción entre el delincuente informático que se dedica únicamente al pasatiempo y diversión, y aquel que se dedica exclusivamente al perjuicio de otras personas, ya sean físicas o morales.

El Hackers es aquella persona que incursiona en los sistemas operativos informáticos con ánimos de entretenimiento, o simplemente para probar sus habilidades, sin objetivo de lucro o perjuicio a lo ajeno, es decir, un hackers es la persona que además de programar su computadora, se introduce en los sistemas operativos y a los programas para descubrir de que manera funcionan, sean dichos programas propios o ajenos. Mientras que el Crackers (rompedor), son aquellas personas que se introducen en los sistemas o redes ajenas con el propósito de desvirtuar, destruir información o robar aquella que resulte de interés económico.

4.2. CARACTERISTICAS DEL DELINCUENTE INFORMATICO.

Contrario a la mayoría de delitos que se encuentran tipificados en las Leyes Penales de todos los países del mundo, el perfil del delincuente informático posee cierta configuración y virtudes que lo hacen único dentro de este enfoque, todo ello en razón a las características siguientes:

a) Hasta cierto grado, se han descubierto una serie de patrones que van desde la apariencia hasta sus hábitos de lectura. Es el sujeto típico inteligente, abstraído y apasionado por la ciencia informática y computacional.
b) Su conducta delictiva no tiene un alto grado de peligrosidad, como en los delitos donde existe una violencia física o moral, ya que un delincuente informático al realizar la comisión de un delito, no utiliza violencia.
c) Su personalidad es original y única, es decir, poseen una inteligencia superior a la normal, y además tienen una gran preparación especial en la materia informática y computacional.
d) Poseen una imaginación extraordinaria, compleja y muy exuberante, es decir, son muy despiertos, impacientes, audaces y aventureros.
e) Son personas que generalmente no tienen antecedentes penales, y que llevan una vida laboral y estable.
f) La gran mayoría de ellos son personas de un nivel económico muy elevado.
g) Así también físicamente poseen similitudes como:
1) Tienden a ser delgados
2) Su piel es pálida.
3) En su mayoría son varones
4) Normalmente son de ascendencia sajona y oriental
5) Visten de manera informal.
6) La mayoría tienen cabello corto, barba y bigote.
7) Usan lentes.
8) Como complemento a su imagen, siempre traen consigo un portafolios.

h) Todos poseen una educación universitaria y el manejo de herramientas técnicos, pero la mayoría de ellos son autodidactas. [64]

4.3. FORMA BASICA DE OPERAR DE UN DELINCUENTE INFORMATICO.

Las tecnologías de la información han facilitado la aparición de nuevas conductas que, con independencia del mayor o menor reproche social generado, han obligado a los países avanzados a adaptar sus legislaciones para dar cabida a modalidades comisivas que no existían hace unos años. A su vez, el auge de Internet ha ayudado a difundir las técnicas utilizadas, de manera que pueden encontrarse webs especializados en cada una de las "disciplinas", en los que tanto los aficionados como los más expertos pueden encontrar manuales de instrucciones, esquemas, programas y todo tipo de utilidades para la práctica del llamado Hacking/ Cracking/ Phreaking (H/C/P)

Con el término "hacking" nos referimos, en este caso, a la técnica consistente en acceder a un sistema informático sin autorización. Entendemos que existe autorización cuando el sistema está conectado a una red pública y no dispone de un control de acceso mediante el uso de identificadores de usuario y passwords.

Al hablar de "cracks" nos referimos a los programas o rutinas que permiten inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática. Dentro de las numerosos tipos de crack existentes, destacan los que permiten seguir utilizando un programa de demostración una vez superado el periodo de prueba establecido. También existen cracks que eliminan la llamada del programa a una llave electrónica, disco llave o número de serie.

Finalmente, en el concepto "phreaking" entrarían las técnicas de fraude en materia de telefonía analógica y digital. Uno de los métodos más utilizados en su día fue el de las denominadas "cajas de colores", que emitían distintas frecuencias, en función del resultado perseguido. Por ejemplo, las cajas azules utilizaban la frecuencia de 2600 hercios empleada por los operadores telefónicos para efectuar llamadas sin cargo.

4.4. HACKING/ CRACKING/ PHREAKING EN EL CÓDIGO PENAL ESPAÑOL.

El ordenamiento jurídico español, como uno de los países precursores en esta materia, ha recibido una importante actualización en el Código Penal de 1995, que incluye gran variedad y modalidades de los delitos informáticos.

---

[64] REVISTA MECANICA POPULAR, Año 55, Núm. 4, Abril 1998, Televisa S.A., México, p. 51.

A). HACKING. En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia. El artículo 197 extiende el ámbito de aplicación de este delito a las siguientes conductas:

- Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.
- Interceptación de las telecomunicaciones, en las mismas condiciones.
- Utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos.

Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad. La pena que se establece es de prisión, de uno a cuatro años y multa de doce a veinticuatro meses (Con el nuevo concepto de días-multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas). También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

El Código Penal de 1995 introduce el concepto de la estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. El artículo 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos. El Código Penal anterior sólo preveía la destrucción de bienes materiales, por lo que los daños causados en bienes inmateriales no quedaba incluida en dicho delito.

El artículo 239 considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

B). CRACKS. El artículo 270 incluye en la categoría de los delitos contra la propiedad intelectual la fabricación, *puesta en circulación y tenencia de cualquier medio* específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

C). PHREAKING. Además de la aplicación del régimen correspondiente a las defraudaciones y a las estafas electrónicas, este tipo de delitos podría encuadrarse en el artículo 256, que castiga el uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular.

4.5. ALGUNOS CASOS FAMOSOS DE DELITOS INFORMATICOS Y SUS AUTORES.

A). En septiembre de 1970, John Draper (después conocido como "Capitán Crunch"), descubre que el silbato obsequiado con el cereal del mismo nombre duplica a la perfección la frecuencia 2600 de un Sistema de Telecomunicaciones de Area Amplia. Esto le permitió realizar llamadas telefónicas gratuitas.

B). En julio de 1981, Ian Murphy ingresa al sistema de la Casa Blanca, del pentágono, de la Corporación BellSouth y de TRW, y en todas deja una solicitud de empleo.

C). En Diciembre de 1992, Kevin Poulsen es acusado de robar varias órdenes de misiones de la Fuerza Aérea.

D). Probablemente el mas célebre, entre junio y Agosto de 1994, Vladimir Levin, un programador de 24 años de San Petersburgo, la antigua Leningrado, logró romper los Códigos de Seguridad nada mas y nada menos que del "Citibank" de Nueva York, obteniendo según expertos, una bolsa aproximada de U.S. $ 12 millones.

E). En Febrero de 1998. Dos adolescentes de San francisco ingresan al sistema del Pentágono cuando todo parece presagiar una nueva guerra con Irak. Según fuentes oficiales, no entraron a redes confidenciales, sino a otras áreas semiclasificadas.

F). Kevin Mitnick, bautizado en 1996, como el cracker del siglo, y preso sin juicio desde hace tres años en una cárcel federal de los Angeles. Un caso bastante excepcional.

G). El 17 de febrero de 1998, el fiscal federal de Nueva Jersey, acusó oficialmente a Timothy Lloyd de haber dejado en el sistema de la empresa para la cual trabajaba hasta el 10 de julio de 1996, una "Bomba de tiempo virtual", un programa que destruyo todos los soportes lógicos de diseño y de producción de la compañía.[65]

[65] REVISTA MECANICA POPULAR, Año 55, Núm. 4, Abril 1998, Televisa S.A., México, p. 75.

4.6. EL CRIMEN INFORMATICO.

El crimen informático aumenta con delitos que van desde robos de computadoras portátiles hasta millonarias estafas a través de Internet, según un resultado del Instituto de Seguridad informática de los USA.

En la tercer encuesta anual de San Francisco, El Instituto de Seguridad Informática entrevistó a 520 especialistas de compañías, agencias de gobierno, grupos financieros y universidades de Estados Unidos, y consideraron que el mundo electrónico se vuelve cada vez más peligroso. Un 64 por ciento de quienes contestaron reportaron haber sufrido violaciones de seguridad en los últimos 12 meses. La mayoría de las víctimas de los crímenes informáticos no pueden calcular cuánto dinero perdieron por culpa de los cyber ladrones. Sin embargo, 241 organizaciones hablaron de pérdidas por unos 136 millones de dólares.

La directora del instituto, Patrice Rapalus, dijo que los hallazgos de la encuesta respecto a pérdidas financieras por problemas de seguridad muestran que no se está haciendo lo suficiente para controlar la delincuencia informática.

Y como ejemplo de ello, cabe señalar lo sucedido a la Oficina Federal de Investigaciones (FBI) la cual detuvo a dos adolescentes por una serie de "asaltos" informáticos a 11 computadoras militares de Estados Unidos. Las investigaciones prosiguen y ninguno de los adolescentes fue arrestado. Sin embargo, funcionarios del gobierno dijeron que la facilidad con la que dos colegiales tuvieron acceso a vitales sistemas del gobierno, fue una alerta sobre la debilidad de las redes informáticas oficiales y corporativas.

El agente especial del FBI a cargo de seguridad informática en San Francisco, Robert Walsh, declaró que un problema parecía ser la resistencia de las compañías a recurrir a la ley cuando sufren delitos electrónicos, probablemente por la publicidad negativa que atraería la misma. Sin embargo, el FBI ha investigado exitosamente y resuelto muchos casos en los que se denuncian crímenes informáticos, con una exposición pública mínima o nula de la compañía víctima.

Por otro lado, el Instituto de Seguridad Informática informó que las organizaciones consultadas reportaron 11.2 millones de dólares en pérdidas por fraudes financieros, 17.2 millones por fraudes de telecomunicaciones, 33.5 millones debido a robos de información de propietarios, 2.1 millones por sabotaje de datos o redes y 5.2 millones por robos de computadoras portátiles y que las pérdidas totales durante los dos últimos años suman 236 millones de dólares. Además muchos de los que respondieron dudaron de si el espionaje de alta tecnología era responsabilidad de gobiernos extranjeros o de

competidores extranjeros. Dos tercios de los consultados consideraron "no probable" que los ataques fueran originados en el exterior.

4.7. RESUMEN DEL COMUNICADO DE LA COMISIÓN AL PARLAMENTO EUROPEO.

El potencial de aprovechamiento de Internet para la información, la educación, el entretenimiento y la actividad económica a escala mundial es muy importante. Por ello, es necesario garantizar un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público.

Por lo que respecta a la distribución de contenidos ilícitos en Internet, corresponde a los Estados miembros garantizar la aplicación de la legislación existente, ya que por la característica "transnacional de Internet", se han de proponer medidas concretas en el ámbito de Justicia para intensificar la cooperación entre los Estados miembros. Internet no se encuentra en un vacío jurídico, ya que todas las partes interesadas (los autores, los suministradores de contenidos, los suministradores de servicios de ordenador central que almacenan los documentos y los transmiten, los operadores de red, los suministradores de acceso y los usuarios finales) están sujetos a las legislaciones de los Estados miembros respectivos.

Los suministradores de acceso a Internet y los suministradores de servicios de ordenador central desempeñan un papel decisivo para dar acceso a los usuarios a los contenidos de Internet. Sin embargo, no se ha de olvidar que la responsabilidad primordial de los contenidos recae sobre los autores y los suministradores de contenidos. Por ello es imprescindible señalar con exactitud la cadena de responsabilidades con el fin de situar la responsabilidad de los contenidos ilícitos en sus creadores.

Algunos países, como Alemania, han introducido una legislación muy amplia para bloquear todo acceso directo a Internet a través de los suministradores de acceso mediante la introducción de la exigencia de servidores "proxy" análogos a los que utilizan las grandes organizaciones por razones de seguridad, junto con "listas negras" centralizadas.

Por otro lado, la norma PICS (Plataforma de Selección de Contenidos de Internet), que lanzó oficialmente el World Wide Web Consortium (www), constituye un intento de establecimiento de una norma mundial para toda la industria. PICS ofrece un "control del acceso a Internet con censura", está apoyada por una amplia asociación de fabricantes de material y programas informáticos, suministradores de acceso, servicios comerciales en línea, editores y suministradores de contenido.

Actualmente se incluye como característica normal de la última generación de navegadores de Internet, como Microsoft Explorer 3.0 y Netscape 3.0, y también cuenta con el apoyo de una serie de conjuntos de programas de filtrado. Los productores de contenidos deberán de cooperar con este sistema mediante la adopción de su propio código de conducta para los contenidos que se publican en Internet.

4.7.1. Argumentos a favor de la regulación tecnico-juridica en Internet.

Los partidarios de la regulación manifiestan que las redes de telecomunicaciones como Internet, han generado la proliferación o incremento de los delitos informáticos, los cuales son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las diferentes modalidades en que se presenta, tales como:

1. Acceso no autorizado.
2. Destrucción de datos.
3. Infracción de los derechos de autor.
4. Infracción del Copyright de bases de datos.
5. Interceptación de e-mail.
6. Estafas electrónicas.
7. Transferencias de fondos.
8. Espionaje.
9. Espionaje industrial.
10. Terrorismo.
11. Narcotráfico.
12. Tráfico de armas.
13. Proselitismo de sectas.
14. Propaganda de grupos extremistas.

4.7.2. Argumentos en contra de la regulación tecnico-juridica en Internet.

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo Estatal. Entre los argumentos más utilizados figuran los siguientes:

1. El derecho a la intimidad.
2. La libertad de expresión.
3. La libertad de acceso a la información.

4.7.3. Autorregulación: códigos de conducta, sistemas de seguridad informática y los ciberpolicías.

A). CÓDIGOS DE CONDUCTA. A falta de una legislación específica (Internacional), en Internet existen unos códigos de ética cuyo incumplimiento está castigado con la censura popular, lo cual acaba siendo, en algunos casos, más eficaz que una norma de derecho positivo. Sí sabemos, qué podemos ser juzgados por nuestros compañeros de la red y somos conscientes de que nuestro comportamiento podría ser calificado de novato, informal o persona no agradable, entonces tendremos que acatar ciertas normas éticas que nos impone la sociedad cibernética. Ello hace que la tónica normal en Internet sea de respeto entre los usuarios de la red, siendo los demás casos la excepción.

B). SISTEMAS DE SEGURIDAD INFORMÁTICA. Los propios sistemas de control implementados en la red, garantizan la seguridad aceptable, aunque no impiden que los archivos que circulan por la red puedan contener algún virus. Y en muchos casos pueden ser neutralizados por un programa generador de passwords.

C). CIBERPOLICIAS. Algunos organismos y corporaciones como son la NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team tienen equipos de especialistas dedicados a la localización de hackers, y protegen contra sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

CAPÍTULO V
LEGISLACIÓN EN MATERIA DE DELITOS INFORMÁTICOS.

SUMARIO: 5.1. LEGISLACIÓN NACIONAL. 5.1.1. MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA. A). Primer evento. Ciudad de Veracruz, Ver., 18 de Septiembre de 1996. B). Segundo evento. Ciudad de Guadalajara, Jal., 20 de Septiembre de 1996. C). Tercer evento. Ciudad de Monterrey, N.L., 25 de Septiembre de 1996. D). Cuarto evento. Ciudad de Tijuana, B.C., 27 de Septiembre de 1996. E). Quinto evento. Ciudad de México, D.F., 4 de Octubre de 1996. 5.1.2. CODIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA. 5.2. LEGISLACIÓN INTERNACIONAL. 5.2.1. ORGANISMOS INTERNACIONALES. A). La Organización de Cooperación y Desarrollo Económico (OCDE). B). La Organización de las Naciones Unidas (ONU). C). La Asociación Internacional de Derecho Penal. 5.2.2. LEGISLACIÓN EN OTROS PAISES. A). Alemania. B). Australia. C). Francia. D). Estados Unidos. 5.2.3. TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE (TLC). 5.2.4. ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCIAS FALSIFICADAS. 5.2.5. EXTRACTO DE LA LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE DEL CÓDIGO PENAL DE ESPAÑA.

5.1. LEGISLACION NACIONAL.

La Legislación Nacional en México no estatuye los llamados "Delitos Informáticos", a excepción del código penal del Estado de Sinaloa, que más adelante analizaremos. Y ante tal situación todas las conductas ilícitas relativas al manejo de la computadora y a la informática, que se realicen en el país o en alguna entidad federativa quedarán impunes a falta de tipo penal a Nivel Federal en nuestra legislación. Cabe aclarar, que tal problemática debe atacarse a Nivel Federal, por la Importancia y Trascendencia de los delitos Informáticos, sus consecuencias económicas, tanto en los sectores públicos y privados, sus efectos internacionales, etc.

Sin perjuicio de lo anterior, algunos países como son Estados Unidos, Alemania, Francia, Austria y España consideran que tal problema debe atacarse a Nivel Internacional, por el flujo de información electrónica en todos los países, y los efectos jurídicos, políticos y económicos que pueden causarse. Sin embargo, tales países manejan gran cantidad de información y la mayoría de su población tienen computadoras propias. Por ello, debe comenzarse a legislar en México a nivel federal, y posteriormente firmar tratados internacionales con los demás países para combatir "El Crimen Informático".

Por otra parte, teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos (Art. 217), contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones

correspondientes, consideramos que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste deberá legislar en materia penal federal, tales ilícitos, dada la naturaleza y consecuencias de los mismos y otros elementos indispensables para su ejecución como son las vías generales de comunicación; quedando así la jurisdicción federal como única competente para conocerlos en juicio.

5.1.1. MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA.

El Instituto Nacional de Estadística, Geografía e Informática, en coordinación con la H. Cámara de Diputados llevó a cabo, del 18 de septiembre al 4 de octubre de 1996, el Foro de Consulta sobre Derecho e Informática, cuyo objetivo fue convocar a especialistas, académicos e investigadores, legisladores, instituciones públicas y privadas, servidores públicos y personas interesadas en el tema, a participar con sus opiniones, propuestas y experiencias, en torno al marco jurídico-administrativo relativo al uso y desarrollo de la informática.(Ver Anexo núm. I)

En este foro, se llevaron a cabo cinco reuniones en diferentes entidades del país, el primer evento se realizó en Boca del río, Veracruz, el día 18 de septiembre de 1996; el segundo en la Ciudad de Guadalajara, Jalisco, el 20 de septiembre; el tercero en la Ciudad de Monterrey, Nuevo León, el 25 de septiembre; el cuarto en la Ciudad de Tijuana, Baja California, el 27 de septiembre; y el quinto evento en la Ciudad de México, D.F., el día 4 de octubre, todos en el mismo año.

A). En la primer reunión de Boca del Río, Veracruz, se presentaron tres trabajos, en los cuales se abordaron diversos aspectos relacionados con los derechos de los ciudadanos, a la confidencialidad de información personal almacenada en bases de datos públicas y privadas, así como la protección jurídica de datos producidos por el sector público y privado. Se contó con la participación de aproximadamente 100 representantes de los sectores público, privado, académico, empresarial y de investigación.(Ver Anexo núm. II)

Los comentarios de este evento giraron en torno a los siguientes aspectos:

1. La propiedad de la información y derechos, tanto del sujeto como del poseedor de los datos. 2. La responsabilidad por daños causados por mal uso de la información, ya sea porque ésta es incorrecta o tergiversada, o por su carácter como información confidencial relativa a propiedad industrial y a información de los particulares. 3. El derecho a preservar la confidencialidad de la información, tanto de la que por ley es

proporcionada al gobierno como de la que reciban los particulares. 4. El acceso a la información propia almacenada en bases de datos y derecho a su revisión.

B). En la Ciudad de Guadalajara, Jalisco, se llevó a cabo el segundo evento, se presentaron cinco participaciones relacionadas con la tipificación de delitos cometidos con el uso de herramientas informáticas que lesionan patrimonios y derechos de personas físicas y morales, así como del valor probatorio del documento electrónico en procesos administrativos y judiciales. Asistieron en esta ocasión 120 representantes de los diferentes sectores.(Ver Anexo núm. III)

En este evento los comentarios estuvieron relacionados con los siguientes aspectos:

1. Actividades informáticas que se pueden considerar como conductas delictivas y su definición. 2. Responsabilidad del uso de los datos confidenciales y personales tanto del prestador de servicio como del usuario. 3. Elementos que deben considerarse para determinar la responsabilidad de las personas autorizadas para administrar bases de datos. 4. Necesidad de definir el ámbito de aplicación del derecho informático. 5. Posibilidad de reconocimiento del documento electrónico como medio de prueba. 6. Requisitos que debe tener un sistema para que su bitácora sea reconocida legalmente.

Asimismo, se presentó una propuesta de iniciativa de ley en la que se contemplan aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente.

C). El tercer evento se realizó en Monterrey, Nuevo León, los temas que se analizaron en esta ocasión fueron sobre la protección de los derechos de autor para desarrolladores de programas, así como la información contenida en medios magnéticos distribuida a través de redes de datos públicas. Asimismo, se discutió la protección de derechos de propiedad industrial.(Ver Anexo núm. IV)

Asistieron al evento 130 representantes de los sectores público, privado, académico, empresarial y de investigación.

El grupo de especialistas invitados, así como el auditorio emitieron diversos comentarios, entre los que destacan:

1. La importancia del procedimiento de registro de programas de cómputo. 2. Titularidad de derechos de los desarrolladores que se realizan en empresas o instituciones por los trabajadores que en ellos intervienen. 3. Responsabilidad de los empleados que hacen uso de programas de cómputo ilegal en la empresa o institución en la que laboran. 4. Definición de términos jurídicos y técnicos para la solución de conflictos derivados del

uso ilegal de programas de cómputo. 5. La posible clasificación y reubicación, en su caso, de los programas de cómputo para su protección en el contexto de la Ley de Propiedad Industrial. 6. Definición de contratos de bienes y servicios informáticos.

D). La cuarta reunión se llevó a cabo en Tijuana, Baja California, durante el evento de este Foro de Consulta sobre Derecho e Informática, las participaciones que se presentaron giraron en torno a los mecanismos de fomento, al desarrollo y uso de la informática, así como a las condiciones adecuadas de competencia y servicio entre los proveedores de bienes y servicios informáticos.(Ver Anexo núm. V)

Se contó con la participación de aproximadamente 110 representantes de diferentes sectores y los comentarios que fueron emitidos en esta ocasión, giraron en torno a:

1. La competitividad de empresas en el mercado informático. 2. Apoyos para el desarrollo de proyectos informáticos y mecanismos de evaluación. 3. Mecanismos para promover y fomentar el desarrollo de empresas de bienes y servicios informáticos. 4. Instancias de evaluación y certificación de calidad de empresas de bienes y servicios informáticos. 5. Situación de las empresas desarrolladoras de programas de cómputo en el mercado de la Ley Federal de Competencia Económica. 6. Programa de estudios de la licenciatura en derecho que incluya conceptos informáticos.

E). El último evento se realizó en el Distrito Federal, en esta reunión se presentaron once participaciones en torno a las condiciones para la prestación de servicios telemáticos, públicos y privados, así como a las condiciones de acceso universal a la información y a la infraestructura tecnológica. Participaron 160 representantes de diferentes sectores.(Ver Anexo núm. VI)

Se emitieron diversos comentarios, los cuales giraron en torno a los siguientes temas:

1. Acceso a la información. 2. Utilidad y aplicación de la informática. 3. Regulación jurídica que proteja y ponga orden para proporcionar el desarrollo informático. 4. Derechos y responsabilidades de desarrolladores de software.

El Foro De Consulta Sobre Derecho E Informática tuvo como resultado de estos cinco eventos, propuestas para líneas de acción inmediata que permitirán revisar el marco jurídico-administrativo, destacando las siguientes:

- **Realizar un estudio de derecho comparado y promover que exista congruencia en la legislación nacional con tratados internacionales de los que México forme parte.**

- **Promover la emisión de disposiciones que agilicen los procesos jurídicos y precisar el proceso para deslindar responsabilidades en caso de que se violen los derechos autorales protegidos por la ley.**
- **Protección de los derechos de propiedad intelectual e industrial para estimular la actividad creadora e instrumentar mecanismos técnicos y legales que proporcionen una protección más efectiva para minimizar el uso ilegal de software.**
- **Definir los términos jurídicos que deben considerarse para su aplicación en litigios derivados de la violación de los derechos autorales o de algún ilícito cometido con el uso de esta tecnología.**
- **Establecer el modelos de "Derecho Informático" que contemple simultáneamente componentes jurídicos, educacionales y administrativos.**
- **Presentar propuestas de iniciativa de ley que contemplen aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente y disposiciones complementarias.**
- **Tipificación del delito informático o electrónico como modalidad de los ya existentes a partir de la identificación y definición de sus características.**
- **Educar a las personas respecto a las consecuencias del mal uso de la tecnología de la información y promover la cultura de las universidades para apoyar la aplicación de las leyes.**
- **Que el gobierno fomente el mercado informático mediante la presentación de sus necesidades a la industria, licitando soluciones que posteriormente podrían ser utilizadas en el sector privado con sus correspondientes utilidades y creación de nuevas fuentes de trabajo.**
- **Ampliar conceptos en la ley que regula los procesos de adquisiciones para que sustenten la compra de soluciones más que de bienes informáticos.**
- **Promover la certificación de la calidad de empresas proveedoras de bienes y servicios informáticos y definir instancias que la validen.**

5.1.2. EL CODIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA.

Sinaloa, es la única Entidad Federativa de México que estatuye especifica y concretamente a los delitos informáticos, y ante la importancia que tiene qué el Congreso Local de tal Estado haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo
"Delitos contra el patrimonio"

Capítulo V
Delito Informático.

