UNIVERSIDAD MICHOACANA

DE SAN NICOLÁS

DE HIDALGO

FACULTAD DE DERECHO Y CIENCIAS SOCIALES
DIVISIÓN DE ESTUDIOS DE POSGRADO

TESIS:

INCORPORACIÓN DE LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL DEL ESTADO DE MICHOACÁN

QUE PARA OBTENER EL GRADO DE MAESTRA EN DERECHO PRESENTA

ERÉNDIRA MORA DE LA PEÑA

ASESOR DE TESIS

DOCTOR EN DERECHO JOSÉ BECERRIL LEAL

MORELIA, MICHOACÁN A JUNIO DEL 2014.

ÍNDICE

RESUMEN 5

ABSTRACT 6

INTRODUCCIÓN 7

CAPÍTULO PRIMERO. ANTECEDENTES SOBRE LA INFORMÁTICA SUS CONCEPTOS Y SUS MÚLTIPLES CAMPOS DE ACCIÓN. 9

1.1 ANTECEDENTES DE LA INFORMÁTICA 9

1.1.1 HISTORIA DE LAS COMPUTADORAS 9

1.2 CONCEPTOS DE LA ELECTRÓNICA, INFORMÁTICA Y CIBERNÉTICA 12

1.2.1 LA ELECTRÓNICA 12

1.2.2 LA INFORMÁTICA 13

1.2.3 LA CIBERNÉTICA. 14

1.2.3.1 ORÍGENES DE LA CIBERNÉTICA 14

1.2.4 EL ORDENADOR Y SUS COMPONENTES 15

1.2.5 EL INTERNET 16

1.2.5.1 HISTORIA DE LA INTERNET EN EL MUNDO 17

1.2.5.2 HISTORIA DE LA INTERNET EN MÉXICO 18

1.2.5.3 SERVICIOS DEL INTERNET 21

1.2.5.4 ORGANIZACIÓN DE LA INTERNET 22

1.2.5.5 DENOMINACIÓN 23

1.2.5.6 DIRECCIÓN DE CORREO ELECTRÓNICO (e-mail) 25

1.3. CAMPOS DE ACCIÓN DE LA INFORMÁTICA 26

1.3.1. LA INFORMÁTICA EN LAS CIENCIAS NATURALES 26

1.3.1.1 LA INFORMÁTICA EN LA MEDICINA, EN LA BIOLOGÍA Y EN LA GENÉTICA. 26

1.3.1.2 LA INFORMÁTICA EN LA QUÍMICA Y FÍSICA 28

1.3.2 LA INFORMÁTICA EN LAS CIENCIAS SOCIALES 28

1.3.2.1 LA INFORMÁTICA EN LA ECONOMÍA Y ADMINISTRACIÓN 28

1.3.2.2 LA INFORMÁTICA EN EL DISEÑO, INGENIERÍAS Y MANUFACTURAS 28

1.3.2.3 LA INFORMÁTICA Y LA GUERRA 31

1.3.3 LA INFORMÁTICA EN EL DERECHO 31
1.3.3.1 DERECHO INFORMÁTICO 32
1.3.3.2 DERECHO A LA INFORMÁTICA Y A LA INFORMACIÓN 33
1.3.3.3 LA INFORMÁTICA JURÍDICA 34
1.3.3.4 LA INFORMÁTICA APLICADA AL DERECHO 34
1.3.3.5 LA CIBERNÉTICA JURÍDICA 45
1.3.3.6 DERECHO DE LA INFORMÁTICA 47
1.3.3.7 CONTRATACIÓN ELECTRÓNICA Y COMERCIO ELECTRÓNICO 54
1.4 LOS DELITOS INFORMÁTICOS EN EL MARCO JURÍDICO FEDERAL EN MÉXICO 61
1.5 CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS 62
1.6 LEY DE LA PROPIEDAD INDUSTRIAL 78
1.7 LEY FEDERAL DEL DERECHO DE AUTOR 80
1.8 LEY DE INSTITUCIONES DE CRÉDITO 85
1.9 LEY FEDERAL DE TELECOMUNICACIONES 89
1.10 LEY FEDERAL DE PROTECCION AL CONSUMIDOR 96