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

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

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.[66]

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

Consideramos que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.[67]

Por ello, sin menospreciar el valor del avance legislativo de tal Entidad en este delito, cabe señalar que este Nuevo Tipo Penal debe consignarse a Nivel Nacional dentro de los delitos patrimoniales del Código Penal Federal.

[66] Véase El Código Penal para el Estado de Sinaloa, Art. 217. Editorial Porrúa.
[67] http://tiny.uasnet.mx/prof/cin/der/silvia/cppps.htm

5.2. LEGISLACION INTERNACIONAL.

A continuación analizaremos algunos de los Organismos Gubernamentales Internacionales tales como La Organización de Cooperación y Desarrollo Económico (OCDE), La Organización de las Naciones Unidas (ONU) y La Asociación Internacional de Derecho Penal al igual que algunos países, han presentado propuestas para enfrentar la problemática de los delitos informáticos, ya que en los últimos años se han ido trazando valoraciones jurídico-políticas respecto al tema en el ámbito internacional, derivadas del mal uso que se hace de las computadoras y ello nos conlleva a que se modifiquen o actualicen las leyes penales de cada país.

5.2.1. LOS ORGANISMOS INTERNACIONALES

A). LA ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE).

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

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. De ello surgió un análisis y valoración de derecho comparado entre varios países, así como propuestas de reforma. Las conclusiones jurídico-políticas se redujeron en una listas de acciones delictivas que podrían ser consideradas por los Estados, como regla general, de merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se establecían las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.[68]

Además de la lista de acciones delictivas mencionada, se recomendó también como protección penal contra otros usos indebidos una Lista Optativa o Facultativa, la

[68] http://tiny.uasnet.mx/prof/cln/der/silvia/lexis.htm

cual contemplaba las siguientes acciones: espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Posteriormente el Consejo Europeo, realizó un estudio respecto de los delitos informáticos a fin de elaborar directrices que ayudaran a los sectores legislativos a determinar qué tipo de conductas debían prohibirse en la legislación penal ampliándose considerablemente, la lista mínima elaborada por la OCDE, añadiéndose a ella otros tipos de abuso que se estimaba merecían sancionarse penalmente.

El Comité Especial de Expertos sobre Delitos relacionados con el uso de las computadoras, del Comité Europeo, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .... y en particular las directrices para los legisladores nacionales".

Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989. Las directrices o lineamientos jurídico-penales para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

B). LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)

Por otra parte, la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se estableció que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difumdido la comisión de actos delictivos.[69]

[69] http://tiny.uasnet.mx/prof/cln/der/silvia/texis.htm

En un principio, el problema principal era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, todavía no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento, ya que eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Actualmente, la comunidad internacional no ha conciliado conceptos o parámetros fijos para determinar a los delitos informáticos en el derecho penal, tales como: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados. internacionales de extradición.

C). LA ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL

En otro orden de ideas, La Asociación Internacional de Derecho Penal en la celebración de un coloquio en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, las cuales contemplaban que cuando el derecho penal tradicional no sea suficiente para prevenir o controlar tal delito, debería promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad).[70]

También advirtió a los Estados que de acuerdo a sus tradiciones jurídicas, su cultura y la aplicabilidad de su legislación vigente, se tomará en cuenta la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático.

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

5.2.2. LEGISLACION EN PAISES EXTRANJEROS.

En los últimos quince años, los países europeos se han preocupado más por la

[70] Idem.

penalización de los delitos informáticos, ya que por ser países que manejan gran cantidad de información, ya sea a través de bases de datos o en distintos soportes de almacenamiento, estos son mas susceptibles de manipulación, robo, modificación o destrucción. Actualmente, pocos son los países que cuenta con una legislación adecuada para enfrentar el problema de los delitos informáticos, a continuación se señalan los países mas avanzados respecto a legislación nacional encauzada a regular y controlar tales delitos y la descripción de los tipos penales mas cometidos en esos países.

A). ALEMANIA.

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: [71]

- **Espionaje de datos** (Art. 202)
- **Estafa informática** (Art. 263)
- **Falsificación de datos probatorios** (Art. 269) , junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (Arts. 270, 271, 273.)
- **Alteración de datos** (Art. 303), es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- **Sabotaje informático** (Art. 303), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- **Utilización abusiva de cheques o tarjetas de crédito** (Art. 266)

Los legisladores alemanes han introducido seis nuevos y diferentes tipos penales, que tratan de abarcar la totalidad de conductas ilícitas relativas al manejo de información a través de un ordenador. Además, al introducir nuevos preceptos penales para combatir a la criminalidad informática, tomaron en cuenta las dificultades de aplicación de las leyes vigentes y qué bien jurídico sufriría afectación o menoscabo.

Por otro lado, las diversas manifestaciones de la criminalidad informática propician la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, ya que tales delitos avanzan a la par con la tecnología.

[71] http://tiny.uasnet.mx/prof/cln/der/silvia/leyint.htm

B). AUSTRIA. LEY DE REFORMA DEL CÓDIGO PENAL DE 22 DE DICIEMBRE DE 1987.

Esta ley contempla los siguientes delitos:

Destrucción de datos (Art. 126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
Estafa informática (Art. 148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.[72]

Además contempla sanciones para quienes cometen estas acciones utilizando su profesión. (situaciones agravantes).

C). FRANCIA. LEY NÚMERO 88-19 DE 5 DE ENERO DE 1988 SOBRE EL FRAUDE INFORMÁTICO.

- **Acceso fraudulento a un sistema de elaboración de datos** (Art. 462).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- **Sabotaje informático** (Art. 462).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- **Destrucción de datos** (Art. 462).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- **Falsificación de documentos informatizados** (Art. 462).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- **Uso de documentos informatizados falsos** (Art. 462) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos (Art. 462)

[72] http://tiny.uasnet.mx/prof/cln/der/silvia/leyint.htm

D). ESTADOS UNIDOS

En 1994, Estados Unidos adoptó La Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó la Acta de Fraude y Abuso Computacional de 1986. La nueva acta prohibe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas. (18 U.S.C.: Sec. 1030 (a) (5) (A).

También diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos (dos supuestos o hipótesis diferentes). El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión. Además se aclara, qué el creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

Los legisladores estadounidenses, opinan que la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistema informáticos en cualquier forma en que se realicen. Y así da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos. Consideramos importante destacar la enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $ 10,000 por cada persona afectada y hasta $.50,000 el acceso imprudencial a una base de datos.[73]

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

[73] Idem.

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

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus informáticos conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones o funciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

El delito de "violencia tecnológica" en la legislación de Nueva York. El 6 de junio de 1993 el Estado de Nueva York modificó su ley penal sobre "fraude informático", la que entró en vigencia el 1 de noviembre de 1993. El objetivo fue reestructurar la ley para que sus sanciones guardaran proporción con los cuantiosos daños que soportan las víctimas de estos delitos.

El concepto de "Violencia Tecnológica" (o alteración fraudulenta de una computadora) da nuevos significados a los actos ilícitos cometidos por el uso de las computadoras y la diseminación de virus. Así, la nueva ley penal, clasifica los delitos por clases A, B, C, D y E, dependiendo de la cuantía del daño, será la multa y/o prisión. Por ejemplo, en los delitos mayores cuando los daños excedan de $ 3.000 (delito mayor de clase D) o de $ 50.000 (delito mayor de clase C). Esto puede llevar a multas de entre $ 5.000 y 10.000 y hasta siete años de prisión por delito.

La Nueva Ley define "La alteración fraudulenta de una computadora" cuando alguien ilegítima e intencionalmente usa, modifica de cualquier modo o destruye los datos almacenados en una computadora o un programa de otra persona.

El ordenamiento en comento, ya tuvo aplicación cuando en un intento de detener a un productor de software. La compañía "MJL Desingn", de Nueva York, envió a uno de sus técnicos a desarmar un programa mientras se hallaba pendiente de resolución una disputa sobre pagos con su cliente. El Director de MJL, Michael Lafaro, fue acusado de haber instruido a uno de sus empleados para que instalara un virus en una aplicación de seguimiento de cuentas desarrollada para una compañía de muebles, Forecast Installations, que no se hallaba satisfecha con el software y se negaba a pagar el saldo de $ 2.400 debidos por el contrato de desarrollo de software y el acuerdo de servicios.

Así como el ejemplo indicado, algunas empresas o compañías de programas de computo hacen uso de la "Violencia Tecnológica", como una herramienta para cobranza de deudas, ésta no estaba contemplada en los objetivos de la nueva ley, sin embargo, gracias al alcance del concepto de "alteración fraudulenta de una computadora", que estatuye la nueva ley, es posible combatir tal tendencia de ciertas compañías.

5.2.3. TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE (TLC)

Este instrumento internacional firmado por el Gobierno de México, él de los Estados Unidos y él de 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. De esta forma, los tres Estados establecieron en el T.L.C. la defensa de los derechos de propiedad intelectual a fin de que su derecho interno contenga procedimientos de defensa que permitan la adopción de medidas eficaces contra cualquier acto que infrinja a los mismos.[74]

Propiedad intelectual

El TLC establece obligaciones sustanciales relativas a la propiedad intelectual, las cuales se fundamentan en el trabajo realizado por el GATT y los convenios internacionales más importantes sobre la materia. Cada país protegerá adecuada y efectivamente los derechos de propiedad intelectual con base en el principio de trato nacional, y asegurará el cumplimiento efectivo de estos derechos, tanto a nivel nacional como en las fronteras.

El Tratado define compromisos específicos sobre la protección de:

- Derechos de autor, incluyendo los fonogramas; (Art. 1705 y1706).
- Patentes; (Art. 1709).
- Marcas; (Art. 1708).
- Derechos de los obtentores de vegetales;
- Diseños industriales; (Art. 1713)
- Secretos industriales; (Art. 1711)
- Circuitos integrados (semiconductores); e (Art. 1710)
- Indicaciones geográficas. (Art. 1712)

Derechos de autor

En el área de derechos de autor, las obligaciones de los países signatarios del Tratado son:[75]

- Proteger los programas de cómputo como obras literarias, y las bases de dato como

[74] http://tiny.uasnet.mx/prof/cln/der/silvia/TLC.htm
[75] TLC de América del Norte. Texto oficial. Secofi. pags. 483-487.

compilaciones;

- Conceder derechos de renta para los programas de cómputo y fonogramas; y
- Estipular un plazo de protección de por lo menos 50 años para los fonogramas.

Patentes

El Tratado otorga protección a las invenciones, requiriendo a cada país:[76]

- Conceder patentes para productos y procesos en prácticamente todo tipo de inventos, incluidos los farmacéuticos y agroquímicos;
- Eliminar cualquier régimen especial para categorías particulares de productos, cualquier disposición para la adquisición de los derechos de patentes, y cualquier discriminación en la disponibilidad y goce de los derechos de patentes que se otorguen localmente y en el extranjero; y
- Brindar la oportunidad a los titulares de las patentes, para que obtengan protección en los inventos relativos a productos farmacéuticos y agroquímicos, que antes no estaban sujetos a ser patentados.

Otros derechos de propiedad intelectual

Además, esta sección establece reglas para proteger a:[77]

- Las marcas de servicios al mismo nivel que las de productos;
- Las señales codificadas emitidas por satélites, en contra de su uso ilegal;
- Los secretos industriales en general, así como la protección contra la divulgación por parte de las autoridades competentes de resultados presentados por las empresas relativos a la seguridad y eficacia de sus productos farmacéuticos o agroquímicos;
- Los circuitos integrados tanto en sí mismos, como a los bienes que los incorporen; y
- Las indicaciones geográficas, para proteger a los titulares de las marcas y evitar inducir al público a error.

Procedimientos de ejecución

También se incluyen obligaciones detalladas sobre:

Los procedimientos judiciales para la puesta en práctica de los derechos de propiedad intelectual incluidas las disposiciones relativas a daños, suspensión precautoria

[76] Ibidem. Págs. 491-495.
[77] Ibidem. Págs. 488-501.

y, en general, a los aspectos de legalidad en los procedimientos; y el cumplimiento de los derechos de propiedad intelectual en la frontera, incluidas las salvaguardas para prevenir el abuso.

Telecomunicaciones

El TLC dispone que las redes públicas de telecomunicaciones ("Internet") y los servicios de telecomunicaciones estarán disponibles, en términos y condiciones razonables y no discriminatorios, para empresas e individuos que las utilicen en la realización de sus actividades. El uso de las redes públicas incluye la prestación de servicios mejorados o de valor agregado, y las comunicaciones internas de las corporaciones. La operación y establecimiento de las redes y servicios públicos de telecomunicaciones no forman parte de este Tratado.[78]

Acceso y uso de las redes públicas

Los países garantizarán que prevalezcan condiciones razonables para el acceso y uso de las redes públicas, incluida la capacidad de: [79]

- Arrendar líneas privadas;
- Conectar equipo terminal u otro equipo a las redes públicas;
- Interconectar circuitos privados a las redes públicas;
- Realizar funciones de conmutación, señalización y procesamiento; y
- Emplear protocolos de operación, a elección del usuario.

Además, sólo se impondrán condiciones al acceso y uso, si son necesarias para salvaguardar la responsabilidad del servicio público de los operadores de la red, o para proteger la integridad técnica de las redes públicas.

Las tarifas de los servicios públicos de telecomunicaciones de los países miembros del TLC deberán reflejar los costos económicos, y los circuitos privados arrendados deberán estar disponibles sobre la base de una tarifa fija. Sin embargo, el Tratado no prohibe el otorgamiento de subsidios cruzados entre los servicios públicos de telecomunicaciones. Las empresas o las personas podrán utilizar las redes y servicios públicos para transmitir información dentro de cada país y dentro del territorio de América del Norte.

---

[78] TLC de América del Norte. Texto oficial. Secofi. pags.431-440.
[79] Ibidem. Págs. 432-434.

Las disposiciones descritas en esta sección no se aplican a las medidas que afectan la distribución de programas de radio o televisión a través de estaciones radiodifusoras o sistemas de cable, las cuales tendrán acceso a, y uso permanentes de las redes y servicios públicos.

Excepciones y limitaciones

Los tres países no estarán obligados a conceder autorización para prestar u operar redes y servicios de telecomunicaciones a una persona de otro país miembro del TLC, y se reservan la facultad de prohibir a los operadores de redes privadas la prestación de redes y servicios públicos de telecomunicaciones.

Telecomunicaciones mejoradas

El Tratado dispone que los procedimientos de cada país para otorgar licencias u otras autorizaciones para la prestación de servicios mejorados o de valor agregado sean transparentes, no discriminatorios y expeditos. Los proveedores de servicios de telecomunicación mejorados de los tres países no estarán sujetos a las obligaciones que generalmente se les imponen a los proveedores de redes y servicios públicos de telecomunicaciones tales como prestar servicios al público en general o justificar sus tarifas con base en los costos.[80]

Medidas de normalización

El Tratado limita las normas que se pueden imponer a la conexión del equipo de telecomunicaciones a las redes públicas. Estas medidas se concretarán a las necesarias para impedir daño técnico o interferencia con las redes y servicios públicos, fallas en el equipo de facturación, y a aquellas pertinentes para garantizar a los usuarios seguridad y acceso. Además, se permitirá a cualquier entidad técnicamente calificada probar el equipo que será conectado a las redes públicas. Este apartado también establece procedimientos en cada país para la aceptación de los resultados de las pruebas realizadas en los otros países del TLC.[81]

Prestación monopólica de servicios

El Tratado reconoce que un país signatario puede mantener o designar a un prestador monopólico de redes o servicios públicos. Cada país garantizará que cualquier monopolio no abuse de su posición en actividades fuera de su campo de acción

[80] Ibidem. Págs. 434-435.
[81] Ibidem. Págs. 435-436.

incurriendo en conductas contrarias a la competencia que afecten adversamente a una persona de algún otro país del TLC. (Art. 1305)

Disponibilidad de información

La información que afecta el acceso y uso de las redes y servicios públicos de telecomunicaciones estará disponible al público en general, incluyendo:

- Tarifas y otros términos y condiciones para la prestación del servicio;
- Especificaciones sobre las interfaces técnicas de redes y servicios;
- Información sobre las entidades reguladoras en materia de normas;
- Condiciones para la conexión de equipo terminal; y
- Requisitos de notificación, permisos, registro o licencias.

Cooperación técnica

Los países cooperarán para el intercambio de información técnica y el desarrollo de programas de capacitación de gobierno a gobierno. Los países reconocen la importancia de las normas internacionales para las telecomunicaciones globales y acuerdan promoverlas mediante los trabajos de la Unión Internacional de Telecomunicaciones, la Organización Internacional de Normalización y otros organismos internacionales pertinentes. (Art. 1309).

5.2.4. ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCIAS FALSIFICADAS.

Al iniciar el contenido de este apartado, debemos aclarar que si bien la institución del GATT se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.[82]

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

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este

[82] http://tiny.uasnet.mx/prof/cln/der/silvia/OAINT.htm

tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

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

Asimismo, en la sección 5, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

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

5.2.5. EXTRACTO DE LA "LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL DE ESPAÑA".

La Ley Orgánica 10/95, de 23 de noviembre, del Código Penal ha sido promulgada para substituir el anterior Código Penal, toda vez que éste ya no cubría las necesidades actuales de la sociedad respecto a la problemática de los delitos cometidos por el uso de la computadora, los denominados "Delitos Informáticos" o en algunos países llamados "Crímenes de la computadora".

La aparición en la sociedad actual de nuevos delitos no recogidos en el anterior texto penal implicaba el riesgo de caer en la atipicidad, por ello fue necesaria una regulación específica que permita enjuiciar las nuevas formas de delincuencia en un marco legal adecuado.

La Exposición de Motivos del Nuevo Código Penal Español literalmente dice: "El Código Penal ha de tutelar los valores y principios básicos de la convivencia social. Cuando esos valores y principios cambian, debe también cambiar la ley...".

El nuevo texto del Código Penal, pone al día la tipicidad delictiva suprimiendo aquellos preceptos que el paso del tiempo ha convertido en arcaicos u obsoletos y añadiendo los que resultan necesarios para hacer frente a determinados comportamientos delictivos, fruto de la sociedad actual y que hasta el momento no se encontraban tipificados, atendiendo a las necesidades colectivas, como se ha indicado anteriormente.

A continuación se transcriben íntegramente los artículos que se relacionan intrínsecamente con los delitos informáticos:

> **Art. 169.** El que amenazare a otro con causarle a él, su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, *el patrimonio y el orden socio económico*, será castigado:
>
> 1.° Con la pena de prisión de uno a cinco años, si se hubiese hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años. Las penas señaladas se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o *por cualquier medio de comunicación o de reproducción*, o en nombre de entidades o grupos reales o supuestos.
> 2.° Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.
>
> **Art. 197.** 1. El que, para descubrir los secretos o vulnerar la intimidad de otros, sin su consentimiento, se apodere de sus papeles, cartas, *mensajes de correo electrónico o cualquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificio técnico de escucha, transmisión o grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicaciones*, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2.° La mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o *soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. [...]
>
> **Art. 256.** El que hiciere uso de cualquier *equipo terminal de telecomunicaciones*, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

> Art. 263. El que causare *daños en propiedad ajena no comprendidos en otros Títulos de este Código*, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.
>
> Art. 264. 1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que *causare daños expresados en el artículo anterior*, si concurre alguno de los supuestos siguientes: [...] 4.° Que afecte a bienes de dominio o uso publico o comunal. [...] 2. La misma pena se impondrá al que por cualquier medio *destruya, altere, inutilice o de cualquier otro modo dañe datos, programas o documentos electrónicos ajenos contenidos en redes, soporte o sistemas informáticos.*
>
> Art. 270. Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, *reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio*, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
>
> La misma pena se impondrá a quien intencionadamente *importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones* sin la referida autorización.
>
> Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio especificamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.[83]

Por otro lado, pero en *un* mismo orden de ideas, en los últimos meses se ha difundido un gran número de noticias relativas a los delitos cometidos a través de Internet, culpando indebidamente a dicho medio de comunicación.

> **INTERNET es un vehículo de comunicación multimedia, mundial, veloz, asequible a casi todas las economías, difícil de controlar por gobiernos y particulares. Supone una auténtica y no acabada revolución en las comunicaciones -como antaño lo constituyó, la prensa, la fotografía, el teléfono, la radio, la televisión, el fax- ya que contiene todos estos medios, albergando textos, sonidos, imágenes con o sin movimiento, difundiéndolas instantáneamente.[84]**

[83] http://ccdis.dis.ulpgc.es/ccdis/legisla/codigopc
[84] http://www.mundolatino.org/i/derecho/delitos.htm

De la misma forma que pueden cometerse delitos por cualquiera de los medios indicados, pueden cometerse por Internet, debiéndose aceptar la diferencia de que la red añade una mayor facilidad y difusión, y especialmente una internacionalización del delito que ha sorprendido a todo tipo de juristas.

El mayor problema que plantea Internet a los legisladores es ¿qué ley debe aplicarse? o ¿qué tribunal debe juzgar?. Actualmente, casi todos los países se rigen por los delitos cometidos en su país o que perjudican a sus ciudadanos. Algunos como España, castiga delitos cometidos en otros países cuando se refieren a materia de terrorismo, genocidio, falsificación de moneda, etc.

Por ejemplo, si en una página Web que reside en un servidor Coreano, se insulta a un gobernante, o a unos empresarios Mexicanos, tales delitos no pueden perseguirse en nuestro país, pues los usuarios de Internet libremente acuden electrónicamente a Corea. Tales situaciones obligarán a los Estados a modificar sus legislaciones y a "Establecer Tratados Internacionales", que permitan que los delitos cometidos en cualquier parte del mundo, puedan ser juzgados en el país donde *resida el ofendido*, y *posibilitar los tratados* de extradición.

La mayoría de los usuarios y no usuarios de la red, creen o tiene la idea de qué en Internet todo es lícito y que todo es incontrolable. Nada más incierto, y en las siguientes líneas analizaremos algunos delitos que se pueden cometer por Internet (los más usuales o *frecuentes*) y *sus formas* de control, sin menoscabo de los artículos transcritos anteriormente, ya que aquellos pueden cometerse con cualquier medio de comunicación (Vía satélite, transmisiones de radio o televisión, o cualquier equipo de telecomunicaciones).

El artículo 10 de la Ley de Propiedad Intelectual establece qué obras son objeto de protección de dicha ley, artículo que se inserta íntegramente por su importancia:

> Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:
>
> a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza. b) Las composiciones musicales, con o sin letra. c) Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales. d) Las obras cinematográficas y cualesquiera otras obras audiovisuales. e) Las esculturas y las obras de pintura, dibujo, grabado, litografía, y las historietas gráficas, tebeos o cómics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas. f) Los

> proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería. g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia. h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía. i) Los programas de ordenador. 2. El título de una obra, cuando sea original, quedará protegido como parte de ella.
>
> También son objeto de propiedad intelectual: 1.° Las traducciones y adaptaciones. 2.° Las revisiones, actualizaciones y anotaciones. 3.° Los compendios, resúmenes y extractos. 4.° Los arreglos musicales. 5.° Cualesquiera transformaciones de una obra *literaria, artística o científica*. [85]

La anterior protección legal supone que para utilizar una obra de las mencionadas, en el caso que *nos ocupa*, ***los programas de ordenador***, será preciso obtener la autorización del autor o de sus herederos. Hay no obstante, obras de dominio público, que son aquellas cuyos autores hayan fallecido hace más de 60 años.

El artículo 270 del Código Penal Español, castiga con penas de prisión de 6 meses a 2 años más una multa, por ejemplo la reproducción, el plagio, la importación, exportación, total o parcial, o el simple almacenamiento de las obras protegidas. Además pueden derivarse responsabilidades civiles, es decir indemnizaciones a favor del autor o de sus causahabientes, siempre y cuando dichas actividades se realicen con ánimo de lucro, en perjuicio de tercero, y lógicamente sin la debida autorización.

Además de ello, también castiga la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

El artículo 274 del Código Penal Español, establece la utilización de marcas y dibujos industriales, su imitación o modificación, sin permiso de su titular y conociendo que están registrados, está sancionada con prisión de 6 meses a 2 años más multa.

El artículo 197 del Código Penal Español sanciona de 1 a 4 años de prisión más multa, la vulneración de la "intimidad de otro", apoderándose de cualquier tipo de documento, o interceptando cualquier señal de comunicación. Igualmente, está castigado el *apoderamiento* de datos reservados de carácter personal o familiar que se hallen en cualquier tipo de soportes informáticos, la ley castiga tanto el apoderamiento, como el simple acceso. Si los referidos datos protegidos se difunden, la pena se agrava con prisión de 2 a 5 años. Asimismo, la persona que a sabiendas del acceso ilícito a dichos datos, los difundiera a su vez, será castigada con la pena de 1 a 3 años de prisión, más multa.

---

[85] http://www.mundolatino.org/i/derecho/delitos.htm

Podría entenderse como "Apoderamiento", cuando se carga en el ordenador la información que se está visualizando, aunque sea de forma temporal, lo que es frecuente en Internet. No obstante, la mera visualización no puede considerarse apoderamiento. Cabe añadir que el art. 270 del Código Penal castiga la tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.[86]

El artículo 278 protege el secreto de las empresas, y sanciona de 2 a 4 años de prisión, el apoderarse por cualquier medio de documentos electrónicos y soportes informáticos, entre otros documentos. Si los secretos descubiertos se difundieren la pena de prisión puede ser de 3 a 5 años de prisión.

Asimismo, el artículo 282 castiga la publicidad engañosa, que se realiza cuando los comerciantes o productores en sus ofertas o publicidad incluyen alegaciones falsas, o manifiestan características inciertas, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores. En tal caso las penas pueden ser de 6 meses a un año más multa.[87]

El artículo 264 castiga la destrucción, alteración, inutilización o cualquier otro daño respecto a los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos.

Por tanto, el envío de un virus por la red, la modificación de un programa o simple documento al cual se ha tenido acceso por Internet, está penado de 1 a 3 años de prisión además de las multas y las responsabilidades civiles.

Cuando la mera alteración a que hemos hecho referencia, se produce con ánimo de perjudicar y sobre un documento (el Código Penal entiende documento de un modo específico: cualquier soporte material que exprese datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica) ya no estamos ante un delito de daños, sino ante una falsedad, y la pena es de 6 meses a 2 años.

La estafa está tipificada en el artículo 248 del Código Penal, estableciéndose que sus requisitos son el engaño y el afán de lucro, y se refiere expresamente a aquellas persona que manipulan elementos informáticos a fin de conseguir la transferencia de cualquier activo patrimonial en perjuicio de tercero. En el caso de Internet se refiere lógicamente a aquellas personas que consiguiendo passwords o números de tarjeta de

[86] http://www.sarenet.es/info/laley.htm
[87] http://www.onnet.es/04001002

crédito se lucran, o benefician a otros, con cualquier tipo de bienes. Las penas previstas son de 6 meses a 4 años.[83]

La calumnia que es toda imputación de un delito con conocimiento de su falsedad o desprecio hacia la verdad, y la injuria es toda acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación, según establecen los artículos 205 y 208 del Código Penal. Pueden cometerse por cualquier medio de comunicación, y por tanto por Internet. Las calumnias están penadas con 6 meses a 2 años de prisión, y las injurias sólo están penadas las que se consideran graves y la sanción es de multa.

El Código Penal no tipifica la pornografía como un delito, pero sí su distribución o exhibición a menores e incapaces, y así viene regulado en el artículo 187 del Código Penal, imponiendo una pena de multa. También es delito la utilización de un menor o incapaz con fines pornográficos, según el art. 189 del mismo código, en tal caso la pena puede ser de 1 a 3 años de prisión.

En resumen, podemos afirmar qué son **"Nueve los Delitos Informáticos"**, que se dan con más frecuencia en España, a saber:

- **Correo electrónico:** Se asimila el correo electrónico al correo penal. El art. 197 penaliza la lectura de mensajes privados de usuarios sin consentimiento de éstos con penas de 1 a 4 años de prisión.
- ***Difusión del material pornográfico:*** **Los servidores en Internet que ofrezcan material pornográfico accesible a menores de 18 años serán penados con 2 años.**
- **Pornografía infantil:** El art. 189 penaliza utilizar a menores para material pornográfico.
- **Publicidad engañosa:** El art. 282 castiga con 2 años la difusión de publicidad engañosa y que cause perjuicio a terceros.
- **Injurias y calumnias:** El art. 212 penaliza cualquier tipo de información o mensaje que contenga calumnias o injurias.
- **Seguridad y ataques a sistemas informáticos:** El art. 266 castiga con penas de hasta 3 años de presión, la destrucción intencionada de datos informáticos. Los virus y la ruptura de sistemas entran también en esta categoría.
- ***Estafas:*** **Se pena la manipulación electrónica de máquinas que generen perjuicios a terceros, incluyéndose en esta categoría delitos como la manipulación de tarjetas o de cajeros automáticos.**
- **Propiedad intelectual:** El art. 270 regula la protección de las obras de propiedad intelectual en cualquier formato.
- **Protección a la intimidad personal:** La difusión de datos personales sin autorización tendrán penas entre 1 y 4 años.

[83] http://www.mundolatino.org/i/derecho/delitos.htm

CAPITULO VI
PROCEDIMIENTO, JURISDICCIÓN Y COMPETENCIA.

SUMARIO: 6.1. EL PROCEDIMIENTO PENAL. 6.2. EL PROCESO PENAL. 6.3. LA PRUEBA. A).- Las pruebas Digitales. B).- Los sistemas de identificación. C).- sniffers. D).- Obstaculos. 6.4. LA PERITACIÓN. 6.5. EL EXHORTO. 6.6. LEY DE EXTRADICIÓN INTERNACIONAL. 6.7. LA JURISDICCION. 6.8. COMPETENCIA JURISDICCIONAL EN INTERNET. 6.9. LOS JUECES DE DISTRITO. 6.10. EL MINISTERIO PUBLICO FEDERAL.

6.1. EL PROCEDIMIENTO PENAL.

El desarrollo del presente capítulo, tiene como fin incorporar la figura jurídica de los delitos informáticos a la legislación penal mexicana, y por ello, es importante vincular tal delito con las instituciones jurídico-penales existentes en nuestro Código Federal de Procedimientos Penales, para saber si son compatibles y no se contrapongan en un momento dado.

Por ello, primero hago un recuento general del Procedimiento Penal, y después un análisis con diversas figuras jurídico-penales, de gran relevancia en nuestro procedimiento penal.

El procedimiento penal ha sido definido como la forma en que deben realizarse todos los actos establecidos por la ley para resolver acerca de la Pretensión Punitiva Estatal y cuya totalidad comprende desde que el Ministerio Público en representación de los intereses de la sociedad y de la víctima, como de los ofendidos, toma conocimiento de la posible lesión de bienes jurídicos y, en su caso, provoca la actividad jurisdiccional, hasta la extinción de la responsabilidad resultante; en la inteligencia de que si esta no llega a declararse o a cumplirse, el procedimiento abarcará hasta las causas que pongan fin anticipadamente a esta actuación.

Doctrinalmente comprende cuatro etapas: averiguación previa o actos preparatorios o paraprocesales, instrucción, juicio y ejecución de sentencias.

El Código Federal de Procedimientos Penales, en su Artículo 1ero. divide al procedimiento en siete periodos: averiguación previa, preinstrucción, instrucción, primera instancia, segunda instancia, ejecución y los relativos a inimputables, menores y los que tienen el habito de consumir estupefacientes y psicotrópicos.

La Pretensión Punitiva Estatal, es la voluntad de la sociedad (contenida en las leyes) manifestada a través del legislador, implícita en el conjunto de actos a cargo del

Ministerio Público cuya realización tiende a obtener elementos de prueba para la determinación jurídica, ante los tribunales, o también es la voluntad manifestada por el actor en su demanda, tendiente a obtener una determinada resolución del órgano jurisdiccional.

Diferencia Cuantitativa entre Procedimiento, Proceso y Juicio.

El procedimiento comprende todos los actos constitutivos de las "formalidades esenciales del procedimiento", referidos en el Artículo 14 de la Constitución Federal, incluyendo los relativos a la averiguación previa; ***el proceso*** tan solo los que se realizan ante el órgano jurisdiccional y, por tanto, se excluyen los que de la averiguación previa; ***el juicio*** comprende una parte de los actos del proceso, desde la acusación hasta la sentencia, en consecuencia, no comprende los actos relativos al termino Constitucional de las 72 horas, ni los de la instrucción.

6.2. EL PROCESO PENAL.

Doctrinalmente ha sido conceptualizado como "el conjunto de actos que se realizan desde el auto de radicación hasta la resolución definitiva (sentencia) en que se declara el Derecho en cada caso concreto y que comprende tres etapas: la relativa al termino constitucional de 72 horas, la instrucción y el juicio; cuya realización precisamente debe ajustarse al orden y a la forma predeterminados por la ley.

El objeto del Proceso Penal es el Conjunto de derechos y obligaciones de las partes (Ministerio Público y Órgano de la defensa), así como de atribuciones del órgano jurisdiccional, de cuyo ejercicio y cumplimiento, respectivamente, depende la resolución de la pretensión punitiva del Estado. Se clasifica en principal y en accesoria, según sea el interés a que se refiera.

A). PRINCIPAL. Cuando se trata de interés de la sociedad, pues con la ejecución de penas se busca: a). Restablecer el orden jurídico alterado con motivo de la comisión de delitos. b). Evitar la comisión de nuevos delitos. (Prevenciones generales y especiales). Es decir, que el objeto fundamental del proceso penal es una determinada relación de derecho penal que surge de un hecho que se considera como delito, y se desarrolla entre el Estado y el individual cual se atribuye el hecho, con el fin de que sea aplicada a este último la ley penal.

Las diversas penas que pueden ser impuestas por los tribunales, se describen genéricamente en los diversos códigos penales, así como su naturaleza y sus alcances, a cada tipo le corresponde una determinada punibilidad, cuyo mínimo debe estimarse como

la retribución debida por haber alterado el orden jurídico, el ***quantum*** de la pena determinable por esos tribunales tiene como limite el máximo y debe precisarse en cada caso concreto considerando las circunstancias de comisión tanto exteriores, como las subjetivas, es decir, el grado de temibilidad o peligrosidad del agente acreditado en autos.

Los códigos penales mexicanos imponen a los juzgadores la obligación de tener como base para determinar la peligrosidad y, en consecuencia, el ***quantum*** de la pena, las causas y circunstancias concurrentes, mas omite el móvil o fin perseguido, elemento esencial según informan los diversos estudios de la Criminología.

B). ACCESORIO.- Esencialmente se refiere al interés de los particulares jurídicamente afectados. Mediante la acción para reparar el daño, se pretende obtener, cuando procede: a). La restitución del objeto obtenido mediante la conducta penalmente reprochable, o bien el pago de su valor. b). La indemnización del daño material y moral causado. c). El resarcimiento de los perjuicios ocasionados.

Concepto de fines del Proceso Penal.- Conocimiento que en cada caso concreto deben alcanzar los tribunales respecto de si la afectación de bienes jurídico-penales constituye o no delito y, en caso afirmativo, los elementos que les servirán de base para determinar el quantum de la pena que debe imponerse a su autor (Responsabilidad Penal).

Si el conocimiento no alcanza el carácter de certeza, sino duda respecto de la integración del delito, o de la plena responsabilidad penal del procesado, deberá dictarse sentencia absolutoria; al igual de que si tuviera certeza de no haberse integrado el delito o no haberse probado la existencia de la responsabilidad penal. La sentencia absolutoria jurídicamente no afecta a los supuestos agraviados, pues en todo caso el derecho que le corresponde es *exclusivamente de carácter civil* (Objeto accesorio) y pueden hacerlo valer ante los Tribunales de esa materia (Responsabilidad civil).

RESPONSABILIDAD. Resolución de los tribunales en el sentido de que una persona debe responder por un determinado comportamiento (negativo o positivo) no autorizado por las normas jurídicas; es decir, que es autor de un ilícito y que por lo tanto, resulta merecedor de la sanción prevista por las leyes.

La responsabilidad penal no comprende exclusivamente al delito consumado, y a la autoria material, sino también a la tentativa y ala participación.

Los fines del proceso se clasifican en GENERAL Y ESPECIFICOS.

A).- FIN GENERAL.- Su logro permite al juzgador declarar el derecho, es decir, aplicar la ley al caso concreto.

B).- FINES ESPECIFICOS.- Logrados permiten conocer tanto la existencia del delito como las circunstancias exteriores y las personales del procesado. Constituyen la base para determinar la responsabilidad penal y el quantum de la pena que debe imponerse.

Una vez estudiado el procedimiento penal y sus nociones generales, pasaremos a desarrollar la compatibilidad o incompatibilidad de las figuras jurídico-penales estatuidas en el Código Federal de procedimientos Penales, respecto a los Delitos Informáticos.

6.3. LA PRUEBA.

La prueba es todo medio factible de ser utilizado para el conocimiento de la verdad histórica y la personalidad del delincuente, bajo esa base definir la pretensión punitiva estatal.

El objeto de la prueba es fundamentalmente: la demostración del delito, con sus circunstancias y modalidades (Conducta o hecho, tipicidad, imputabilidad; la personalidad del delincuente; y el grado de responsabilidad y el daño producido). Son objetos de prueba, la conducta o hecho, aspecto interno y manifestación; las personas, probables autor del delito, ofendido, testigos; las cosas, en tanto que en estás recae el daño o sirvieron de instrumento o medio para llevar a cabo el delito y por último los lugares, porque de su inspección, tal vez, se colija algún aspecto o alguna modalidad del delito.

Ahora, ¿Cómo podríamos obtener pruebas a través de Internet?

El anonimato de la red no es obstáculo para la identificación de probables delincuentes.

La imagen o representación de las redes telemáticas como un nuevo espacio, en el que los delitos acostumbran quedar impunes carece de fundamento. Las mismas ventajas que permiten al delincuente moderno aumentar la efectividad de sus acciones, pueden ayudar a los técnicos que participan en la investigación a obtener pruebas evidentes de la identidad y ubicación del probable delincuente o infractor.

Los Nuevos Tipos Penales (Delitos Informáticos) generan otra clase de huellas y evidencias que pueden resultar inequívocas para determinar la autoría de un delito, pero exigen al investigador un conocimiento específico de la materia.

Por otro lado, la gran innovación que Internet aporta a las técnicas de investigación, es la posibilidad de obtener una copia exacta de todos los elementos que han participado en una transacción ilícita. Desde los mensajes transmitidos por los participantes (usuarios) hasta los propios efectos del delito.

A).- LAS PRUEBAS DIGITALES.

Resulta difícil obtener una prueba o por lo menos una evidencia clara en la comisión de los delitos informáticos, ya que sus efectos acostumbran ser únicos e irrepetibles. La tecnología digital utilizada en las redes telemáticas provoca la desaparición del concepto "Original". Los bienes que circulan por Internet han perdido el carácter de irrepetibles, ya que un objeto digital puede reproducirse hasta el infinito sin merma de su calidad y sin huellas que permitan apreciar diferencias entre las distintas reproducciones.

En el caso de los programas de computo, por ejemplo, el órgano judicial que haya ordenado la intervención, puede obtener una copia completa y fehaciente de las aplicaciones informáticas transferidas ilícitamente, sin que las partes que participen en la transacción lleguen a saberlo.

Los mensajes y datos adjuntos que se transmiten a través del correo electrónico, de una lista de distribución, un grupo de noticias o una sesión chat, pueden ser intervenidos en tiempo real y, en algunos casos, incluso unos días después.

B).- LOS SISTEMAS DE IDENTIFICACION.

Durante los primeros años de las redes telemáticas, la información era escasa y estaba limitada a usuarios con privilegios para acceder a la misma. Al mismo tiempo, los diferentes protocolos de transferencia de datos hacían difícil una búsqueda global. En la actualidad, organizaciones públicas y privadas, personas físicas y morales se han lanzado a nutrir la red con datos de toda índole. Los propietarios de contenido han abierto sus sistemas y permitido el acceso al público y a los robots o motores de búsqueda que permiten localizar la información.[89]

En las investigaciones que se han llevado a cabo hasta ahora en nuestro país, la propia red ha suministrado los datos necesarios para completar la identificación de los probables infractores.

[89] http://www.aserte.es/es/04006001.htm

En una primera aproximación, las bases de datos WHOIS, de acceso público y gratuito, permiten conocer la titularidad de un dominio, y con ello, los datos del responsable administrativo, técnico y financiero de un servidor o de una sede Web en la que se están cometiendo actos ilícitos. La información suministrada consta del nombre y los apellidos, el domicilio y el teléfono, así como el IP del servidor primario y secundario. También existen herramientas que permiten conocer el origen de un mensaje, analizando la cabecera del mismo y la ruta que ha seguido.

Existen numerosas fuentes de información, de acceso público que permiten asociar una dirección de correo electrónico a una persona concreta sin alertar a su titular. Además de las bases de datos en las que el propio usuario registra sus datos con el fin de que sus amistades puedan conocer su dirección de correo electrónico (por ejemplo, LISTIN.COM), existen zonas de anuncios gratuitos, clubs de usuarios, asociaciones deportivas, universidades, etc., donde es fácil encontrar el nombre y la dirección e-mail juntos.

El uso de e-mails anónimos o de sistemas de Correo Gratuito como Hotmail, Latinmail, Mailcity, etc., no suponen un obstáculo para conocer la identidad de un usuario, ya que los propietarios de este tipo de servidores están obligados a facilitar los datos de sus usuarios a la autoridad judicial que lo requiera.

C).- SNIFFERS.

España fue el primer país europeo en aplicar la técnica de los sniffers en la investigación de los delitos en Internet. La intervención tuvo lugar en diciembre de 1996, a raíz de una denuncia por distribución no autorizada de programas, obras multimedia y base de datos jurídicos a través de Internet.

El mandamiento judicial recogió cada uno de los pasos necesarios para la interceptación de los mensajes de correo electrónico del probable responsable y su grabación automática en el disco de un ordenador habilitado al efecto. Los treinta días de la intervención telemática arrojaron pruebas concluyentes de la infracción, ya que, junto a los mensajes transferidos se hallaron catálogos, pedidos, ordenes de transferencia de fondos, cracks y los propios programas distribuidos ilícitamente.

D).- OBSTACULOS.

En la mayoría de los países con más incidencia en este tipo de delitos, se presentan problemas que impiden la práctica de las citadas diligencias de investigación, y que en la actualidad son principalmente, los que se enumeran a continuación:

1. Escasez de medios técnicos dedicados a la actividad investigadora.
2. Ventajas tecnológicas de los delincuentes profesionales.
3. Exceso de tiempo transcurrido entre la solicitud de mandamiento de intervención electrónica y su concesión y trámite.
4. Uso de contramedidas, como el cifrado de la información y los sistemas de anonimato real.
5. Problemas de jurisdicción en los delitos transfronterizos.

Los usuarios de Internet, al igual que su colaboración y su comportamiento diario serán los que, en definitiva, deberán reducir las conductas delictivas en la red a un simple e irrisorio dato estadístico.

6.4. LA PERITACIÓN.

Frecuentemente durante la secuela procedimental, las limitaciones en el campo el conocimiento, los representantes del Ministerio Público, del Juez, del procesado y su defensor, motiva el concurso de la técnica especializada en múltiples órdenes, para dilucidar o precisar las muy variadas situaciones, relacionadas con la conducta o hecho, para así, estar en aptitud de definir la Pretensión Punitiva Estatal. Esto justifica la intervención de terceros, poseedores o expertos en técnicas o especialidades diversas, los cuales se denominan PERITOS.

Según el maestro Guillermo Colín Sánchez, hablar de Peritación implica los siguientes conceptos:

PERITO. Es toda persona, a quien se atribuye capacidad, técnico-científica, o práctica, en una ciencia o arte.
PERICIA. Es la capacidad técnico-científica, o práctica, que sobre una ciencia o arte posee el sujeto llamado Perito.
PERITACIÓN. Es el procedimiento empleado por el perito, para realizar sus fines.
PERITAJE. Es la operación el especialista, traducida en puntos concretos, en inducciones razonadas y operaciones emitidas, como generalmente se dice, de acuerdo con su "leal saber y entender" y en donde se llega a conclusiones concretas.[90]

Para el Dr. Guillermo Colín Sánchez la peritación, es el acto procedimental, en el que, el técnico o especialista en un arte o ciencia (perito), previo examen de una persona, de una conducta o hecho, cosa, circunstancia, efectos, etc., emite un dictamen,

[90] http://info1.juridicas.unam.mx/legfed/8/

conteniendo su parecer, basado en razonamientos técnicos sobre aquellos en lo que se ha pedido su intervención.

El Código Federal de Procedimientos Penales, establece las siguientes disposiciones respecto a los peritos.

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES
CAPITULO IV
PERITOS

Artículo 220.- Siempre que para el examen de personas, hechos u objetos, se requieran conocimientos especiales se procederá con intervención de peritos.

Artículo 221.- Los peritos que dictaminen serán dos o más; pero bastara uno cuando solamente este pueda ser habido, o cuando el caso sea urgente.

Artículo 222.- Con independencia de las diligencias de pericia desahogadas en la averiguación previa, la defensa y el ministerio público tendrán derecho a nombrar hasta dos peritos en el proceso, para dictaminar sobre cada punto que amerite intervención pericial. El tribunal hará saber a los peritos su nombramiento y les ministrara todos los datos que fueren necesarios para que emitan su opinión.

Artículo 223.- Los peritos deberán tener titulo oficial en la ciencia o arte a que se refiere el punto sobre el cual deba dictaminarse, si la profesión o arte están legalmente reglamentadas; en caso contrario, se nombrara peritos prácticos.

Artículo 224.- También podrán ser nombrados peritos prácticos cuando no hubiere titulados en el lugar en que se siga la instrucción; pero en este caso se librara exhorto o requisitoria al tribunal del lugar en que los haya, para que en vista del dictamen de los prácticos emitan su opinión.

Artículo 225.- La designación de peritos hecha por el tribunal o por el ministerio publico deberá recaer en las personas que desempeñen ese empleo por nombramiento oficial y a sueldo fijo, o bien en personas que presten sus servicios en dependencias del gobierno federal, en universidades del país, o que pertenezcan a asociaciones de profesionistas reconocidas en la república. Si no hubiere peritos oficiales titulares se nombraran de entre las personas que desempeñen el profesorado del ramo correspondiente en las escuelas nacionales, o bien de entre los funcionarios o empleados de carácter técnico en establecimientos o corporaciones dependientes del gobierno.

Artículo 226.- Si no hubiere peritos de los que menciona el Articulo anterior y el tribunal o el ministerio publico lo estiman conveniente, podrán nombrar otros. En estos casos los honorarios se cubrirán según lo que se acostumbre pagar en los establecimientos particulares del ramo de que se trate a los empleados

permanentes de los mismos, teniendo en cuenta el tiempo que los peritos debieron ocupar en el desempeño de su comisión.

Artículo 227.- Los peritos que aceptan el cargo, con excepción de los oficiales titulares, tiene obligación de protestar su fiel desempeño ante el funcionario que practique las diligencias.

En casos urgentes la protesta la rendirán al producir o ratificar su dictamen.

Artículo 228.- El funcionario que practique las diligencias fijara a los peritos el tiempo en que deban cumplir su cometido. Si transcurrido ese tiempo no rinden su dictamen o si legalmente citados y aceptado el cargo, no concurren a desempeñarlo, se hará uso de alguno de los medios de apremio.

Si a pesar de haber sido apremiado el perito no cumple con las obligaciones impuestas en el párrafo anterior, se hará su consignación al ministerio publico para que proceda por el delito a que se refiere el Artículo 178 del código penal.
Artículo 233.- El funcionario que practique las diligencias y las partes, podrán hacer a los peritos las preguntas que resulten pertinentes sobre la materia objeto de la pericia; les dará por escrito o de palabra, pero sin sugestión alguna, los datos que tuviere y hará constar estos hechos en el acta respectiva.

Artículo 234.- Los peritos practicaran todas las operaciones y experimentos que su ciencia o arte les sugiera y expresaran los hechos y circunstancias que sirvan de fundamento a su opinión.

Artículo 235.- Los peritos emitirán su dictamen por escrito y lo ratificaran en diligencia especial. Los peritos oficiales no necesitaran ratificar sus dictámenes, sino cuando el funcionario que practique las diligencias lo estime necesario. En esta diligencia el juez y las partes podrán formular preguntas a los peritos.

Artículo 236.- cuando las opiniones de los peritos discordaren, el funcionario que practique las diligencias los citara a junta en la que se discutirán los puntos de diferencia, haciéndose constar en el acta el resultado de la discusión. Si los peritos no se pusieren de acuerdo se nombrara un perito tercero en discordia.

Artículo 238.- cuando el funcionario que practique las diligencias lo crea conveniente, podrá ordenar que asistan peritos a ellas.[91]

Los artículos transcritos, regulan la conducta, actividades, y limitantes de los peritos (formalidades que deben observarse en el proceso), los cuales son aplicables - una vez ya tipificados -, a los Delitos Informáticos, es decir, a aquellos peritos encargados de intervenir algún medio de comunicación, rastrear a alguna persona en determinado país, vigilar y controlar el acceso a usuarios extraños a los sistemas de seguridad de

[91] http://info1.juridicas.unam.mx/legfed/18/

determinada empresa, o presentar algún soporte de almacenamiento magnético con información que sirva de prueba para imputar responsabilidad al inculpado, etc.

Ahora bien, por cuanto hace a la valoración de los dictámenes de peritos científicos, será calificada por el Juez o tribunal, según las circunstancias. Aunque el Juez goza de libertad suficiente para valorar el dictamen pericial, ello, no es sinónimo de arbitrariedad; sí de valoración se trata, esto implica un razonamiento suficiente, para justificar él porque se acepta o se rechaza el dictamen.

6.5. EL EXHORTO.

El oficio que el juez o tribunal libra a otro de igual categoría a la suya y en que le pide practique alguna notificación, embargo, o en general cualquiera especie de diligencia judicial que debe tener lugar dentro de la jurisdicción del juez exhortado. Al exhorto se le da ese nombre porque en él se usaba y aun se usa; aunque menos que antes, la siguiente formula: ***por lo expuesto, exhorto y requiero a Usted y de mi parte le encarezco se sirva diligenciar el presente, seguro de mi reciprocidad cuando por Usted fuese requerido.***

A continuación veremos algunas disposiciones jurídicas relativas a los Exhortos tanto en nuestro país, como en el extranjero.

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES.
CAPITULO VI
REQUISITORIAS Y EXHORTOS

Artículo 45.- Las diligencias de averiguación previa que deban practicarse fuera del lugar en que se este tramitando alguna averiguación, se encargaran a quien toque desempeñar esas funciones en el lugar donde deban practicarse, enviándole la averiguación original o un oficio con las inserciones necesarias.

Artículo 46.- Cuando tengan que practicarse diligencias judiciales fuera del territorio jurisdiccional del tribunal que conozca del asunto, se encomendara su cumplimiento al de igual categoría del territorio jurisdiccional donde deban practicarse.

Si las diligencias tuvieren que practicarse fuera del lugar de la residencia del tribunal, pero dentro de su territorio jurisdiccional, y aquel no pudiere trasladarse, se encargara su cumplimiento al inferior del mismo fuero, o a la autoridad judicial del orden común del lugar donde deban practicarse.

Se empleara la forma de exhorto cuando se dirija a un tribunal igual en categoría, y de requisitoria cuando se dirija a un inferior. Al dirigirse los tribunales a

funcionarios o autoridades que no sean judiciales, lo harán por medio de oficio.

Artículo 47.- Cuando el tribunal federal requerido no pudiere practicar por si mismo, en todo o en parte, las diligencias que se le encarguen, podrá encomendar su ejecución al juez del orden común del lugar donde deban practicarse, remitiéndole el exhorto original o un oficio, con las inserciones necesarias.

Artículo 48.- Cuando el tribunal no pueda dar cumplimiento al exhorto o requisitoria, por hallarse en otra jurisdicción la persona o las cosas que sean objeto de la diligencia, lo remitirá al tribunal del lugar en que aquella o estas se encuentren, y lo hará saber al requirente.

El cumplimiento de los exhortos o requisitorias no implica prorroga ni renuncia de competencia.

Artículo 49.- Los exhortos y requisitorias contendrán las inserciones necesarias, según la naturaleza de las diligencias que hayan de practicarse; llevaran el sello del tribunal, e irán firmados por el funcionario correspondiente y por el secretario respectivo o por testigos de asistencia.

Los tribunales requeridos tramitaran los exhortos y requisitorias aun cuando carezcan de alguna formalidad, si la ausencia de esta no afecta su validez o impide el conocimiento de la naturaleza y características de la diligencia solicitada, excepto ordenes de aprehensión y de cateo, las que deben llenar todas las formalidades.

Artículo 50.- En casos urgentes, notificado que fuere de ello previamente el ministerio publico y quien corresponda conforme a la ley, podrá resolverse que se haga uso de la vía telegráfica, expresándose con toda claridad las diligencias que han de practicarse, la parte que las solicito, el nombre del inculpado, si fuere posible, el delito de que trata y el fundamento de la providencia. Estos exhortos se mandaran mediante oficio al jefe de la oficina telegráfica de la localidad, Acompañados de una copia, en la cual el empleado respectivo de dicha oficina extenderá recibo; el oficio será entregado por conducto del secretario o del actuario del tribunal, quienes se identificaran ante el encargado del servicio telegráfico, quien deberá agregar esta circunstancia al texto del telegrama. En la misma fecha en que se entregue el citado oficio a la oficina telegráfica, el tribunal requirente enviara por correo el exhorto o requisitoria en forma.

Artículo 53.- El tribunal que recibiere un *exhorto o requisitoria extendido* en debida forma, procederá a cumplimentarlo en un plazo no mayor de cinco días contados a partir de la fecha de su recibo; si por la naturaleza o circunstancia de la diligencia no fuere posible su cumplimentación en el plazo indicado, el tribunal lo resolverá así, determinando o razonando las causas de ello. Si estimare que no concurren en el todos los requisitos legales, lo devolverá al requirente, fundando su negativa dentro del mismo plazo establecido en este Artículo.

Cuando un tribunal no atienda un exhorto o requisitoria sin motivo justificado, el

que lo haya expedido podrá ocurrir en queja ante el superior de aquel. Recibida la queja, será resuelta dentro del termino de tres días, con vista de las constancias del exhorto o requisitoria, de lo que expongan las autoridades contendientes y audiencia del ministerio publico.
Artículo 54.- Si el tribunal exhortado estimare que no debe cumplimentar el exhorto por interesarse en ello su jurisdicción, oirá al ministerio publico y resolverá dentro de tres días, promoviendo en su caso la competencia respectiva.

Artículo 55.- Se dará entera fe y crédito a los exhortos y requisitorias que libren los tribunales de la federación, debiendo cumplimentarse siempre que llenen las condiciones fijadas por este código.

Artículo 56.- Cuando se demore el cumplimiento de un exhorto o requisitoria, se recordara su despacho por medio de oficio. Si a pesar de esto continua la demora, el tribunal requirente lo pondrá en conocimiento del superior inmediato del requerido, si se trata de exhorto. Dicho superior apremiara al moroso, obligándolo a que diligencie el exhorto y hará la consignación del caso al ministerio publico, si procede.

Si se tratare de requisitoria y continuare la demora, el tribunal requirente hará uso de los medios de apremio y, si procediere, consignara el caso al ministerio publico.

Artículo 57.- La resolución dictada por el tribunal requerido ordenando negando la practica de las diligencias que se le hayan encomendado, admite los recursos que este código establece y que se resolverán por el órgano jurisdiccional federal competente en el circuito en que se ubique el citado tribunal requerido.

Artículo 58.- Los exhortos dirigidos a los tribunales extranjeros se remitirán, con aprobación de la suprema corte de justicia, por la vía diplomática al lugar de su destino. Las firmas de las autoridades que los expidan serán legalizadas por el presidente o el secretario general de acuerdos de aquella y las de estos servidores públicos por el secretario de relaciones exteriores o el servidor publico que el designe.

Artículo 59.- Podrá encomendarse la practica de diligencias en países extranjeros a los secretarios de legaciones y a los agentes consulares de la república, por medio de oficio con las inserciones necesarias.

Artículo 60.- Los exhortos de los tribunales extranjeros deberán tener, además de los requisitos que indiquen las legislaciones respectivas y los tratados internacionales, la legalización que haga el representante autorizado para atender los asuntos de la república en el lugar donde sean expedidos.[92]

[92] El código federal de procedimientos penales, publicado en el D.O.F. el 10 de enero de 1994.

6.6.- LEY DE EXTRADICION INTERNACIONAL

La ley de Extradición Internacional, no favorece la extradición de inculpados, que hayan cometido algún Delito Informático, ya sea que el delito haya tenido origen en nuestro país y efectos en otro; o que se haya cometido en el extranjero y el delincuente este refugiado en México, ya que en los artículos 5 y 6 de la ley citada, limita y condiciona tal extradición (Ver Anexo VII).

> **Artículo 5.-** Podrán ser entregados conforme a esta ley los individuos contra quienes en otro país, se haya incoado un proceso penal como presuntos responsables de un delito o que sean reclamados para la ejecución de una sentencia dictada por las autoridades judiciales del estado solicitante.
>
> **Artículo 6.-** Darán lugar a la extradición los delitos dolosos o culposos, definidos en la ley penal mexicana, si concurren los requisitos siguientes:
>
> I.- Que tratándose de delitos dolosos, sean punibles conforme a la ley penal mexicana y a la del estado solicitante, con pena de prisión cuyo termino medio aritmético por lo menos sea de un año; y tratándose de delitos culposos, considerados como graves por la ley, sean punibles, conforme a ambas leyes, con pena de prisión.[93]

Por cuanto hace al artículo 5, este condiciona la entrega del delincuente, solo si se inicio un procedimiento penal en su contra o para la ejecución de una sentencia penal. Y el artículo 6, limita la extradición del reo, si el delito por el cual se reclama se encuentra definido y sancionado por las leyes mexicanas, en consecuencia, los Delitos Informáticos al no estar estatuidos en las leyes penales mexicanas, no se podrá extraditar a ningún indiciado por tal delito. Al margen de que tampoco existe un tratado internacional que regula tal situación.

Por otro lado, presentamos algunas tesis jurisprudenciales relativas a la extradición de reos.

> **| InfoJus | Consulta | Derechos Reservados, (C)1996 IIJ-UNAM**
> **Instituto de Investigaciones Jurídicas de la UNAM**
> **Tesis correlacionada con los artículos:**
> **| 6 del Código Penal | 395 del Código Penal |**
> **Registro: 32863**
>
> **Título: EXTRADICION. EL TRATADO INTERNACIONAL RELATIVO (4 DE MAYO DE 1978) CELEBRADO POR LOS ESTADOS UNIDOS DE AMERICA Y LOS ESTADOS UNIDOS MEXICANOS NO VIOLA**

[93] http://info1.juridicas.unam.mx/legfed/34

EL Artículo 14 CONSTITUCIONAL.

Texto: El tratado internacional de extradición celebrado por los Estados Unidos de América y los Estados Unidos Mexicanos no viola el artículo 14 constitucional al no establecer un período de pruebas y alegatos dentro del procedimiento de extradición de un reo, ya que dicha extradición sólo puede llevarse a cabo *mediante la aplicación del tratado internacional* mencionado, cuyas partes son las naciones contratantes. En el curso de tal aplicación, una de ellas deberá demostrar la procedencia de la extradición solicitada, y la otra la calificará. Consecuentemente, el reo respecto del cual exista solicitud de extradición no es parte directa en ese procedimiento, por lo que nada tiene que alegar ni probar.

Amparo en revisión 5707/86. Richard Lyman Pitt. 15 de marzo de 1990. Unanimidad de 18 votos de los señores ministros: Magaña Cárdenas, Alba Leyva, Azuela Güitrón, Rocha Díaz, López Contreras, Fernández Doblado, Pavón Vasconcelos, Adato Green, Rodríguez Roldán, Martínez Delgado, Carpizo Mac Gregor, Villagordoa Lozano, Moreno Flores, García Vázquez, Chapital Gutiérrez, Díaz Romero, Schmill Ordóñez y Presidente del Río Rodríguez. Ausentes: de Silva Nava, González Martínez y Castañón León. Ponente: Ulises Schmill Ordóñez. Secretario: Víctor Ernesto Maldonado Lara. Tesis número XLV/90, fue aprobada por el Tribunal en Pleno en Sesión Privada celebrada el miércoles doce de septiembre en curso. Unanimidad de 19 votos de los señores ministros: Presidente Carlos del Río Rodríguez, Carlos de Silva Nava, Ignacio Magaña Cárdenas, Mariano Azuela Güitrón, Samuel Alba Leyva, Noé Castañón León, Felipe López Contreras, Luis Fernández Doblado, José Antonio Llanos Duarte, Santiago Rodríguez Roldán, José Martínez Delgado, Clementina Gil de Lester, Atanasio González Martínez, José Manuel Villagordoa Lozano, Fausta Moreno Flores, Carlos García Vázquez, Sergio Hugo Chapital Gutiérrez, Juan Díaz Romero y Ulises Schmill Ordóñez. Ausentes: Salvador Rocha Díaz y Victoria Adato Green. México, Distrito Federal, a veinte de septiembre de mil novecientos noventa.

Semanario Judicial de la Federación, octava época, tomo VI primera parte. Pág. 30.

Registro: 739
Año: 1931
Epoca: 5

Título: EXTRADICION, TRATADOS DE.

Texto: Cuando al reclamar contra una extradición, se invoque por el quejoso, la violación de las garantías que otorga el artículo 22 constitucional, que prohibe las penas inusitadas y, además, el artículo 15 constitucional, alegando la improcedencia de la extradición, la Corte debe estudiar la constitucionalidad o inconstitucionalidad del acto reclamado, bajo ese aspecto. ID. ID. Los tratados

celebrados con un país extranjero, no pueden desconocer o alterar las garantías y derechos del hombre y del ciudadano, porque tales derechos constituyen la razón y el objeto de nuestras instituciones; y obligándose nuestra Ley Fundamental a respetarlos, sería contradictorio y absurdo consignar su desconocimiento en convenios con potencias extranjeras; de suerte es que, de acuerdo con el tratado que se haya celebrado entre México y otro país, puede concederse la extradición de un reo, si las penas que tenga que sufrir en ese país, no son de las prohibidas por razón de las garantías individuales que el nuestro otorga y que protegen al extranjero, así es que habiendo concordancia entre el Tratado y la Constitución, de acuerdo con el artículo 15 del mismo, deben aplicarse nuestras leyes y, en primer término, la Suprema de ellas, que es la Constitución, desde el momento en que ésta, al prohibir la celebración de tratados, en los que se alteren las garantías y derechos establecidos para el hombre y el ciudadano, está ordenando el respecto a tales garantías, aun en casos de extradición. T. XXXI, p. 347.

Amparo administrativo en revisión 2339/30, Sichel Enrico, 21 de enero de 1931, unanimidad de 4 votos.

Novena Epoca
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: II, Octubre de 1995
Tesis: 1a. XXXIX/95
Página: 200

EXTRADICION, PROCEDIMIENTO DE. FASES PROCESALES. Existen tres períodos perfectamente definidos en los que se encuentra dividido el citado procedimiento: a) el que se inicia con la manifestación de intención de presentar formal petición de extradición, en la que el Estado solicitante expresa el delito por el cual pedirá la extradición y que existe en contra del reclamado una orden de aprehensión emanada de autoridad competente; o en su caso, a falta de tal manifestación de intención, el que inicia con la solicitud formal de extradición, la cual debe contener todos y cada uno de los requisitos a que se refiere el artículo 16 de la Ley de Extradición Internacional o los establecidos en el tratado respectivo; b) el que comienza con la decisión de la Secretaría de Relaciones Exteriores de admitir la petición, por estar satisfechos los requisitos legales correspondientes, etapa dentro de la cual interviene el juez de Distrito competente y emite su opinión; y c) aquel en el que esta dependencia del Ejecutivo Federal resuelve si concede o rehusa la extradición, sin estar vinculado jurídicamente a la opinión que dictó el juez de Distrito. Luego entonces, las violaciones que en su caso se cometan en una etapa concluida quedan consumadas irreparablemente por cesación de efectos del acto y no pueden afectar ni trascender a la otra.

Amparo en revisión 1752/94. Mario Fernando Zablah o Carlos Bendeck o Jorge Samur. 4 de agosto de 1995. Cinco votos. Ponente: Humberto Román Palacios. Secretario: Manuel Rojas Fonseca.

En resumen, sí cualquier país que sí tipifique los delitos informáticos (Estados Unidos, Francia, España, Alemania, Japón, Austria, entre otros) nos solicita la extradición de algún delincuente, una vez iniciado un proceso en su contra o para la ejecución de una sentencia penal, en este tipo de delitos, México se la negará toda vez, que no cumple con los requisitos establecidos en la ley de extradición internacional Art. 5 y 6. Y más aún por no existir un Tratado Internacional respecto a los Delitos Informáticos y la Extradición de sus Autores.

6.7. LA JURISDICCIÓN.

La Jurisdicción es la función Estatal que tiene el cometido de dirimir los conflictos entre los individuos para imponer el derecho. Como su etimología lo expresa, significa "decir el derecho" (Juris-dictio) aunque en la concepción más moderna, no solo es eso (juzgar) sino también ejecutar lo juzgado.[94]

Según el maestro Eduardo Pallares, la jurisdicción penal es la que ejercen los tribunales cuando aplican las leyes penales, o sea la potestad jurídica de aplicar y hacer que se cumplan dichas leyes.[95]

El órgano judicial aplica el derecho establecido. Por eso el juez debe buscar la norma (inclusive interpretarla, buscar su sentido, integrarla, si hay un vacío) para luego aplicarlo al caso concreto que se le plantea. La potestad jurisdiccional, entonces, es el poder-deber de realizar dicha tarea la de imponer la norma jurídica resolviendo los casos concretos con el fin de lograr la paz social mediante la imposición del derecho. Naturalmente que en su realización satisface intereses privados (y derechos subjetivos) al cumplir dicha función pública.[96]

La jurisdicción y la competencia, son conceptos que no deben confundirse, debido a que, se puede tener jurisdicción, más no competencia; la primera implica la potestad para declarar el derecho y, la segunda, para precisar la rama del derecho o el ordenamiento jurídica sobre la que se tendrá dicha potestad.[97]

La competencia, se ha clasificado en diversas formas; la más reconocidas, tanto en la doctrina como en la legislación, es en razón de la materia, del territorio, del grado y la cuantía. En el Derecho Mexicano, se determina en razón de la materia, de las personas,

---

[94] Enrique Véscovi. Teoria General de Proceso. Editorial Temis. Libreria Bogotá-Colombia. 1984. Pág. 8.
[95] Eduardo Pallares. Diccionariode Derecho Procesal Civil Editorial Porrúa. s.a. Vigésima Edición. México 1991. Pag. 515.
[96] Enrique Véscovi. Teoria General de Proceso. Editorial Temis. Libreria Bogotá-Colombia. 1984. Pág. 117.
[97] Colin Sánchez, Guillermo. Derecho mexicano de procedimientos penales. Edición 14. Editorial Porrúa s.a. Pág. 179

del lugar y como excepción a las reglas generales, en función de Conexidad.[98]

La distinción entre Jurisdicción y Competencia, estriba en que la primera es la potestad genérica de todo tribunal; y la segunda, el poder específico (concreto) de intervenir en determinadas causas. Es decir, que todos los jueces ejercen Jurisdicción, pero algunos son competentes para conocer determinados asuntos y otros no, dependiendo de distintos factores como son el territorio, materia, grado y la cuantía.

Una vez estudiados los conceptos anteriores, analizaremos como se maneja y aplica la competencia jurisdiccional en Internet, respecto a los Delitos Informáticos.

6.8. COMPETENCIA JURISDICCIONAL EN INTERNET.

Es irreversible el aumento de procedimientos judiciales relativos a los Delitos Informáticos que se cometen a través de Internet. Los efectos transfronterizos de estas actividades Ilícitas (tipificadas solo en algunos países) obligan a determinar cuál debe ser la jurisdicción competente para enjuiciar los delitos que tienen origen en un país y causan sus efectos en otro.

En España, la Ley Orgánica del Poder Judicial establece en su artículo 23 que corresponderá a la jurisdicción española el conocimiento de las causas por delitos cometidos en territorio español.

La jurisprudencia del Tribunal Supremo de España, define como "delitos a distancia" aquéllos en los que la actividad se realiza en un lugar y el resultado se consigue en otro distinto. A la hora de determinar el lugar de la comisión de estos delitos, se enfrentan las teorías de la manifestación de la voluntad y la del resultado, no dominando exclusivamente ninguna de ellas, pues siempre se debe atender a la condición, naturaleza y presupuestos de las infracciones criminales a que se aplica.

Por ello, si se trata de delitos continuados, debe ser competente el Juez del lugar donde radique el centro de las actividades criminales y en el que se fraguaron los distintos delitos, y se cursaron órdenes y datos para su realización .Sin embargo, algunas sentencias dictadas, asignan la competencia jurisdiccional al Juez del lugar donde se produjo el resultado perjudicial del delito. Pero ambas corrientes jurisprudenciales apoyan la tesis de que la jurisdicción española es competente para enjuiciar los delitos planeados y organizados en España, por ciudadanos españoles, dirigidos al público español y cuyos resultados se producen también en nuestro país, a pesar de que los medios técnicos utilizados para promocionar la actividad infractora se hallen situados en

[98] Ibidem. Pág. 180.

un país extranjero.[99]

El artículo 23 de la Ley Orgánica de Poder Judicial en España, señala los supuestos de Extraterritorialidad, los cuales se enumeran de la siguiente manera:

1. En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte.

2. Asimismo conocerá de los hechos previstos en las leyes penales españolas como delitos, aunque hayan sido cometidos fuera del territorio nacional, siempre que los criminalmente responsables fueren españoles o extranjeros que hubieren adquirido la nacionalidad española con posterioridad a la comisión del hecho y concurrieren los siguientes requisitos:

a) Que el hecho sea punible en el lugar de ejecución.
b) Que el agraviado o el Ministerio Fiscal denuncien o interpongan querella ante los Tribunales españoles.
c) Que el delincuente no haya sido absuelto, indultado o penado en el extranjero, o, en este último caso, no haya cumplido la condena. Si sólo la hubiere cumplido en parte, se le tendrá en cuenta para rebajarle proporcionalmente la que le corresponda.

3. Conocerá la jurisdicción española de los hechos cometidos por españoles o extranjeros fuera del territorio nacional cuando sean susceptibles de tipificarse, según la ley penal española, como alguno de los siguientes delitos:

a) De traición y contra la paz o la independencia del Estado.
b) Contra el titular de la Corona, su Consorte, su Sucesor o el Regente.
c) Rebelión y sedición.
d) Falsificación de la firma o estampilla reales, del sello del Estado, de las firmas de los Ministros y de los sellos públicos u oficiales.
e) Falsificación de moneda española y su expedición.
f) Cualquier otra falsificación que perjudique directamente al crédito o intereses del Estado, e introducción o expedición de lo falsificado.
g) Atentado contra autoridades o funcionarios públicos españoles.
h) Los perpetrados en el ejercicio de sus funciones por funcionarios públicos españoles residentes en el extranjero y los delitos contra la Administración pública española.
i) Los relativos al control de cambios.

4. Igualmente será competente la jurisdicción española para conocer de los hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse, según la ley penal española, como alguno de los siguientes delitos:

a) Genocidio.

[99] http://www.asertel.es/cs/0400400.htm

b) Terrorismo.
c) Piratería y apoderamiento ilícito de aeronaves.
d) Falsificación de moneda extranjera.
e) Los relativos a la prostitución.
f) Tráfico ilegal de drogas psicotrópicas, tóxicas y estupefacientes.
g) Y cualquier otro que, según los tratados o convenios internacionales, deba ser perseguido en España.

5. En los supuestos de los apartados 3 y 4 será de aplicación lo dispuesto en la letra c) del apartado 2 de este artículo. [100]

Cabe recordar que en la legislación Española, se encuentran tipificados los Delitos Informáticos en varias modalidades y que además España tiene firmados Tratados Internacionales con otros países, en donde en ambos se regulan como conductas ilícitas, el mal uso y manejo de las computadoras, en perjuicio y/o con efectos en otros países. Consecuentemente, la competencia jurisdiccional para resolver un Delito Informático entre dos países que lo tipifican como tal, se regirá de acuerdo a su Legislación Nacional, o en su caso, por el Tratado Internacional vigente para ambos.

A continuación se transcribe: El Caso Mecklermedia, sucedido en Septiembre de 1997, en el que se suscita el problema de la Competencia Jurisdiccional para resolver un Delito Informático.

Caso Mecklermedia
Noticia. Septiembre de 1997

Un nuevo precedente judicial en Europa contribuye a reforzar la tesis de que el tribunal del lugar donde se producen los efectos de un delito puede declararse competente para enjuiciar los hechos cometidos a través de un servidor ubicado en otro país.

Un tribunal inglés considero que tenía competencia jurisdiccional para valorar la ilicitud del dominio HARRODS.COM, que entraba en conflicto con la marca inglesa HARRODS.

Ahora, el Tribunal Supremo del Reino Unido ha reiterado que los problemas de marcas que afectan a una marca inglesa en Internet, deber ser enjuiciados en Inglaterra.

En este caso, el demandante es una empresa norteamericana, Mecklermedia, que organiza el congreso INTERNET WORLD y ofrece información del mismo en su Web en Internet.

[100] http://www.ascrtel.es/es/o4004002.htm

> **La demandada es una empresa alemana que organiza un congreso con la misma denominación y hace publicidad del mismo en inglés, en un web al que se accede a través del dominio IWORLD.**
>
> **Mientras la empresa alemana argumentaba que el procedimiento debía entablarse en Alemania, por ser el país en el que estaba el servidor, el tribunal inglés ha entendido que la jurisdicción del Reino Unido debe conocer aquellos casos en los que la actividad va dirigida a los habitantes de dicho país y en su idioma oficial, que es diferente al del lugar de origen (Alemania). Además, el material infractor se recibe también en el Reino Unido.**[101]

Por otro lado, en México no se encuentran tipificados Los Delitos Informáticos a Nivel Federal (a excepción del Código Penal del Estado de Sinaloa que los estatuye a nivel local) y por ello no sería posible enjuiciar a ninguna persona, si cometiera tal actividad ilícita, con origen en nuestro país o fuera de él y con efectos en el mismo o en el extranjero.

Sin embargo, al margen del mismo, analizaremos algunas disposiciones Extraterritoriales, del **Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal**, en las que corresponde a la jurisdicción Mexicana el conocimiento de las causas por delitos cometidos en el mismo.

> **Artículo 1.-** *Este código se aplicara en el distrito federal,* por los delitos de la competencia de los tribunales comunes; y en toda la república, para los delitos de la competencia de los tribunales federales.
>
> **Artículo 2.-** Se aplicara, asimismo:
> I.- Por los delitos que se inicien, preparen o cometan en el extranjero, cuando produzcan o se pretenda que tenga efectos en el territorio de la república, y
> II.- Por los delitos cometidos en los consulados mexicanos o en contra de su personal, cuando no hubieren sido juzgados en el país en que se cometieron.
>
> **Artículo 3.-** Los delitos continuos cometidos en el extranjero, que se sigan cometiendo en la república, se perseguirán con arreglo a las leyes de esta, sean *mexicanos o extranjeros los* delincuentes.
>
> La misma regla se aplicara en el caso de delitos continuados.
>
> **Artículo 4.-** Los delitos cometidos en territorio extranjero por un mexicano contra mexicanos o contra extranjeros, o por un extranjero contra mexicanos, serán penados en la república, con arreglo a las leyes federales, si concurren los

[101] http://www.asertel.es/es/04004004.htm.

requisitos siguientes:
I.- Que el acusado se encuentre en la república;
II.- Que el reo no haya sido definitivamente juzgado en el país en que delinquió, y
III.- Que la infracción de que se le acuse tenga el carácter de delito en el país en que se ejecuto y en la república.

Artículo 5.- Se consideraran como ejecutados en territorio de la república:
I.- Los delitos cometidos por mexicanos o por extranjeros en alta mar, a bordo de buques nacionales;
II.- Los ejecutados a bordo de un buque de guerra nacional surto en puerto o en aguas territoriales de otra nación. Esto se extiende al caso en que el buque sea mercante, si el delincuente no ha sido juzgado en la nación a que pertenezca el puerto;
III.- Los cometidos a bordo de un buque extranjero surto en puerto nacional o en aguas territoriales de la república, si se turbare la tranquilidad pública o si el delincuente o el ofendido no fueren de la tripulación. En caso contrario, se obrara conforme al derecho de reciprocidad;
IV.- Los cometidos a bordo de aeronaves nacionales o extranjeras que se encuentren en territorio o en atmósfera o aguas territoriales nacionales o extranjeras, en casos análogos a los que señalan para buques las fracciones anteriores, y
V.- Los cometidos en las embajadas y delegaciones mexicanas.

Artículo 6.- Cuando se cometa un delito no previsto en este código, pero si en una ley especial o en un tratado internacional de observancia obligatoria en México, se aplicaran estos, tomando en cuenta las disposiciones del libro primero del presente código y, en su caso, las conducentes del libro segundo.

Cuando una misma materia aparezca regulada por diversas disposiciones, la especial prevalecerá sobre la general.[102]

Por otro lado, **El Código Federal de Procedimientos Penales,** publicado en el Diario Oficial de la Federación de 30 de Agosto de 1934 y corregido según fe de erratas de Diario Oficial de 1°. De Noviembre de 1934, establece en su Titulo Primero, Reglas Generales para el Procedimiento Penal, Capitulo I, Competencia:

Artículo 6.- Es tribunal competente para conocer de un delito, el del lugar en que se comete, salvo lo previsto en los párrafos segundo y tercero del Artículo 10.

Si el delito produce efectos en dos o más entidades federativas, será competente el juez de cualquiera de estas o el que hubiera prevenido.

Artículo 7.- En los casos de los artículos 2, 4 y 5, Fracción V, del código penal, será competente el tribunal en cuya jurisdicción territorial se encuentre el

[102] http://info1.juridicas.unam.mx/legfed/11

inculpado; pero si este se hallare en el extranjero, lo será para solicitar la extradición, instruir y fallar el proceso, el tribunal de igual categoría en el distrito federal, ante quien el ministerio publico ejercite la acción penal.

Artículo 8.- En los casos de las fracciones I y II del Artículo 5 del código penal, es competente el tribunal a cuya jurisdicción corresponda el primer punto del territorio nacional donde arribe el buque; y en los casos de la fracción III del mismo Artículo, el tribunal a cuya jurisdicción pertenezca el puerto en que se encuentre o arribe el buque.

Artículo 9.- Las reglas del artículo anterior son aplicables, en los casos análogos, a los delitos a que se refiere la fracción IV del mismo artículo 5 del Código Penal.

Artículo 10.- Es competente para conocer de los delitos continuados o y de los continuos o permanentes, cualquiera de los Tribunales en cuyo territorio aquellos produzcan efectos o se hayan realizado actos constitutivos de tales delitos.

En caso de concurso de delitos, el Ministerio Público Federal será competente para conocer de los delitos del fuero común que tengan conexidad con delitos federales y los jueces federales tendrán, asimismo, competencia para juzgarlos.

También será competente para conocer de un asunto, un juez de Distrito distinto al del lugar de comisión del delito, si por razones de seguridad en las prisiones, atendiendo a las características del hecho imputado, a las circunstancias personales del inculpado y a otras que impidan garantizar el desarrollo adecuado del proceso, el Ministerio Público Federal considera necesario llevar el ejercicio de la acción penal ante otro juez. Lo anterior es igualmente aplicable para los casos en que, por las mismas razones, la autoridad judicial de oficio o a petición de parte, estime necesario trasladar a un procesado a algún centro de reclusión de máxima seguridad, en las que será competente el tribunal del lugar en que se ubica dicho centro.

Artículo 11.- Para la decisión de las competencias se observarán las siguientes reglas:

I.- Las que se susciten entre los tribunales federales se decidirán a conforme a los artículos anteriores, y si hay dos o más competentes, a favor del que haya prevenido;

II.- Las que se susciten entre los tribunales de la federación y los de los Estados Unidos o Distrito Federal, se decidirán declarando cual es el fuero en que radica la jurisdicción; y

III.- Las que se susciten entre los tribunales de un Estado y los de otro, o entre los del Distrito Federal, se decidirán conforme a las leyes de esas entidades, si tienen la misma disposición respecto del punto jurisdiccional controvertido. En caso contrario, se decidirán con arreglo a lo dispuesto en ese capítulo.[103]

[103] http://info1.juridicas.unam.mx/legfed/8/

En resumen, el Código Penal Federal, no obstante que establece disposiciones para aplicarlas extraterritorialmente y enjuiciar a los infractores de las normas mexicanas en nuestro país, no estatuye los Delitos Informáticos a nivel federal y por ello, no podría conocer tales ilícitos.

Y por cuanto hace al Código Federal de Procedimientos Penales, en su capítulo de Competencia, toda vez que no existe el tipo penal de los Delitos Informáticos, no estatuye que juez será competente para conocer del mismo.

Ahora bien, a excepción del Estado de Sinaloa, los Delitos Informáticos pueden sancionarse penalmente (por vía Jurisdiccional), ya que el Código Penal de este Estado, los estatuye al igual que sus diferentes modalidades.

Título Décimo
"Delitos contra el patrimonio"

Capítulo V
Delito Informático.

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

I. Use o entre a una base de datos, 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

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

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días *multa*".[104]

No obstante ello, las sanciones establecidas son mínimas, toda vez que pueden cometerse "Fraudes Informáticos" muy cuantiosos o grandes "Daños Patrimoniales", luego entonces, la sanción debe ir acorde a los daños causados. Y por cuanto hace a las modalidades de los "Delitos Informáticos", son muy limitativas, ya que en el ámbito internacional, las actividades ilícitas respecto a este delito son abundantes y complejas.

[104] http://tiny.uasnet.mx/prof/cln/der/silvia/cppps.htm

6.9. LOS JUECES FEDERALES PENALES

Ahora cabe preguntar ¿Qué juez será el competente para conocer los asuntos relativos a los Delitos Informáticos, en México?.

La Ley Orgánica Del Poder Judicial De La Federación, publicada en el Diario Oficial de la Federación el 26 de mayo de 1995 (En vigor a partir del 27 de mayo del mismo año), establece lo siguiente:

TITULO PRIMERO
DEL PODER JUDICIAL DE LA FEDERACION

CAPITULO UNICO
DE LOS ORGANOS DEL PODER JUDICIAL DE LA FEDERACION

Artículo 1. El poder judicial de la federación se ejerce por:

I. La suprema corte de justicia de la nación;
II.- El tribunal electoral;
III. Los tribunales colegiados de circuito;
IV. Los tribunales unitarios de circuito;
V. Los juzgados de distrito;
VI. El consejo de la judicatura federal;
VII. El jurado federal de ciudadanos, y
VIII. Los tribunales de los estados y el distrito federal en los casos previstos por el Artículo 107, fracción XII, de la constitución política de los estados unidos mexicanos y en los demás en que, por disposición de la ley deban actuar en auxilio de la justicia federal.

TITULO CUARTO
DE LOS JUZGADOS DE DISTRITO

CAPITULO II
DE SUS ATRIBUCIONES

Artículo 50. Los jueces federales penales conocerán:

I. DE LOS DELITOS DEL ORDEN FEDERAL.
Son delitos del orden federal:

a) Los previstos en las leyes federales y ***en los tratados internacionales;***
b) Los señalados en los artículos 2. A 6. Del código penal para el distrito federal en materia común y para toda la república en materia federal;
c) Los cometidos en el extranjero por los agentes diplomáticos, personal oficial de las legaciones de la república y cónsules mexicanos;

d) Los cometidos en las embajadas y legaciones extranjeras;
e) Aquellos en que la federación sea sujeto pasivo;
f) Los cometidos por un servidor publico o empleado federal, en ejercicio de sus funciones o con motivo de ellas;
g) Los cometidos *en contra* de un servidor publico o empleado federal, en ejercicio de sus funciones o con motivo de ellas;
h) Los perpetrados con motivo del funcionamiento de un servicio publico federal, aunque dicho servicio este descentralizado o concesionado;
i) Los perpetrados en contra del funcionamiento de un servicio publico federal o en menoscabo de los bienes afectados a la satisfacción de dicho servicio, aunque este se encuentre descentralizado o concesionado;
j) Todos aquellos que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la federación;
k) Los señalados en el artículo 389 del código penal, cuando se prometa o se proporcione un trabajo en dependencia, organismo descentralizado o empresa de participación estatal del gobierno federal, y
l) Los cometidos por o en contra de funcionarios electorales federales o de funcionarios partidistas en los términos de la fracción *II del Artículo 401* del código penal;

II. DE LOS PROCEDIMIENTOS DE EXTRADICION, SALVO LO QUE SE DISPONGA EN LOS TRATADOS INTERNACIONALES.

III.- DE LAS AUTORIZACIONES PARA INTERVENIR CUALQUIER COMUNICACION PRIVADA.

(ADICIONADO, D.O.F. 7 DE NOVIEMBRE DE 1996)**Artículo 50-Bis.**- En materia federal, la autorización para intervenir las comunicaciones privadas, será otorgada de conformidad con la ley federal en materia de delincuencia organizada.

(ADICIONADO, D.O.F. 7 DE NOVIEMBRE DE 1996)**Artículo 50-Ter.**- Cuando la solicitud de autorización de intervención de comunicaciones privadas, sea formulada en los términos previstos en las legislaciones locales, por el titular del ministerio publico de alguna entidad federativa, exclusivamente se concederá si se trata de los delitos de homicidio, asalto en carreteras o caminos, robo de vehículos, privación ilegal de la libertad o secuestro y trafico de menores, todos ellos previstos en el código penal para el *distrito federal en materia* de fuero común y para toda la república en materia de fuero federal, o sus equivalentes en las legislaciones penales locales.

La autorización se otorgara únicamente al titular del ministerio publico de la entidad federativa, cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de los delitos arriba señalados. El titular del ministerio publico será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la fundan, el razonamiento

por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevaran a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención,

Incluyendo sus prorrogas, pueda exceder de *seis meses*. Después de dicho plazo, solo podrán autorizarse nuevas intervenciones cuando el titular del ministerio publico de la entidad federativa acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinara las características de la intervención, sus modalidades y limites y, en su caso, ordenara a instituciones publicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la *misma* practica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenara que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio o video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo *sin* que ello suceda, el juez que autorizo la intervención ordenara que se pongan a su disposición las cintas resultado de las intervenciones, los originales y sus copias y ordenara su destrucción en presencia del titular del ministerio publico de la entidad federativa.[105]

En resumen, ***La Ley Orgánica del Poder Judicial de la Federación***, no establece concretamente que juez o tribunal será competente para conocer de los Delitos Informáticos, sin embargo, los artículos anteriores dan cabida a que si los delitos informáticos se tipificaran a nivel federal, (como debería de ser) los tribunales *competentes serían los jueces* federales penales (Art. 1 frac. V. y el Art. 50 de la L.O.P.J.F.).

Concretamente, el Artículo 1 dispone qué el Poder Judicial de la Federación se ejerce (fracción V.) por "los juzgados de distrito", en íntima relación el artículo 50 estatuye qué los jueces federales penales conocerán:

[105] http://info1.juridicas.unam.mx/legfed/171/

I. De los delitos del orden federal. Son delitos del orden federal:
a) Los previstos en las leyes federales y en los tratados internacionales;
e) Aquellos en que la federación sea sujeto pasivo;
j) Todos aquellos que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la federación; Entre otras disposiciones.

Por cuanto hace al artículo 50 fracciones *II* y *III*, también las consideramos importantes, ya que los jueces federales penales conocerán de los procedimientos de extradición, salvo lo que se disponga en los tratados internacionales y de las autorizaciones para intervenir cualquier comunicación privada.

El artículo 50. Ter. Establece las formalidades y condiciones para intervenir cualquier comunicación privada, lo cual es indispensable para la obtención de pruebas en Internet, en tratándose de los Delitos Informáticos, como veremos más adelante.

6.10. EL MINISTERIO PÚBLICO FEDERAL

Como consecuencia de lo anterior, al tipificarse los Delitos Informáticos a Nivel Federal, *corresponderia* la intervención del Ministerio Público Federal, para la representación del interés social con el ejercicio de la acción penal, y la persecución de los probables autores de los delitos.

A continuación transcribimos los artículos de La ley orgánica de la procuraduría general de la república, que tienen o podrían tener íntima relación con los Delitos Informáticos (una vez tipificados) y que establecen las atribuciones del Ministerio Público Federal.

La Ley Orgánica De La Procuraduría General De La República. (Publicada en el D.O.F. el 10 de mayo de 1996). Ultima reforma D.O.F. del 7 de noviembre de 1996.

CAPITULO I
ATRIBUCIONES

Artículo 2.- Corresponde al ministerio publico de la federación:

I. Vigilar la observancia de la constitucionalidad y legalidad en el ámbito de su competencia, sin perjuicio de las atribuciones que legalmente correspondan a otras autoridades jurisdiccionales o administrativas;
II. Promover la pronta, expedita y debida procuración e impartición de justicia;
III. Velar por el respeto de los derechos humanos en la esfera de su competencia;
IV. Intervenir ante las autoridades judiciales en todos los negocios en que la federación sea parte, cuando se afecten sus intereses patrimoniales o tenga interés

jurídico, así como en los casos de los diplomáticos y los cónsules generales;

V. Perseguir los delitos del orden federal;
VI. Intervenir en el sistema nacional de planeación democrática, en lo que hace a las materias de su competencia;
VII. Participar en el sistema nacional de seguridad publica de conformidad con lo establecido en la ley general que establece las bases de coordinación del sistema nacional de seguridad publica, este ordenamiento y demás disposiciones aplicables;
VIII. Dar cumplimiento a las leyes así como a los tratados y acuerdos internacionales en los que se prevea la intervención del gobierno federal en asuntos concernientes a las atribuciones de la institución y con la intervención que, en su caso, corresponda a las dependencias de la administración publica Federal;
IX. Representar al gobierno federal en la celebración de convenios de colaboración a que se refiere el Artículo 119 de la constitución política de los estados unidos mexicanos;
X. Convenir con las autoridades competentes de las entidades federativas sobre materias del ámbito de su competencia; y
XI. Las demás que las leyes determinen.

Artículo 8.- La persecución de los delitos del orden federal a que se refiere la fracción v del Artículo 2. de esta ley, comprende:

I. En la averiguación previa:
a) Recibir denuncias o querellas sobre acciones u omisiones que puedan constituir un delito;
b) Investigar los delitos del orden federal con la ayuda de los auxiliares a que se refiere el Artículo 19 de esta ley, y otras autoridades, tanto federales como de las entidades federativas, en los términos de los convenios de colaboración;
c) Practicar las diligencias necesarias para la acreditación de los elementos del tipo penal del delito y la probable responsabilidad del indiciado, así como para la reparación de los daños y perjuicios causados;
d) Ordenar la detención y, en su caso, retener a los probables responsables de la comisión de delitos, en los términos previstos por el Artículo 16 de la constitución política de los estados unidos mexicanos;
e) Realizar el aseguramiento y tramitación del destino de los instrumentos, objetos y productos del delito, en los términos de los artículos 40, 41 y 193 del código penal para el distrito federal en materia de fuero común y para toda la república en materia de fuero federal, y demás disposiciones legales y reglamentarias aplicables;
f) Restituir provisionalmente al ofendido en el goce de sus derechos, en los términos del código federal de procedimientos penales;
g) Conceder la libertad provisional a los indiciados, en los términos previstos por la fracción I y el penúltimo párrafo del Artículo 20 de la constitución política de los estados unidos mexicanos,
h) Solicitar al órgano jurisdiccional las ordenes de cateo, las medidas precautorias de arraigo. el aseguramiento o el embargo precautorio de bienes,

que resulten indispensables para los fines de la averiguación previa, así como. en su caso, y oportunidad, para el debido cumplimiento de la sentencia que se dicte. Al ejercitar la acción, el ministerio publico de la federación formulara a la autoridad jurisdiccional los pedimentos que legalmente correspondan;

i) En aquellos casos en que la ley lo permita. el ministerio publico de la federación propiciara conciliar los intereses en conflicto, proponiendo vías de solución que logren la avenencia;

j) Determinar el no ejercicio de la acción penal, cuando:

1. Los hechos de que conozca no sean constitutivos de delito;

2. Una vez agotadas todas las diligencias y los medios de prueba correspondientes, no se acredite la probable responsabilidad del indiciado:

3. La acción penal se hubiese extinguido en los términos de las normas aplicables;

4. De las diligencias practicadas se desprenda plenamente la existencia de una causa de exclusión del delito, en los términos que establecen las normas aplicables;

5. Resulte imposible la prueba de la existencia de los hechos constitutivos de delito, por obstáculo material insuperable; y

6. En los demás casos que determinen las normas aplicables;

k) Poder a disposición del consejo de menores, a los menores de edad que hubieren cometido infracciones correspondientes a ilícitos tipificados por las leyes penales federales;

l) Poner a los inimputables mayores de edad, a disposición del órgano jurisdiccional, cuando se deban aplicar medidas. de seguridad, ejercitando las acciones correspondientes, en los términos establecidos en las normas aplicables; y

m) Las demás que determinen las normas aplicables. Cuando el ministerio publico de la, federación tenga conocimiento por si o por conducto de sus auxiliares, de la probable comisión de un delito cuya persecución dependa de querella o de cualquier otro acto equivalente, que deba formular alguna autoridad, lo comunicara por escrito y de inmediato a la autoridad legitimada para presentar la querella o cumplir el requisito equivalente, a fin de que resuelva con el debido conocimiento de los hechos lo que a sus facultades o atribuciones corresponda. las autoridades harán saber por escrito al ministerio publico de la federación la determinación que adopten.

II. Ante los órganos jurisdiccionales:

a) Ejercer la acción penal ante el órgano jurisdiccional competente por los delitos del orden federal cuando exista denuncia, acusación o querella, estén acreditados los elementos del tipo penal del delito de que se trate y la probable responsabilidad de quien o quienes en el hubieren intervenido, solicitando las ordenes de aprehensión o de comparecencia, en su caso;

b) Solicitar al órgano jurisdiccional las ordenes de cateo, las medidas precautorias de arraigo, de aseguramiento o embargo precautorio de bienes, los exhortos, o la constitución de garantías para los efectos de la reparación de los daños y perjuicios, salvo que el inculpado los hubiese garantizado previamente;

c) Poner a disposición de la autoridad judicial, a las personas detenidas y

aprehendidas, dentro de los plazos establecidos por la ley;
d) Aportar las pruebas y promover las diligencias conducentes para la debida comprobación de la existencia del delito, las circunstancias en que hubiese sido cometido y las peculiares del inculpado, de la responsabilidad penal de la existencia de los daños y perjuicios así como para la fijación del monto de su reparación;
e) Formular las conclusiones, en los términos señalados por la ley, y solicitar la imposición de las penas y medidas de seguridad que correspondan y el pago de la reparación de los daños y perjuicios o, en su caso, plantear las causas de exclusión del delito o las que extinguen la acción penal;
f) Impugnar en los términos previstos por la ley, las resoluciones judiciales; y
g) En general, promover lo conducente al desarrollo de los procesos y realizar las demás atribuciones que le señalen las normas aplicables,

III. En materia de atención a la víctima o el ofendido por algún delito:

a) Proporcionar asesoría jurídica así como propiciar su eficaz coadyuvancia en los procesos penales;
b) Promover que se garantice y haga efectiva la reparación de los daños y perjuicios; y
c) Concertar acciones con instituciones de asistencia medica y social, publicas y privadas, para los efectos del último párrafo del Artículo 20 de la constitución política de los estados unidos mexicanos; y

IV. Las demás que prevean otras disposiciones aplicables.

Artículo 11.- La atribución que se contiene en el artículo 2 fracción VIII de esta ley, comprende:

I. La formulación y presentación de las propuestas de los instrumentos de alcance internacional, a que se refiere el Artículo 4, fracción VIII de este ordenamiento;
II. La intervención en la extradición internacional de indiciados, procesados y sentenciados, así como en la aplicación de los tratados celebrados conforme al ultimo párrafo del Artículo 18 de la constitución política de los estados unidos Mexicanos, en los términos que dispongan las leyes e instrumentos jurídicos aplicables; y
III. La intervención en el cumplimiento de otras disposiciones de carácter o con alcance internacional, cuando se relacionen con la competencia de la institución. Cualquier apoyo o colaboración para la ejecución de programas derivados de instrumentos de carácter o con alcance internacional que involucren asuntos de la competencia de la institución, se entiende con reserva sobre evaluaciones o medidas que excedan la naturaleza de los programas, otorguen autoridad a personas o entidades extranjeras en territorio mexicano, o involucren consecuencias sobre materias ajenas al ámbito especifico que cubre el programa respectivo. Esta reserva se consignara en los instrumentos que fijen las bases de dichos programas de conformidad con lo que establece la ley sobre la celebración de tratados.

Artículo 12.- La atribución a que se refiere el Artículo 2 fracción X de esta ley, comprende:
I. La promoción y celebración de convenios con las entidades federativas, con apego a las disposiciones aplicables, y sin perjuicio de las facultades de otras autoridades, sobre apoyo y asesoría recíprocos en materia policial técnica, jurídica, pericial y de formación de personal para la procuración de justicia; y II. La promoción y celebración de acuerdos con arreglo a las disposiciones aplicables para efectos de auxilio al ministerio público de la federación por parte de autoridades locales, cuando se trate de funciones auxiliares previstas en esta ley o en otros ordenamientos.

Artículo 13.- En el cumplimiento de sus atribuciones, el ministerio público de la federación y sus auxiliares en su caso, y conforme a sus funciones, podrán requerir informes, documentos, opiniones y elementos de prueba en general a las dependencias y entidades de la administración pública federal, a las correspondientes al distrito federal, y a otras autoridades y personas que puedan suministrar elementos para el debido ejercicio de dichas atribuciones. Es obligatorio proporcionar los informes que solicite el ministerio público de la federación y que se realicen con las formalidades de la ley; en caso de incumplimiento, la autoridad correspondiente incurrirá en responsabilidad en los términos de la legislación aplicable.[106]

Tales artículos tendrían aplicación y gran relevancia para llevar a cabo el ejercicio de la acción penal satisfactoriamente e imputar la responsabilidad correspondiente al infractor de la norma.

Cabe señalar que muchos de los sujetos activos de los Delitos Informáticos son menores de edad, jóvenes extranjeros que se infiltran a los sistemas operativos de seguridad de empresas gubernamentales o no gubernamentales y se apoderan de información oficial o confidencial o en su caso, la mutilan, modifican o destruyen, creando daños y perjuicios a su propietario o poseedor.

Ante ello, es necesario reformar nuestras leyes penales, disminuyendo la edad de los infractores o indiciados para poder ser sentenciados a partir de los 15 o 16 años (tanto para mexicanos como para extranjeros), ya que algunos alcanzan tal grado de madures psicológica y otras veces también física que es necesaria la misma. Tomando en cuenta que en países avanzados como Estados Unidos, Alemania, Francia, Japón entre otros, la tecnología a alcanzado niveles altos y el desarrollo mental y cultural de los jóvenes es distinto al de nuestro país.

[106] http://info1.juridicas.unam.mx/legfed/152/

PROPUESTA

Toda vez que las acciones ilícitas cometidas por el mal uso o manejo de las computadoras, son muy complejas y a la vez múltiples, es menester particularizar lo mas posible tales conductas delictivas, para que el juzgador al momento de aplicar la ley no aplique equivocadamente otros tipos penales; es decir, no podemos elaborar tipos penales genéricos o que abarquen varias conductas ilícitas, sino, mas bien tenemos que estatuir cada una de las acciones delictivas y enlazarlas a una sanción dependiendo del daño físico (económico) y/o moral y demás bienes jurídicos vulnerados.

Por ello, consideramos pertinente la elaboración de un Título Especial, dentro del Capítulo del Patrimonio de las personas, en el Código Penal Federal, quedando de la siguiente manera:

Título Vigésimo Segundo
"Delitos en Contra de las Personas en su Patrimonio"

Capítulo Especial
De los Delitos Informáticos

Artículo xxx.- Comete delito informático, y se sancionará con la pena respectiva, la persona que cometa una o mas de las siguientes acciones:

I.- Al que acceda o se mantenga en un sistema de elaboración de datos o cualquier red de información, sin consentimiento de quien deba otorgarlo, independientemente de causar daños o perjuicios a terceros y se sancionará con pena de prisión de tres a seis meses y multa de 30 a 50 salarios mínimos.

II.- Al que con dolo introduzca datos falsos, información o virus informáticos, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas y se sancionará con pena de prisión de uno a siete años y multa de 100 a 3000 salarios mínimos.

III.- Al que falsifique datos o información respecto a soportes o documentos electrónicos que deban presentarse como prueba en un juicio, se sancionará con pena de prisión de seis meses a cinco años y multa de 100 a 450 salarios mínimos.

IV.- Al que utilice, transmita, reproduzca, o distribuya un programa de computo protegido por derecho de autor, sin consentimiento de su propietario, a través de Internet o cualquier otra red, se sancionará de uno a tres años de prisión y multa de 100 a 800 salarios mínimos.

V.- Al que, sin estar autorizado, intercepte correos electrónicos o acceda a ellos, se apodere, utilice o modifique, en perjuicio de terceros, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, se sancionará de seis a dos años de prisión y multa de 50 a 300 salarios mínimos.

VI.- El que, para descubrir los secretos comerciales o vulnerar la intimidad de otros, sin su consentimiento, se apodere o intercepte mensajes de correo electrónico y/o sus telecomunicaciones o utilice artificio técnico de escucha, transmisión o grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicaciones, será castigado con las penas de prisión de uno a cuatro años y multa de 100 a 1500 salarios mínimos

VII.- Al que ofrezca o publique material pornográfico accesible a menores de 18 años de edad, se sancionara de seis meses a dos años de prisión y multa de 100 a 800 salarios mínimos.

VIII,- Al que difunda publicidad falsa u ofrezca productos o servicios ficticios a través de Internet o cualquier otra red y que cause daños y perjuicios a terceros, se sancionará de seis a tres años de prisión y multa de 100 a 1200 salarios mínimos.

IX.- Al que cause daños y perjuicios a terceros a través de mensajes o publicación de injurias o calumnias, vía Internet o cualquier otra red o simplemente publique información personal sin autorización de quien deba darla, se sancionará de seis a tres años de prisión y multa de 100 a 800 salarios mínimos.

X.- Al que reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, y se sancionará de seis meses a cinco años de prisión y multa de 100 a 1500 salarios mínimos.

Todas las multas serán independientes de los daños y perjuicios que se causen a la víctima y se nos adherimos a la propuesta hecha por el Dr. Ernesto Zedillo Ponce de León, respecto a la suma o acumulación de sanciones para la compurgación de dos o mas delitos.

SECCIÓN DE ANEXOS

MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA.

ANEXO I.- Foro de consulta sobre derecho e informática del 18 de septiembre al 4 de octubre de 1996. Convocatoria.

ANEXO II.- Relatoria del primer evento del foro de consulta sobre derecho de informática. Ciudad de Veracruz, Ver., 18 de Septiembre de 1996.

ANEXO III.- Relatoria del segundo evento del foro de consulta sobre derecho de informática. Ciudad de Guadalajara, Jal., 20 de Septiembre de 1996.

ANEXO IV.- Relatoria del tercer evento del foro de consulta sobre derecho de informática. Ciudad de Monterrey, N.L., 25 de Septiembre de 1996.

ANEXO V.- Relatoria del cuarto evento del foro de consulta sobre derecho de informática. Ciudad de Tijuana, B.C., 27 de Septiembre de 1996.

ANEXO VI.- Relatoria del quinto evento del foro de consulta sobre derecho de informática. Ciudad de México, D.F., 4 de Octubre de 1996..

ANEXO VII.- Ley de extradición internacional.

Foro de Consulta Sobre Derecho e Informática del 18 de septiembre al 4 de Octubre de 1996.

Convocatoria

Considerando:

Que el Plan Nacional de Desarrollo 1995-2000 destaca que en materia de informática, la acción del Gobierno Federal se orientará a impulsar la generación, difusión y aplicación de las innovaciones tecnológicas, su aprovechamiento en todos los sectores, así como la promoción de mecanismos para asegurar la coordinación, promoción, seguimiento y evaluación de las actividades relativas a la tecnología de la información en el ámbito nacional.

Que para tal efecto, en dicho Programa se determina dentro de las líneas de acción, instancias de coordinación para el análisis y adecuaciones de la normatividad en la materia, con la finalidad de sustentar la evolución y el uso de la informática, acorde a las necesidades del país, y

Que de acuerdo con lo anterior, el Programa de Desarrollo Informático 1995-2000 establece dentro de sus objetivos el de contar con disposiciones jurídicas que aseguren las condiciones adecuadas para favorecer el aprovechamiento de la informática y el desarrollo de la infraestructura en la materia.

Que la evolución de las tecnologías inherentes a la informática, ha propiciado que su uso adquiera un carácter estratégico, para elevar los niveles de bienestar de los individuos y para mejorar la competitividad y productividad de las naciones.

La Cámara de Diputados del H. Congreso de la Unión y el Instituto Nacional de Estadística, Geografía e Informática Convocan al Foro de Consulta sobre Derecho e Informática

A especialistas, académicos e investigadores, legisladores, instituciones educativas públicas y privadas, servidores públicos, trabajadores, empresarios y demás personas interesadas en participar con sus opiniones, propuestas y experiencias, en torno al marco jurídico administrativo relacionado con la informática, conforme a las siguientes:

B a s e s :

Primera. Los trabajos del Foro sobre Derecho e Informática, se realizarán del 18 de septiembre al 4 de octubre del presente año. Su organización y desarrollo estará a cargo del Comité de Biblioteca e Informática de la Cámara de Diputados y del Instituto Nacional de Estadística, Geografía e Informática.

Segunda. Para la realización del Foro de Consulta, se llevarán a cabo 5 reuniones en las sedes, fechas, y temas siguientes:

1. Veracruz, Ver., el miércoles 18 de septiembre, con los temas:
Derechos de los ciudadanos a la confidencialidad de información personal, almacenada en bases de datos públicos y privados. Protección jurídica de datos de carácter estratégico o confidencial, producidos por el sector público y privado.

2. Guadalajara, Jal., el viernes 20 de septiembre, con los temas:
Tipificación de delitos cometidos con el uso de herramientas informáticas que lesionan patrimonios y derechos de personas físicas y morales (sabotaje, fraude, espionaje, etc.) Valor probatorio del documento electrónico en procesos administrativos y judiciales.

3.- Monterrey, N. L., el miércoles 25 de septiembre, con los temas:
Protección de los derechos de autor para desarrolladores de programas, así como de la información contenida en medios magnéticos y distribuida a través de redes de datos públicas. Protección de derechos de propiedad industrial.

4. Tijuana, B. C., el viernes 27 de septiembre, con los temas:
Mecanismos de fomento al desarrollo y uso de la informática. Condiciones adecuadas de competencia y servicio entre los proveedores de bienes y servicios informáticos.

5. Distrito Federal, el viernes 4 de octubre, con los temas:
Condiciones para la prestación se servicios telemáticos públicos y privados. Condiciones de acceso universales a la información y a la infraestructura tecnológica.

En esta última, se hará la integración y relatoría de las propuestas presentadas en las diferentes sedes, y se presentará las Conclusiones Generales del Foro.

Tercera. Los interesados en participar, para formular sus puntos de vista, comentarios y opiniones deberán inscribirse en el tema de su interés, sin que esto limite la posibilidad de expresarse en cualquiera de ellos. Asimismo, podrán participar con algún trabajo sobre dichos temas, los cuales deberán presentar en forma escrita diez días hábiles antes de la celebración de los foros, mismos que se constituirán de un diagnóstico, análisis y desarrollo del tema y propuesta legislativa de 10 cuartillas como mínimo y 15 como máximo, acompañado de un resumen ejecutivo con las conclusiones de su propuesta y su justificación, de no más de 5 cuartillas a doble espacio y, de ser posible, un archivo del mismo en disco flexible, en formato Word, así como un resumen curricular y sus datos personales.

Cuarta. Los trabajos registrados serán tomados en cuenta para el análisis correspondiente a cada tema, en los foros de las diversas sedes.

Quinta. Los trabajos se dirigirán al Comité de Biblioteca e Informática de la Cámara de Diputados; Av. Congreso de la Unión s/n, edificio "C" segundo piso, col. El Parque, C. P. 15969 México, D. F., o a la Dirección de Políticas y Normas en Informática del Instituto Nacional de Estadística, Geografía e Informática, Av. Patriotismo Núm. 711, Torre "A" Piso 10, col. San Juan Mixcoac, C. P. 03730 México, D. F. y en las oficinas de los Directores Regionales y Coordinadores Estatales del INEGI.

Sexta. Para cada reunión, la Comisión Organizadora formulará las invitaciones correspondientes y determinará los lugares específicos y horarios en que se efectuarán las reuniones.

Séptima. Los aspectos no previstos en esta convocatoria, serán resueltos por la Comisión Organizadora del Foro de Consulta Sobre Derechos e Informática.

Palacio Legislativo, 9 de agosto de 1996.
Informes e inscripciones:
México, D. F.:
(91) (5) 628 1316, 628 1383, 628 1318, 598 9997 y 598 6836; fax 522 1463, 522 4340 y 598 7738; correo electrónico seginf@dpni.inegi.gob.mx, lvc@info.cddhcu.gob.mx

Puebla, Pue.:
(91) (22) 32 29 51 y 32 09 68; fax 46 42 02

Jalapa, Ver.:
(91) (28) 18 18 83, 18 18 38, y 18 92 52; fax 18 15 00

Guadalajara, Jal.:
(91) (36) 13 43 02, 13 95 01 y 47 49 19; fax 58 39 69.

Zapopan, Jal.:
(91) (36) 47 29 72

Monterrey, N. L.:
(91) (83) 69 48 48, 69 48 49 y 69 48 28; fax 69 48 49

Hemosillo, Son.:
(91) (62) 16 19 85, 16 07 63 y 16 13 68; fax 16 07 63.

Tijuana, B. C.:
(91) (66) 21 04 64 y 85 67 86; fax 85 67 86.

MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA

Relatoria del Primer Evento del Foro de Consulta Sobre Derecho de Informática

En la ciudad de Monterrey, N.L., el 25 de septiembre de 1996 se realizó el tercer evento del Foro de Consulta sobre Derecho e Informática, organizado en forma conjunta por el Instituto Nacional de Estadística, Geografía e Informática y la H. Cámara de Diputados, con la finalidad de revisar el marco jurídico inherente a la informática.

En esta reunión asistieron aproximadamente 130 representantes de los sectores público, privado, académico, empresarial y de investigación.

La ceremonia de inauguración estuvo presidida por el Lic. Juan Francisco Rivera Bedoya, Secretario General de Gobierno, en representación del Lic. Benjamín Clarion Reyes Retana, Gobernador Constitucional del Estado de Nuevo León; el Dip. Gustavo Salinas Iñiguez, Secretario del Comité de Biblioteca e Informática de la H. Cámara de Diputados; el Dr. Alfredo Bustos y de la Tijera, Director General de Política Informática del INEGI; el Dip. Carlos Alejandro Ramírez Campos, Presidente del H. Congreso del Estado, la Lic. Alejandra Vela Salinas, Directora Regional Noreste del INEGI; la Lic. Ma. Teresa Herrera Tello, Presidenta del H. Tribunal Superior de Justicia; el Lic. Carlos H. Suárez Garza, Presidente del Colegio de Notarios; Dip. Raúl Livas Vera, Secretario de la Comisión de Programación y Presupuesto de la H. Cámara de Diputados y el Lic. Salvador Benítez Lozano, Presidente del Colegio de Abogados de Nuevo León, A.C.

Primeramente hizo uso de la palabra la Lic. Alejandra Vela Salinas, quien dio la bienvenida a los participantes, comentando la relevancia de la tecnología informática, cuya dinámica ha dejado a la zaga al Derecho. Por esta razón, en el Programa de Desarrollo Informático derivado el Plan Nacional de Desarrollo, se contempla de manera específica la necesidad de revisar las disposiciones jurídicas que tienen incidencia en el ámbito de la informática.

Al hacer uso de la palabra el Dip. Gustavo Salinas Iñiguez, señaló que este Foro representa un ejercicio de reflexión y análisis de la Informática vinculada con el Derecho, que la irrupción de la informática permite realizar más y mejores actividades y que sin ésta no podría concebirse la globalización en que vivimos.

Que esta tecnología ha permitido un acceso más ágil a la información lo que permite la realización de actividades de una manera más eficiente.

Indicó, que el propósito de este Foro, es el de recoger las inquietudes de la comunidad con la finalidad de llegar a un proyecto legislativo acorde a las necesidades de protección que permitan apoyar su adecuado desarrollo.

Mencionó los temas tratados en los eventos de Veracruz y Guadalajara, así como los que habrán de desarrollarse en las reuniones que se realizarán en Tijuana, B. C., y México, D.F.

A continuación el Lic. Juan Francisco Rivera Bedoya, hizo referencia al compromiso del gobierno federal, de proporcionar a la población información que le permita realizar con mejores elementos el desarrollo de sus actividades. Señaló, que en este proceso el INEGI realiza las actividades necesarias para la divulgación de la información y resaltó el apoyo que la informática representa para el cumplimiento del compromiso señalado.

Al concluir su intervención, procedió a realizar la declaratoria inaugural en representación del C. Gobernador del Estado de Nuevo León.

Los trabajos de la reunión dieron inicio con la participación del Dr. Alfredo Bustos y de la Tijera, quien se refirió al impacto de la tecnología informática cuya evolución hace necesaria la revisión de temas relativos a la aplicación del derecho y su relación con esta tecnología.

Lo anterior derivado de la consulta popular que para la integración del Plan Nacional de Desarrollo se llevó a cabo y en la que se pudo identificar la incidencia de la informática en las diferentes actividades de la sociedad, a partir de lo cual se integró el Programa de Desarrollo Informático, que plantea como objetivo general el de promover el adecuado uso y aprovechamiento de la informática en los diferentes sectores del país. Señaló que para tal efecto este Programa contempla como una de sus acciones la de revisar y adecuar el marco jurídico aplicable.

Posteriormente, hizo referencia a los objetivos y fases del Foro, presentando los antecedentes y conclusiones respecto de los temas que se abordaron en Boca del Río, Ver., y en la ciudad de Guadalajara, Jal., así como de los que se trataron en la ciudad de Monterrey.

Los temas que se abordaron en este evento giraron en torno a la protección de los derechos de autor para desarrolladores de programas, así como de la información contenida en medios magnéticos y distribuida a través de redes de datos públicas, y sobre de la protección de derechos de propiedad industrial.

La sesión de conferencia inició con la participación de la Ing. Mayra Rivero de la Asociación Latinoamericana de Profesionales de Seguridad en Informática, quien comentó la necesidad de que en la Ley Federal de Derechos de Autor, y en su caso, la de Propiedad Industrial, se precisen condiciones de protección a desarrolladores de programas de cómputo, que permitan garantizar los derechos de titularidad y propiedad de su autor, debiéndose buscar congruencia con la protección que en la materia se da en las convenciones internacionales.

Respecto a la protección de los derechos de autor de la información distribuida a través de redes de datos públicas, indicó que la promoción de innovación tecnológica, debe perseguir el avance de producción y servicios de conocimiento tecnológico, tanto para el emisor como para el

receptor y de manera conducente para el bienestar social y económico que permita un balance de derechos y obligaciones.

Posteriormente, el Ing. Fernando Román Contreras de Internet Place, S.A. de C.V., presentó el tema "Propiedad Intelectual y Generación de Nueva Tecnología", señalando que la protección jurídica de la innovación y la inventiva ha sido una preocupación constante de las personas, empresas y países, y que el análisis del problema presenta aristas que dificultan el consenso en la creación de mecanismos de solución.

Indicó, que mientras para algunos el "caldo de cultivo" que fomenta la actividad creadora, motivando la innovación y la generación de nuevas tecnologías está fuertemente soportada por el derecho de autor, las patentes y las marcas registradas, generando desarrollo económico y bienestar social, para otros son un medio para aumentar las ventajas comerciales de los poseedores de la tecnología por sobre los que están en vías de desarrollo de sus propias tecnologías.

Comentó sobre la dificultad de identificar la línea que divide la actividad creativa y la generación de conocimiento nuevo, de la simple variación de tecnología existente, que la necesidad de utilizar tecnología competitiva y la falta de recursos económicos para comprarla afectan no solo a los negocios, sino también limitan principalmente el alcance de universidades, gobiernos, programas de salud y centros de investigación.

Asimismo, comentó que la competencia desleal y la creación de monopolios tecnológicos son en una más avanzada etapa consecuencias de una normatividad o legislación inadecuada, cuya solución no sólo se debe imponer a través de éstas, sino que también deben existir programas que promuevan la conciencia en los usuarios y en los propietarios de tecnología respecto a sus costos y compromiso social como elementos que permitan facilitar su acceso y desarrollo.

ANALISIS Y REFLEXIÓN

A continuación, el panel de especialistas así como el auditorio emitieron diversos comentarios, los cuales giraron en torno a los siguientes temas:

- La importancia del procedimiento de registro de programas de cómputo.
- Titularidad de derechos de los desarrollos que realizan personas físicas que laboran en empresas o instituciones.
- Responsabilidad de los empleados del uso de software ilegal en la empresa o institución en la que laboran.
- Definición de términos jurídicos y técnicos para la solución de conflictos derivados del uso ilegal de programas de cómputo.
- La posible protección de los programas de cómputo en el contexto de la Ley de Propiedad Industrial.

- Responsabilidad de la veracidad de información contenida en bases de datos públicas.
- Definición de contratos de bienes y servicios informáticos.

CONCLUSIONES

Entre las conclusiones preliminares que se alcanzaron en este tercer evento, destacan:

- Proteger los derechos de propiedad tecnológica para estimular la actividad creadora.
- Crear programas que promuevan la conciencia en los usuarios sobre los costos de generación de tecnología, y de los propietarios de la misma en su compromiso social, con la finalidad de facilitar su acceso.
- Promover que exista congruencia de la legislación nacional respecto de la protección que en materia de derechos de autor está prevista en las leyes y convenciones internacionales.
- Simplificar el proceso para realizar auditorías a usuarios de programas de cómputo, para asegurar el cumplimiento de las leyes.
- Precisar el proceso para deslindar responsabilidades en caso de que se violen los derechos autorales protegidos por la ley.
- Promover la emisión de disposiciones que agilicen los procesos jurídicos.
- Definir los términos jurídicos que deben considerarse para su aplicación en litigios derivados de la violación a los derechos autorales.
- Promover la realización de cursos en cuanto a la aplicación y alcance del Derecho de Autor.
- Promover la cultura en las universidades para el apoyo de leyes.
- Actualizar la constitución acorde a las necesidades del país y disposiciones reglamentaria.
- Promover la creación de leyes claras, precisas y oportunas.
- Creación de tribunales especiales en la materia a nivel regional.
- Partir de la Ley Federal de Derechos de Autor vigente y enriquecerla con un capítulo específico.
- Definir los problemas que sustenten los procesos legislativos.

MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA

Relatoria del Segundo Evento del Foro de Consulta Sobre Derecho de Informática.

En la ciudad de Boca del Río, Ver., el 18 de septiembre de 1996 se realizó el primer evento del Foro de Consulta sobre Derecho e Informática, organizado en forma conjunta por el Instituto Nacional de Estadística, Geografía e Informática y la H. Cámara de Diputados, con la finalidad de revisar el marco jurídico inherente a la informática.

En esta reunión asistieron aproximadamente 100 representantes de los sectores público, privado, académico, empresarial y de investigación.

El acto inaugural estuvo presidido por el Lic. Francisco Loyo Ramos, Subsecretario de Gobierno en representación del Lic. Patricio Chirinos Calero, Gobernador Constitucional del Estado de Veracruz; el Dip. Eurgenio Ortiz Walls, Presidente del Comité de Biblioteca e Informática de la H. Cámara de Diputados; Dr. Carlos M. Jarque, Presidente del Instituto Nacional de Estadística, Geografía e Informática: el Dip. Gustavo Salinas Iñiguez, Secretario del Comité de Biblioteca e informática de la H. Cámara de Diputados: el Lic. Ubaldo Flores Alpizar, Presidente Municipal de Boca del Río, Ver., el Lic. Raúl Pimentel Murrieta, en representación del Presidente del H. Tribunal Superior de Justicia del Estado de Veracruz, el Dip. Oswaldo Cházaro, en representación del Presidente del H. Congreso del Estado de Veracruz y el Dr. Alfredo Bustos y de la Tijera, Director General de Política Informática del INEGI.

A continuacion el Dip. Eugenio Ortiz Walls en su intervención comentó que el lenguaje y la norma son herramientas fundamentales en la vida del hombre, que la ley y la comunicación inciden en la vida social, lo que reclama cada vez más una puntual, amplia y diversificada información. También señaló, que el avance en las tecnologías de la información en la sociedad, requiere considerar no sólo aspectos cuantitativos si no cualitativos, que permitan acceder a respuestas puntuales y adecuadas, destacando que este Foro es la oportunidad propicia para reflexionar, profundizar y proponer los tiempos y formas que deben dar cuerpo a la singular relación del derecho y la informática.

El Dr. Carlos M. Jarque, por su parte, comentó entre otros aspectos el carácter estratégico de la informática y la importancia de analizar y reflexionar respecto al marco jurídico relativo al uso y desarrollo de esta tecnología, con la finalidad de contar con disposiciones que aseguren las condiciones requeridas para su mejor aprovechamiento.

En este evento se abordaron diversos aspectos relacionados con los derechos de los ciudadanos a la confidencialidad de información personal almacenada en bases de datos públicos y privados, así como de la protección jurídica de datos producidos por el sector público y privado.

Se inició la sesión con una conferencia sobre Derecho a la confidencialidad de la información personal almacenada en bases de datos públicas y privadas y protección jurídica de

Posteriormente, el Ing. Armando Arteaga King, procedió a declarar formalmente inaugurados los trabajos de esta reunión, en representación C. Gobernador Constitucional del Estado de Baja California.

Para iniciar los trabajos el Dr. Alfredo Bustos y de la Tijera, hizo uso de la palabra, comentando sobre el impacto de las tecnologías de información, a través de las cuales se tiene la posibilidad de consultar información de una manera más amplia, lo cual ha contribuido en forma decisiva en todas las actividades del país.

Comentó, que el Plan Nacional de Desarrollo señala en forma explícita las directrices para promover el desarrollo de las tecnologías de la información en nuestro país, a partir de lo cual se integró el Programa de Desarrollo Informático, que plantea como objetivo general el de promover el adecuado uso y aprovechamiento de la informática en los diferentes sectores del país. Señaló que para tal efecto este Programa contempla como una de sus acciones la de revisar y adecuar el marco jurídico aplicable.

Posteriormente, hizo referencia a los objetivos y fases del Foro, presentando los antecedentes y conclusiones respecto de los temas que se abordaron en Boca del Río, Ver., en Guadalajara, Jal., y en Monterrey, N.L., así como de los que se trataron en la ciudad de Tijuana.

Los temas que se abordaron en este evento giraron en torno a los mecanismos de fomento al desarrollo y uso de la informática, así como a las condiciones adecuadas de competencia y servicio entre los proveedores de bienes y servicios informáticos.

La sesión de conferencias inició con la presentación del Dr. Macedonio Alanís sobre el resumen ejecutivo de la conferencia presentada por la Asociación Latinoamericana de Profesionales en Seguridad Informática, que expone que para estar en posibilidad de ser competitivos en el mundo de los negocios y de las actividades productivas, se requiere de nuevos elementos de manejo de información, como parte de la operación y estrategias de las administraciones, para lo cual se requiere la definición de una serie de políticas.

Señala, que estas políticas deberán estar enmarcadas en la política general de gobierno, con objetivos específicos orientados al aprovechamiento de las tecnologías de la información, como factor estratégico, para producir mejores niveles de bienestar de la población y competitividad del país.

Asimismo, se resaltó la importancia de fomentar las actividades empresariales para desarrollar la competencia, como la mejor forma de luchar contra los monopolios, y que a su vez permita a los proveedores ofrecer mejores condiciones de oferta, en beneficio de las actividades de las organizaciones, dentro de un marco de referencia cliente-proveedor, mutuamente aceptable.

ANALISIS Y REFLEXIÓN

A continuación, el panel de especialistas así como el auditorio emitieron diversos comentarios, los cuales giraron en torno a los siguientes temas:

- Competitividad de empresas en el mercado informático.
- Apoyos para el desarrollo de proyectos informáticos y mecanismos de evaluación.
- Mecanismos para promover y fomentar el desarrollo de empresas de bienes y servicios informáticos.
- Instancias de evaluación de calidad de empresas de bienes y servicios informáticos.
- Situación de las empresas desarrolladoras de software en el marco de la ley de competencia económica.
- Programas de estudios de la licenciatura en derecho que incluyen conceptos informáticos.

CONCLUSIONES

Entre las conclusiones preliminares que se alcanzaron en este cuarto evento, destacan:

- Buscar el equilibrio legal que salvaguarde tanto los derechos de los productores de bienes y servicios informáticos como de los usuarios de estos.
- Que el gobierno fomente el mercado informático mediante la presentación de sus necesidades a la industria, licitando soluciones que posteriormente podrían ser utilizadas en el sector privado con sus correspondientes utilidades y creación de nuevas fuentes de trabajo.
- Definir mecanismos que evalúen y validen el potencial y riesgo de proyectos informáticos.
- Definir instancias que validen la calidad de empresas proveedoras de bienes y servicios informáticos.
- Que se promueva la certificación de empresas de bienes y servicios informáticos.
- Promover mecanismos que regulen el comercio electrónico para que tenga mayor seguridad en las transacciones que se hacen por este medio.
- Promover en las universidades la conciencia de lo que implica la ética profesional.

MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA

Relatoria del Cuarto Evento del Foro de Consulta Sobre Derecho de Informática.

En la ciudad de Guadalajara, Jal., el 20 de septiembre de 1996 se realizó el segundo evento del Foro de Consulta sobre Derecho e Informática, organizado en forma conjunta por el Instituto Nacional de Estadística, Geografía e Informática y la H. Cámara de Diputados, con la finalidad de revisar el marco jurídico inherente a la informática.

En esta reunión asistieron aproximadamente 120 representantes de los sectores público, privado, académico, empresarial y de investigación.

El acto inaugural estuvo presidido por el Lic. Francisco Javier Vizcaíno Gutiérrez, Director General de Planeación de la Secretaría de Promoción de Desarrollo Económico, en representación del Ing. Alberto Cárdenas Jiménez, Gobernador Constitucional del Estado de Jalisco; el Dip. Eurgenio Ortiz Walls, Presidente del de Biblioteca e Informática de la H. Cámara de Diputados; el Dip. Gustavo Salinas Iñiguez, Secretario del Comité de Biblioteca e Informática de la H. Cámara de Diputados; el Dr. Alfredo Bustos y de la Tijera, Director General de Política Informática del INEGI, el Lic. Pedro Rodríguez Villaseñor, Director Regional Occidente del INEGI y el Dip. Gildardo González Galindo, en representación del H. Congreso del Estado.

Al hacer uso de la palabra el Dip. Eugenio Ortiz Walls, señaló que el impacto de las tecnologías de la información nos llevan a pensar en profundos cambios políticos, económicos y sociales, en virtud de su fuerte presencia en las diferentes actividades del país.

Comentó que los temas que se expondrán en este evento representan la oportunidad propicia para reflexionar, profundizar y proponer los tiempos y formas que deben dar cuerpo a la singular relación del Derecho y la Informática.

A continuación el Lic. Francisco Javier Vizcaíno Gutiérrez realizó la declaratoria inaugural en representación del C. Gobernador del Estado de Jalisco.

Los trabajos de la reunión iniciaron con una intervención del Dr. Alfredo Bustos y de la Tijera, quien hizo referencia a los objetivos y fases del Foro, comentando los temas que se abordaron en Boca del Río, Ver., así como de los que serán tratados en las reuniones que se realizarán en las ciudades de Monterrey, N.L., de Tijuana, B. C., y de México, D. F.

En este evento se abordaron diversos aspectos relacionados con la tipificación de delitos cometidos con el uso de herramientas informáticas que lesionan patrimonios y derechos de personas físicas y morales, así como el valor probatorio del documento electrónico en procesos administrativos y judiciales.

La sesión de conferencias dio inicio con la participación de la Dra. Luz Ma. Del Pozo y Contreras quien presentó el tema "Prospectiva del Derecho Informático", en el que define el delito informático como "delito electrónico", considerado éste como aquel que se comete con el uso de las computadoras o cualquier otro medio electrónico, como pueden ser las telecomunicaciones. Resaltó la necesidad de reglamentación jurídica en campos tales como prevención, caracterización del delito electrónico, determinación técnica del grado delictuoso, fijación de responsabilidades, negligencia, restitución e indemnización por daños, etc., ya que su impunidad propicia su reincidencia.

Manifestó, que la tipificación del delito electrónico se podría realizar a partir de la identificación de las siguientes categorías: Sabotaje político o económico, uso desmesurado de poder, discriminación o marginación, manipulación de datos y personas, hurto de ideas y propiedades, como algunos ejemplos.

Asimismo, la Dra. del Pozo presentó un documento sobre "Mecanismos existentes con ausencia de estructura", señalando que el Derecho Informático, hasta el presente, se encuentra sin estructuralidad institucional y con una gran necesidad de investigación y desarrollo.

Propuso que se establezca un modelo donde el campo universal del Derecho Informático se componga de elementos tales como la informática legislativa, jurídica, educacional y administrativa, entre otros. En este tema presentó la definición de términos como "delito electrónico", "derecho a la privacidad" y "principio a la seguridad" entre otros, en consideración a que los conceptos antiguos perjudican a un país, mencionando algunos aspectos que considera corresponden al perfil del delincuente.

Posteriormente, el Lic. Juan Manuel Moran Amador presento el tema "Alternativas de auditoría informática contra la piratería", refiriéndose a la educación como elemento básico para propiciar actitudes éticas en los estudiantes, ya que el problema de piratería se presenta principalmente en las escuelas y siguen practicándola como usuarios de tecnología.

Propone un procedimiento que permita un mayor control en el registro de programas de computación y la realización de auditorías para detectar uso de programas no autorizados. En estas acciones sugiere la participación de maestros y alumnos, así como entregar un programa con el que se haya realizado la auditoría y el cual se haga llegar a la autoridad competente.

Con el tema "Copia ilegal del software" el Ing. Víctor Rodríguez Medina se refirió a la problemática que representa la piratería del software y la pérdida económica que significa para sus desarrolladores.

Indicó, que no obstante que en países como Estados Unidos, Canadá y Japón existe alguna legislación al respecto, el problema de uso ilegal de software subsiste a grandes escalas, la legislación actual no ha sido suficiente para minimizar el uso ilegal de software, por lo que propone se instrumenten mecanismos técnicos y legales que propicien una protección mas eficiente.

Posteriormente, se presentó una conferencia sobre "Elementos para fincar responsabilidades a los administradores de sistemas de redes" a cargo del Lic. Luis Manuel Ramírez Perches, quien manifestó que la falta de preparación de las personas a cargo de las redes computacionales, las hace vulnerables a la introducción de personal ajeno a éstas, como lo son los "hackers" y la introducción de virus informáticos debido a negligencia.

Propuso la determinación de la responsabilidad de los administradores de una red de cómputo, basándose en su nivel de conocimiento y capacitación, así como el grado de negligencia o de dificultad para perpetrar los ilícitos.

A continuación, el Lic. Antonio Aveleyra habló sobre las medidas penales aplicables a los delitos cometidos con medios electrónicos, indicándo que no obstante que existe alguna legislación en la que se consideran aspectos relacionados con las Tecnologías de la Información, existen conductas sociales que debido a su novedad no están aun tipificadas, mencionando como ejemplo las de alteración de datos, acceso no autorizado a la información o servicios de cómputo, uso de información privilegiada, así como la intervención de líneas de teleproceso.

Para tal efecto presentó una propuesta de iniciativa de ley en la que se contemplan aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente.

ANALISIS Y REFLEXIÓN

Cabe señalar, que adicionalmente se recibieron ponencias a cuyos autores no les fue posible asistir a este evento, con temas relacionados con la tipificación del delito informático, las cuales serán integradas a las memorias de este Foro.

Acto seguido, el panel de especialistas así como el auditorio emitieron diversos comentarios, los cuales giraron en torno a los siguientes temas:

- Actividades informáticas que se pueden considerar como conductas delictivas y su definición.
- Responsabilidad del uso de tarjetas de crédito tanto del prestador de servicio como del usuario.
- Elementos que deben considerarse para determinar la responsabilidad de las personas autorizadas para administrar bases de datos.
- Necesidad de definir el ámbito de aplicación del derecho informático.
- Posibilidad de reconocimiento del documento electrónico como medio de prueba.
- Requisitos que debe tener un sistema para que su bitácora sea reconocida legalmente.

CONCLUSIONES

Entre las conclusiones preliminares que se alcanzaron en este segundo evento, destacan:

- La tipificación del delito electrónico se podría realizar a partir de la identificación y definición de sus características.
- Establecer un modelo de Derecho Informático que incluya componentes jurídicos, educacionales y administrativos.
- Establecer un procedimiento que permita un mayor control en el registro de programas de computación y la realización de auditorías para detectar uso de programas no autorizados.
- Instrumentar mecanismos técnicos y legales que propicien una protección más eficiente para minimizar el uso ilegal de software.
- Determinar la responsabilidad de los administradores de una red de cómputo, basándose en su nivel de conocimiento y capacitación, así como el grado de negligencia o de dificultad para perpetrar los ilícitos.
- Presentar propuestas de iniciativa de ley que contemplen aspectos relacionados con las conductas que no están claramente tipificadas en el Código Penal vigente y disposiciones complementarias.
- La invitación a los asistentes que tengan alguna propuesta que pueda integrarse a las memorias de este evento.

MEMORIAS DEL FORO DE CONSULTA SOBRE DERECHO E INFORMÁTICA

Relatoria del Quinto Evento del Foro de Consulta Sobre Derecho de Informática

En la ciudad de México, D.F, el 4 de octubre de 1996 se realizó el quinto evento del Foro de Consulta sobre Derecho e Informática, organizado en forma conjunta por la Honorable Cámara de Diputados y el Instituto Nacional de Estadística, Geografía e Informática y, con la finalidad de revisar el marco jurídico inherente a la informática.

A esta reunión asistieron aproximadamente 160 representantes de los sectores público, privado, académico, empresarial y de investigación.

El acto inaugural estuvo presidido por el Dip. Humberto Roque Villanueva, Presidente de la Gran Comisión de la Cámara de Diputados; el Dr. Alfredo Bustos y de la Tijera, Director General de Política Informática en representación del Dr. Carlos M. Jarque, Presidente del INEGI; el Dip. Eugenio Ortiz Walls, Presidente del Comité de Biblioteca e Informática de la Cámara de Diputados; el Dip. Gustavo Salinas Iñiguez, Secretario del Comité de Biblioteca e Informática de la H. Cámara de Diputados; el Dr. Francisco J. Paoli Bolio, Presidente de la Comisión de Ciencia, Tecnología e Informática de la Asamblea de Representantes; Lic. María del Socorro Téllez Silva como integrante de la Facultad de Derecho de la UNAM; el Ing. Erasmo Marín Córdova, Presidente de la Academia Mexicana de Informática, A.C., y el Lic. Jesús de la Rosa, Presidente de la Asociación Nacional de la Industria de Programas para Computadoras.

Primeramente hizo uso de la palabra el Dip. Eugenio Ortiz Walls, quien mencionó que en el marco del Derecho y la informática, es necesaria la actualización de las normas aplicables a la informática.

Hizo una reflexión al indicar que la mecánica acordada para llevar a cabo este foro, ha sido la acertada ya que los resultados son los adecuados. Mencionó los temas que han sido abordados en cada una de las sedes, e indicó que con éstos no queda agotada la temática, sino que se sientan las bases para realizar un esfuerzo para la solución práctica de los problemas, mediante la aplicación de las normas jurídicas.

El Dip. Gustavo Salinas Iñiguez, dio la bienvenida a los participantes, comentando que encuentros como éste, donde se manifiesta un amplio espíritu de colaboración entre dos Poderes de la Unión, constituyen la oportunidad de buscar el marco jurídico que favorezca el aprovechamiento de las tecnologías de la información, el cual estuvo inspirado en lo señalado en el Plan Nacional de Desarrollo 1995-2000.

Mencionó algunos países que cuentan con una legislación en la materia, y señaló que en nuestro país existen algunas disposiciones diseminadas, las cuales es necesario analizar para precisar su aplicación en el ámbito de la informática.

Finalmente, resaltó la importancia de preparar a la sociedad para dotar al país de una legislación para cumplir con el propósito de promover el desarrollo y aprovechamiento de la tecnología informática.

Más adelante, el Dr. Alfredo Bustos y de la Tijera, señaló que uno de los objetivos generales del Programa de Desarrollo Informático establece contar con disposiciones jurídicas que aseguren las condiciones adecuadas para favorecer el aprovechamiento de la informática y el desarrollo de la infraestructrura en la materia. Determina, además, dentro de las líneas de acción, instancias de coordinación para el análisis y adecuación de la normatividad, con la finalidad de sustentar la evolución y el uso de la informática, acorde con las necesidades del país.

Resaltó, que con base en lo anterior y a iniciativa de la Honorable Cámara de Diputados, se promovió la realización de este Foro, con la finalidad de recopilar las propuestas y experiencias en torno al marco jurídico relativo al uso y desarrollo de la informática.

Para concluir, hizo referencia a los objetivos y fases del Foro, presentando los antecedentes y comentarios respecto a los temas que se abordaron en Boca del Río, Ver., en Guadalajara, Jal., en Monterrey, N.L., y en Tijuana, B.C.

A continuación el Dip. Humberto Roque Villanueva durante su intervención, comentó que a través del Foro de Consulta sobre Derecho e Informática se han obtenido importantes propuestas que contribuyan a formar criterios que deben prevalecer para legislar en el ámbito informático.

Señaló que el uso generalizado de esta tecnología plantea necesidades normativas que deben ser estudiadas para conciliar la participación de todas las áreas en las que esté inmersa la informática.

Resaltó la necesidad de realizar un análisis comparativo de la legislación de otros países que permita crear nuevas formas que apoyen una mayor competitividad y productividad con el adecuado uso de recursos e infraestructura informática.

El desarrollo de la informática, continuó, hace necesario un marco que se apegue a las condiciones que presenta este fenómeno mundial, que es susceptible de ser asociada con conductas antisociales que requieren definición de tipos penales y de sus respectivas sanciones, por lo que se requiere reflexionar en cuanto a su impacto y alcance de aplicación.

Finalmente, el Diputado Roque Villanueva procedió a declarar formalmente inaugurados los trabajos de esta reunión.

Para iniciar los trabajos el Dr. Macedonio Alanís González, hizo uso de la palabra, explicando la mecánica de participación de los ponentes y la forma en que el público debería hacer llegar sus comentarios y sugerencias.

Los temas que se abordaron en este evento giraron en torno a las condiciones para la prestación de servicios telemáticos, públicos y privados, así como a las condiciones de acceso universales a la información y a la infraestructura tecnológica.

La sesión de conferencias inició con la participación de la Dra. Ma. del Socorro Téllez Silva, quien realizó una presentación sobre la Naturaleza Jurídica del Programa de Cómputo, planteando la falta de una regulación sui géneris de los derechos de autor que produce problemas de inseguridad jurídica en los autores intelectuales de los programas de cómputo, incidiendo en la producción de virus informático, plagio, piratería y riesgo del desplome de los sistemas de cómputo existentes, con graves consecuencias en la economía nacional.

Manifestó la hipótesis de que el desconocimiento de la naturaleza de los programas de cómputo, provoca su inadecuada regulación dentro de la legislación.

Indicó, que es necesario que exista coherencia entre la técnica y la legislación ya que desde su nomenclatura produce sorpresa e inseguridad al inventor que al tratar de ubicar su programa de cómputo que servirá a la industria, lo remitan a la Ley de Derechos de Autor.

Concluyó que considerando lo anterior, debe crearse una legislación especial para los bienes informáticos, que garantice una protección completa o, en su caso, que se integre un apartado especial en la Ley de la Propiedad Industrial que de seguridad al inventor de un programa que servirá para dar una solución a algún problema de la industria.

A continuación el Ing. José Luis Echandi Aguilar, presentó el tema Impacto Jurídico en la Seguridad Informática, refiriéndose a los riesgos potenciales en el manejo de la información y la fragilidad jurídica para sancionar los delitos.

Asimismo, comentó que al entrar las organizaciones en el remolino de la productividad, las áreas de tecnología se han visto en la necesidad de actuar a ritmos vertiginosos para satisfacer las necesidades del negocio, lo que ha ocasionado que los aspectos de seguridad queden un tanto a la deriva, ya que esta dinámica provoca que existan mayores riesgos en el manejo de información.

Hizo énfasis en la necesidad de recapacitar sobre los imprevistos que se presentan cuando se realizan las auditorías, o presentan contingencias, aparecen los virus, u otros factores que nos hacen meditar sobre la importancia de los esquemas de seguridad.

Propuso como medidas para atenuar el impacto de lo anterior las de sensibilizar a los diferentes niveles de la organización sobre la importancia que representa la seguridad y su legislación para proteger la información, equipos e instalaciones; formalizar la función de seguridad informática con personal que cuente con un perfil que le permita involucrarse en las diferentes plataformas tecnológicas de la organización; así como contar con el marco jurídico que permita cubrir a las organizaciones de acciones fraudulentas que pongan en riesgo la integridad, confidencialidad y confiabilidad de la información.

El Dr. Julio Téllez, durante su intervención, manifestó que la informática es un verdadero fenómeno social que requiere tutela del Derecho.

Consideró importante establecer un concepto constitucional que manifieste la responsabilidad del Estado de promover y regular el desarrollo científico y técnico en nuestro país. Asimismo, agregó, que el uso de la informática respetará los derechos de las personas y de la misma sociedad.

Más adelante el Lic. Jesús de la Rosa comentó que la industria de cómputo en México no ha logrado alcanzar un desarrollo pleno de acuerdo a sus potencialidades ya que a traves de ésta se puede fomentar la mano de obra y la generación de empleos, así como impulsar a la micro y medianas empresas en virtud de no requerir una inversión cuantiosa.

Señaló, que al igual que en otros países México debe realizar programas de fomento de esta industria que además de una infraestructura tecnológica y de recursos humanos calificados contemple el marco jurídico de protección legal que brinde seguridad y confianza a inversionistas extranjeros y nacionales.

Mencionó que no obstante las reformas a la Ley Federal de Derechos de Autor en el año de 1991, dio bases para una protección a desarrolladores de programas de cómputo, no se ha podido erradicar el problema de copias ilegales, lo que ha inhibido la atracción de capitales para fomentar esta industria.
Para tal efecto hizo referencia a una nueva propuesta por parte de la ANIPCO para efectuar algunas precisiones en la ley referida.

Posteriormente, el Ing. Miguel Angel Alvarado, Presidente de la Asociación Latinoamericana de Profesionales de Seguridad en Informática, A.C., presentó una serie de políticas y recomendaciones para la prestación de servicios públicos y privados, así como las condiciones de acceso universal a la información, acceso a la infraestructura tecnológica y protección de información en el ambiente telemático.

El Lic. Rosendo Sánchez Palma, participó con una ponencia sobre Intercambio Electrónico de Información, señalando que a través de este proceso ha sido posible tener nuevas formas de organización en el comercio, en la educación y en general en la realización de las diversas actividades y proyectos de trabajo.

Mencionó, que para el eficaz aprovechamiento de una infraestructura de comunicación, es necesario que garantice elementos de autenticidad, integridad y el no rechazo de la información, con lo cual el uso del documento electrónico no debe presentar problemas distintos a los que se presentan al usar documentos tradicionales.

Señaló, además, que las leyes deben contemplar dichos elementos y reconocer la validez de los documentos que cumplan con ellos y que, asimismo, deben estudiarse aspectos relacionados con el uso de medios informáticos con intención de defraudar y el uso no autorizado de información personal contenida en bases de datos, en los que se determinen penas que desanimen cualquier actividad.

Posteriormente, el Dr. Jorge Borrego durante su participación con el trabajo titulado "¿Una autopista de información sin tráfico? Reflexiones sobre las condiciones para el desarrollo de los servicios telemáticos públicos y privados de la infraestructura mexicana de información", señaló que en México se debe considerar la creación de la infraestructura de información aprovechando la tecnología que se ha venido aplicando en INTERNET, ya que este tipo de red de interconectividad e intercambio de información ha sido desde hace algunos años, el eje principal del avance tecnológico de nuestros socios comerciales como son EE. UU. y Canadá. Indicó, también, que siendo ésta la tendencia mundial, las empresas que se han conectado a estas grandes redes conocen ya los beneficios de comunicación, información y de transacciones comerciales que se pueden realizar.

Resaltó la importancia de estas redes a nivel mundial, y de los beneficios que ha brindado y el tipo de tecnología que se utiliza, así como el alcance no sólo para las empresas, universidades, dependencias y otros lugares públicos, sino también en el hogar.

Finalmente, indicó que es necesario que las dependencias gubernamentales compartan información de dominio público, por lo que es indispensable la determinación de una legislación que permita al sector gubernamental no sólo compartir información, sino brindar servicios al público que agilicen trámites administrativos, lo cual repercutirá en beneficios para la sociedad.

Por su parte, el Lic. Sergio Huacuja, durante su intervención con el tema "Actualización normativa sobre bienes y servicios informáticos", comentó que la complejidad de las relaciones gubernamentales y su interacción con los fenómenos sociales, obliga a revisar el marco jurídico regulatorio de las adquisiciones de bienes y servicios del Estado, y muy particularmente del régimen de contratación informática que utilizará como medio para la consecución más eficiente de sus fines.

Señaló que actualmente la Ley de Adquisiciones y Obras Públicas reglamentaria del artículo 134 constitucional, si bien prevé los procedimientos indispensables para la salvaguarda de los principios de eficiencia, eficacia, imparciabilidad y honestidad, omite el uso de la informática como apoyo sistemático para las dependencias y entidades de la Administración Pública Federal, lo cual supone que debe integrarse en la nueva legislación que está en proceso de debate la regulación de los sistemas COMPRANET y establecer sobre sus bases objetivas el valor y alcance legal de la información en él manejada.

Posteriormente, el Act. Carlos Jasso, presentó la ponencia titulada "Un marco normativo administrativo que favorezca la prestación de servicios gubernamentales por medio de redes informáticas".

Resaltó la importancia del uso de la comunicación electrónica y la transferencia electrónica de documentos en la prestación de servicios telemáticos públicos y privados como herramienta que brinda la oportunidad de simplificar y mejorar los servicios gubernamentales en la realización de trámites administrativos por parte de los ciudadanos, aun en comunidades lejanas y marginadas.

Señaló que para poder aprovechar el potencial de la aplicación de estas tecnologías, es necesario contar con un marco normativo-administrativo que favorezca su desarrollo, en especial aquel que incide en la interacción del sector público con la ciudadanía, a fin de posibilitar, además de los procedimientos tradicionales, el uso de medios electrónicos para la notificación y entrega de documentación y que, asimismo, se contemplen aspectos que garanticen los derechos de los ciudadanos en cuanto a igualdad de acceso para la utilización de estos medios y la protección de la información contenida o transmitida por ellos. Además, indicó que debe contarse con lineamientos administrativos en los que se definan estándares y medidas de seguridad indispensables para el uso de medios electrónicos.

Más adelante, el Dr. Noé Riande Juárez, presentó el trabajo "Democracia de la información, Derecho a la Información y Servicio al ciudadano", en el cual señaló que el acceso democrático a la información, requiere de la coordinación y de la adopción de estándares para la interconexión de los sistemas de información pública y de las redes de distribución, esto es, se requiere de una reglamentación de los servicios de información para facilitar el acceso a la misma.

En lo que se refiere a la situación del Estado como ofertador de servicios de información, por darse en un contexto de mercado, exige de la administración pública el manejo de las herramientas de la publicidad y la mercadotecnia, como condición para poder ofrecerlos de manera profesional y competitiva.

Para finalizar la sesión de conferencias, el Ing. Leopoldo Vega realizó una serie de señalamientos en torno a servicios telemáticos en México. Comentó que la legislación que se genere deberá contemplar que la información electrónica fluya de manera democrática. Asimismo, aseveró que deberá fomentarse y reglamentarse la creación de una infraestructura telemática y de comunicaciones a nivel nacional.

ANALISIS Y REFLEXIÓN

A continuación, el panel de especialistas así como el auditorio emitieron diversos comentarios, los cuales giraron en torno a los siguientes temas:

- Acceso a la información
  Analfabetismo informático
  Disponibilidad de tecnologías y herramientas
  Disponibilidad de información

- Utilidad y aplicación de la informática
  Valor probatorio del documento electrónico
  Valor de las transacciones electrónicas
- Regulación jurídica que proteja y ponga orden para propiciar el desarrollo informático
- Derechos y responsabilidades de desarrolladores de software

LEY DE EXTRADICIÓN INTERNACIONAL

CAPITULO I
OBJETO Y PRINCIPIOS

Artículo 1.- Las disposiciones de esta ley son de orden publico, de carácter federal y tienen por objeto determinar los casos y las condiciones para entregar a los estados que lo soliciten, cuando no exista tratado internacional, a los acusados ante sus tribunales, o condenados por ellos, por delitos del orden común.

Artículo 2.- Los procedimientos establecidos en esta ley se deberán aplicar para el trámite y resolución de cualquier solicitud de extradición que se reciba de un gobierno extranjero.

Artículo 3.- Las extradiciones que el gobierno mexicano solicite de estados extranjeros, se regirán por los tratados vigentes y a falta de estos, por los artículos 5, 6, 15 y 16 de esta ley.

Las peticiones de extradición que formulen las autoridades competentes federales, de los estados de la república o del fuero común del distrito federal, se tramitaran ante la secretaria de relaciones exteriores por conducto de la procuraduría general de la república.

Artículo 4.- Cuando en esta ley se haga referencia a la ley penal mexicana, deberá entenderse el código penal para el distrito federal en materia de fuero común y para toda la república en materia de fuero federal, así como todas aquellas leyes federales que definan delitos.

Artículo 5.- Podrán ser entregados conforme a esta ley los individuos contra quienes en otro país, se haya incoado un proceso penal como presuntos responsables de un delito o que sean reclamados para la ejecución de una sentencia dictada por las autoridades judiciales del estado solicitante.

Artículo 6.- Darán lugar a la extradición los delitos dolosos o culposos, definidos en la ley penal mexicana, si concurren los requisitos siguientes:

I.- Que tratándose de delitos dolosos, sean punibles conforme a la ley penal mexicana y a la del estado solicitante, con pena de prisión cuyo termino medio aritmético por lo menos sea de un año; y tratándose de delitos culposos, considerados como graves por la ley, sean punibles, conforme a ambas leyes, con pena de prisión.

II.- Que no se encuentren comprendidos en alguna de las excepciones previstas por esta ley.

Artículo 7.- No se concederá la extradición cuando:

I.- El reclamado haya sido objeto de absolución, indulto o amnistía o cuando hubiere cumplido la condena relativa al delito que motive el pedimento;

II.- Falte querella de parte legitima, si conforme a la ley penal mexicana el delito exige ese requisito;
III.- Haya prescrito la acción o la pena, conforme a la ley penal mexicana o a la ley aplicable del estado solicitante, y
IV.- El delito haya sido cometido dentro del ámbito de la jurisdicción de los tribunales de la república.

Articulo 8.- En ningún caso se concederá la extradición de personas que puedan ser objeto de persecución politica del estado solicitante, o cuando el reclamado haya tenido la condición de esclavo en el país en donde se cometió el delito.

Articulo 9.- No se concederá la extradición si el delito por el cual se pide es del fuero militar.

Articulo 10.- El estado mexicano exigirá para el tramite de la petición, que el estado solicitante se comprometa:

I.- Que, llegado el caso, otorgara la reciprocidad;
II.- Que no serán materia del proceso, ni aun como circunstancias agravantes, los delitos cometidos con anterioridad a la extradición, omitidos en la demanda e inconexos con los especificados en ella. El estado solicitante queda relevado de este compromiso si el inculpado consciente libremente en ser juzgado por ello o si permaneciendo en su territorio mas de dos meses continuos en libertad absoluta para abandonarlo, no hace uso de esta facultad;
III.- Que el presunto extraditado será sometido a tribunal competente, establecido por la ley con anterioridad al delito que se le impute en la demanda, para que se le juzgue y sentencie con las formalidades de derecho;
IV.- Que será oído en defensa y se le facilitaran los recursos legales en todo caso, aun cuando ya hubiere sido condenado en rebeldía;
V.- Que si el delito que se impute al reclamado es punible en su legislación hasta con la pena de muerte o alguna de las señaladas en el articulo 22 constitucional, solo se impondrá la de prisión o cualquier otra de menor gravedad que esa legislación fije para el caso, ya sea directamente o por substitución o conmutación.
VI.- Que no se concederá la extradición del mismo individuo a un tercer estado, sino en los casos de excepción previstos en la segunda fracción de este articulo; y
VII.- Que proporcionara al estado mexicano una copia autentica de la resolución ejecutoriada que se pronuncie en el proceso.

Articulo 11.- Cuando el individuo reclamado tuviere causa pendiente o hubiere sido condenado en la república por delito distinto del que motive la petición formal de extradición, su entrega al estado solicitante, si procediere, se diferirá hasta que haya sido decretada su libertad por resolución definitiva.

Articulo 12.- Si la extradición de una misma persona fuere pedida por dos o mas estados y respecto de todos o varios de ellos fuere procedente, se entregara el acusado:

I.- Al que lo reclame en virtud de un tratado;
II.- Cuando varios estados invoquen tratados, a aquel en cuyo territorio se hubiere cometido el delito;
III.- Cuando concurran dichas circunstancias, al estado que lo reclame a causa de delito que merezca pena mas grave; y
IV.- En cualquier otro caso, al que primero haya solicitado la extradición o la detención provisional con fines de extradición.

Articulo 13.- El estado que obtenga la preferencia de la extradición con arreglo al articulo anterior, podrá declinarla en favor de un tercero que no la hubiere logrado.

Articulo 14.- Ningún mexicano podrá ser entregado a un estado extranjero sino en casos excepcionales a juicio del ejecutivo.

Articulo 15.- La calidad de mexicano no será obstáculo a la entrega del reclamado cuando haya sido adquirida con posterioridad a los hechos que motiven la petición de extradición.

CAPITULO II
PROCEDIMIENTO

Articulo 16 .- La petición formal de extradición y los documentos en que se apoye el estado solicitante, deberán contener:

I.- La expresión del delito por el que se pide la extradición;
II.- La prueba que acredite los elementos del tipo del delito y la probable responsabilidad del reclamado. cuando el individuo haya sido condenado por los tribunales del estado solicitante, bastara acompañar copia autentica de la sentencia ejecutoriada.
III.- Las manifestaciones a que se refiere el articulo 10, en los casos en que no exista tratado de extradición con el estado solicitante.
IV.- La reproducción del texto de los preceptos de la ley del estado solicitante que definan el delito y determinen la pena, los que se refieran a la prescripción de la acción y de la pena aplicable y la declaración autorizada de su vigencia en la época en que se cometió el delito;
V.- El texto autentico de la orden de aprehensión que, en su caso, se haya librado en contra del reclamado; y
VI.- Los datos y antecedentes personales del reclamado, que permitan su identificación, y siempre que sea posible, los conducentes a su localización. Los documentos señalados en este articulo y cualquier otro que se presente y estén redactados en idioma extranjero, deberán ser acompañados con su traducción al español y legalizados conforme a las disposiciones del código federal de procedimientos penales.

Articulo 17.- Cuando un estado manifieste la intención de presentar petición formal para la extradición de una determinada persona, y solicite la adopción de medidas precautorias respecto

de ella, estas podrán ser acordadas siempre que la petición del estado solicitante contenga la expresión del delito por el cual se solicitara la extradición y la manifestación de existir en contra del reclamado una orden de aprehensión emanada de autoridad competente.

Si la secretaria de relaciones exteriores estimare que hay fundamento para ello, transmitirá la petición al procurador general de la república, quien de inmediato promoverá ante el juez de distrito que corresponda, que dicte las medidas apropiadas, las cuales podrán consistir, a petición del procurador general de la república, en arraigo o las que procedan de acuerdo con los tratados o las leyes de la materia.

Articulo 18.- Si dentro del plazo de dos meses que previene el articulo 119 de la constitución política de los estados unidos mexicanos, contados a partir de la fecha en que se hayan cumplimentando las medidas señaladas en el articulo anterior, no fuere presentada la petición formal de extradición a la secretaria de relaciones exteriores, se levantaran de inmediato dichas medidas.

El juez que conozca del asunto notificara a la secretaria de relaciones exteriores el inicio del plazo al que se refiere este articulo, para que la secretaria, a su vez, lo haga del conocimiento del estado solicitante.

Articulo 19.- Recibida la petición formal de extradición, la secretaria de relaciones exteriores la examinara y si la encontrare improcedente no la admitirá, lo cual comunicara al solicitante.

Articulo 20.- Cuando no se hubieren reunido los requisitos establecidos en el tratado o, en su caso, en el articulo 16, la secretaria de relaciones exteriores lo hará del conocimiento del estado promovente para que subsane las omisiones o defectos señalados, que en caso de estar sometido el reclamado a medidas precautorias, deberá cumplimentarse dentro del termino a que se refiere el articulo 18.

Articulo 21.- Resuelta la admisión de la petición la secretaria de relaciones exteriores enviara la requisitoria al procurador general de la república acompañando el expediente, a fin de que promueva ante el juez de distrito competente, que dicte auto mandándola cumplir y ordenando la detención del reclamado, así como, en su caso, el secuestro de papeles, poder, relacionados con el delito imputado o que puedan ser elementos de prueba, cuando así lo hubiere pedido el estado solicitante.

Articulo 22.- Conocerá el juez de distrito de la jurisdicción donde se encuentre el reclamado. Cuando se desconozca el paradero de este, será competente el juez de distrito en materia penal en turno del distrito federal.

Articulo 23.- El juez de distrito es irrecusable y lo actuado por el no admite recurso alguno. Tampoco serán admisibles cuestiones de competencia.

Articulo 24.- Una vez detenido el reclamado, sin demora se le hará comparecer ante el respectivo juez de distrito y este le dará a conocer el contenido de la petición de extradición y los documentos que se acompañen a la solicitud. En la misma audiencia podrá nombrar defensor. en caso de no tenerlo y desea hacerlo, se le presentara lista de defensores de oficio para que elija. si no designa, el juez lo hará en su lugar.

El detenido podrá solicitar al juez se difiera la celebración de la diligencia hasta en tanto acepte su defensor cuando este no se encuentre presente en el momento del discernimiento del cargo.

Articulo 25.- Al detenido se le oirá en defensa por si o por su defensor y dispondrá hasta de tres días para oponer excepciones que únicamente podrán ser las siguientes:

I.- La de no estar ajustada la petición de extradición a las prescripciones del tratado aplicable, o a las normas de la presente ley, a falta de aquel; y
II.- La de ser distinta persona de aquella cuya extradición se pide. El reclamado dispondrá de veinte días para probar sus excepciones. Este plazo podrá ampliarse por el juez en caso necesario, dando vista previa al ministerio publico. dentro del mismo plazo, el ministerio publico podrá rendir las pruebas que estime pertinentes.

Articulo 26.- El juez atendiendo a los datos de la petición formal de extradición, a las circunstancias personales y a la gravedad del delito de que se trata, podrá conceder al reclamado, si este lo pide, la libertad bajo fianza en las mismas condiciones en que tendría derecho a ella si el delito se hubiere cometido en territorio mexicano.

Articulo 27.- Concluido el termino a que se refiere el articulo 25 o antes si estuvieren desahogadas las actuaciones necesarias, el juez dentro de los cinco días siguientes, secretaria de relaciones exteriores su opinión jurídica respecto de lo actuado y probado ante el.

El juez considerara de oficio las excepciones permitidas en el articulo 25, aun cuando no se hubieren alegado por el reclamado.

Articulo 28.- Si dentro del termino fijado en el articulo 25 el reclamado no opone excepciones o consciente expresamente en su extradición, el juez procederá sin mas tramite dentro de tres días, a emitir su opinión.

Articulo 29.- El juez remitirá, con el expediente, su opinión a la secretaria de relaciones exteriores, para que el titular de la misma dicte la resolución a que se refiere el articulo siguiente. el detenido entre tanto, permanecerá en el lugar donde se encuentra a disposición de esa dependencia.

Articulo 30.- La secretaria de relaciones exteriores en vista del expediente y de la opinión del juez, dentro de los veinte días siguientes, resolverá si se concede o rehusa la extradición. En el

mismo acuerdo, se resolverá, si fuere el caso, sobre la entrega de los objetos a que se refiere el articulo 21.

Articulo 31.- Si la decisión fuere en el sentido de rehusar la extradición, se ordenara que el reclamado sea puesto inmediatamente en libertad a menos que sea el caso de proceder conforme al articulo *siguiente*.

Articulo 32.- Si el reclamado fuere mexicano y por ese solo motivo se rehusare la extradición, la secretaria de relaciones exteriores notificara el acuerdo respectivo al detenido, y al procurador general de la república, poniéndolo a su disposición, y remitiéndole el expediente para que el ministerio público consigne el *caso al tribunal competente si hubiere lugar a ello*.

Articulo 33.- En todos los casos si la resolución fuere en el sentido de conceder la extradición, esta se notificara al reclamado.

Esta resolución solo será impugnable *mediante juicio de amparo*. Transcurrido el termino de quince días sin que el reclamado o su legitimo representante haya interpuesto demanda de amparo o si, en su caso, este es negado en definitiva, la secretaria de relaciones exteriores comunicara al estado solicitante el acuerdo favorable a la extradición y ordenara que se le entregue el sujeto.

Articulo 34.- La entrega del reclamado, previo aviso a la secretaria de gobernación, se efectuara por la procuraduría general de la república al personal autorizado del estado que obtuvo la *extradición*, en el puerto fronterizo o en su caso a bordo de la aeronave en que deba viajar el extraditado. La intervención de las autoridades mexicanas cesara, en este ultimo caso, en el momento en que la aeronave este lista para emprender el vuelo.

Articulo 35.- Cuando el estado solicitante deje pasar el termino de sesenta días naturales desde el *día siguiente en que el reclamado* quede a su disposición sin hacerse cargo de el, este recobrara su libertad y no podrá volver a ser detenido ni entregado al propio estado, por el mismo delito que motivo la solicitud de extradición.

Articulo 36.- El ejecutivo de la *unión podrá* acceder en los términos del articulo 10, cuando lo solicite un estado extranjero para concederle una extradición que no sea obligatoria en virtud de un tratado.

Articulo 37.- Los gastos que ocasione toda extradición podrán ser gastados por el erario federal con cargo al estado solicitante que la haya promovido.

TRANSITORIOS

Articulo primero.- Esta ley entrara en vigor al día siguiente de su publicación en el "diario oficial" de la federación y abroga la ley de extradición de 19 de mayo de 1897.

Articulo segundo.- *Todas las* extradiciones que estén en tramite al entrar en vigor esta ley se sujetaran a sus disposiciones.

México, D. F., a 18 de diciembre de 1975.- *Emilio M. González Parra*, S. P.- Luis del Toro Calero, D. P.- German Corona del Rosal, S. S.- Rogelio García González, D. S.- Rubricas. En cumplimiento de lo dispuesto por la fracción I del articulo 89 de la Constitución politica de los estados unidos mexicanos y para su debida publicación y observancia, expido el *presente decreto* en la residencia del poder ejecutivo federal, en la ciudad de México, Distrito Federal, a los Veintidos días del mes de diciembre de mil novecientos setenta y cinco.- Luis Echeverria Alvarez.- rubrica.- El Secretario de Relaciones Exteriores, Emilio o. Rabasa.- Rubrica.- El Secretario de Gobernación, Mario Moya Palencia.- Rubrica.

BIBLIOGRAFIA GENERAL

Amuchategui Requena, Irma G. Derecho Penal. Curso Primero y Segundo. Colección de Textos Jurídicos Universitarios. Editorial Harla. México 1990.

Carranca y Trujillo, Raúl. Derecho Penal Mexicano. México. Editorial Porrúa. Quinceava Edición. México 1988.

Castellanos Tena, Fernando. Lineamientos elementales de Derecho Penal. Editorial Porrúa. S.A. México 1984. Vigésima Edición.

Colin Sánchez, Guillermo. Derecho Mexicano de Procedimientos Penales. Edición Décimocatorce Editorial Porrúa S.A. México 1988.

Correa M. Carlos. Derecho Informático. Buenos Aires. Editorial Depalma. 1987.

Cuello Calon, Eugenio. Derecho Penal I. Décimocuarta Edición. Barcelona. 1964.

Fix Fierro, Héctor. Informática y documentación jurídica. 2da. Edición. UNAM. México. D.F. 1996.

González Quintanilla, José Arturo. Derecho Penal Mexicano. Parte General . Editorial Porrúa. México 1991.

H. Aiken. Ch. Babbage. J. Von Neumann. C.E. Shannon. A.M. Turing. W. G. Walter y otros. Perspectivas de la revolución de los computadores. Selección y comentarios de Zenon. W. Pylyshyn. Editorial Alianza. 1994.

IBM de México. Historia de la comunicación. IBM MEXICO. 1997.

Jiménez de Azua. Luis. Principios del Derecho Penal, La Ley Penal y El Delito. Editorial Sudamericana Abelardo Perrot. Buenos Aires 1990.

Jiménez de Azua. Luis. La Ley y el Delito. Décima Edición Sudamericana. Buenos Aires. 1980.

Joyanes Aguilar, Luis. Programación Basica para computadoras. 3era. Edición. Editorial McGraw-Hil. México 1990.

Lima Ma. de la Luz. Delitos Electrónicos. México. Revista Criminalia. No. 50. 1984.
Martínez Garnelo, Jesús. La Investigación Ministerial Previa. Primera Edición. Editorial OGS. Editores S.A. de C.V.

Montoya Martin del Campo, Alberto. México ante la revolución tecnológica. Asociación Mexicana de Investigadores de la Comunicación. Editorial Diana. México 1993.

Mora Enzo Molino, José Luis. Introducción a la Informática. Editorial Trillas. México 1973.

Pavon Vasconcelos, Francisco. Derecho Penal Mexicano. Déciam Edición. S.A. Editorial Porrúa. México 1991.

Ricardo A. Guibourg, Jorge O. Allende. Elena M. Campanella. Manual de Informática Jurídica. Editorial Astrea. Buenos Aires. 1996

Téllez Valdez, Julio. Derecho Informático. 2da. Edición. Editorial McGraw-Hill. México 1996.

Téllez Valdez, Julio. La Protección Jurídica de los Programas de Computo. UNAM. México 1989. 2da. Edición. Instituto de Investigaciones Jurídicas.

Véscovi, Enrique. Teoria General del Proceso. Editorial Temis. Libreria Bogotá-Colombia. 1984.

LEYES Y CODIGOS.

Ley Publicada en el Diario Oficial de la Federación el Lunes 24 de Diciembre de 1996.

Ley Publicada en el Diario Oficial de la Federación el jueves 27 de Junio de 1991.

Código Penal para el Estado de Sinaloa. Editorial Porrúa. Tercera Edición.

TLC de America del Norte. Texto Oficial. Secofi.

DICCIONARIOS Y REVISTAS.

Nuevo Diccionario Enciclopédico Universal y de México 1996. Ediciones Trébol. S.L. Barcelona España.

Eduardo Pallares. Diccionario de Derecho Procesal Civil. Editorial Porrúa. Vigésima Edición. México 1991.

Revista Mecánica Popular. Año 55. Núm. 4, Abril 1998. Televisa S.A. México.

DIRECCIONES EN INTERNET.

http://tiny.uasnet.mx/prof/cin/der/silvia/cppps.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/lexis.htm
http://tiny.uasnet.mx/prof/cin/der/silvia/leyint.htm
http://tiny.uasnet.mx/prof/cin/der/silvia/TLC.htm
http://tiny.uasnet.mx/prof/cin/der/silvia/OAINT.htm
http://ccdis.dis.ulpgc.es/ccdis/legisla/codigope
http://www.mundolatino.org/i/derecho/delitos.htm
http://www.sarenet.es/info/laley.htm
http://www.onnet.es/04001002
http://www.aserte.es/es/04006001.htm
http://info1.juridicas.unam.mx/legfed/8/
http://info1.juridicas.unam.mx/legfed/18/
http://info1.juridicas.unam.mx/legfed/34
http://www.asertel.es/es/0400400.htm
http://www.asertel.es/es/04004002.htm
http://www.asertel.es/es/04004004.htm
http://info1.juridicas.unam.mx/legfed/11
http://info1.juridicas.unam.mx/legfed/8
http://info1.juridicas.unam.mx/legfed/171/
http://info1.juridicas.unam.mx/legfed/152/