1.11 LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL 99
1.12 LEY DE INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA 111
1.13 LEY ORGÁNICA DEL PODER JUDICIAL DE LA FEDERACIÓN 112
1.14 LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA 116
1.15 CÓDIGO FISCAL DE LA FEDERACIÓN 129
1.16 CÓDIGO DE COMERCIO 130
1.17 CÓDIGO PENAL FEDERAL 132
1.18 CÓDIGO CIVIL FEDERAL 136
1.19 CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES 137
1.20 ÓRGANOS NACIONALES 138
1.21 POLICÍA CIBERNÉTICA 139
CAPÍTULO SEGUNDO. EL DELINCUENTE, LOS DELITOS INFORMÁTICOS Y LOS BIENES JURÍDICOS QUE TUTELAN. 142
2.1 SUJETOS DEL DELITO INFORMÁTICO 142
2.2 EL DELINCUENTE INFORMÁTICO 142
2.3 CARACTERISTICAS DE LOS DELITOS INFORMÁTICOS 144

2.4 CLASIFICACION DEL DELITO INFORMÁTICO 146
2.5 LOS DELITOS INFORMÁTICOS CONOCIDOS POR LAS NACIONES UNIDAS 148
2.5.1 LOS FRAUDES 148
2.5.1.1 LOS DATOS FALSOS O ENGAÑOSOS 148
2.5.1.2 MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA" 149
2.5.1.3 LA TÉCNICA DEL SALAMI 149
2.5.1.4 FALSIFICACIONES INFORMÁTICAS 149
2.5.1.5 MANIPULACIÓN DE LOS DATOS DE SALIDA 150
2.5.1.6 PISHING 150
2.5.2 EL SABOTAJE INFORMÁTICO. 151
2.5.2.1 BOMBAS LÓGICAS (LOGIC BOMBS) 151
2.5.2.2 GUSANOS 151
2.5.2.3 VIRUS INFORMÁTICOS Y MALWARE 151
2.5.2.4 CIBERTERRORISMO 152
2.5.2.5 ATAQUES DE DENEGACIÓN DE SERVICIO 152
2.5.3 EL ESPIONAJE INFORMÁTICO Y EL ROBO O HURTO DE SOFTWARE 153
2.5.3.1 FUGA DE DATOS (DATA LEAKAGE) 153
2.5.3.2 REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL 153
2.5.4 EL ROBO DE SERVICIOS 154
2.5.4.1 HURTO DEL TIEMPO DEL COMPUTADOR 154
2.5.4.2 APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING) 154
2.5.4.3 PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION) 154
2.5.5 EL ACCESO NO AUTORIZADO A SERVICIOS INFORMÁTICOS 155
2.5.5.1 LAS PUERTAS FALSAS (TRAP DOORS) 155
2.5.5.2 LA LLAVE MAESTRA (SUPERZAPPING) 155
2.5.5.3 PINCHADO DE LÍNEAS (WIRETAPPING) 155
2.5.5.4 PIRATAS INFORMÁTICOS O HACKERS 156
2.6 DELITOS INFORMÁTICOS COMETIDOS COMO MEDIO O INSTRUMENTO PARA PERPETRAR OTROS ILÍCITOS 156

2.7 BIENES JURÍDICOS 176
2.8 LOS BIENES JURÍDICOS PROTEGIDOS EN EL DELITO INFORMÁTICO 177
2.9 DERECHO A LA INTIMIDAD Y CONFIDENCIALIDAD 179
2.10 DERECHO A LA INFORMACIÓN 185
2.11 DERECHOS PATRIMONIALES 188
2.12 SEGURIDAD NACIONAL 198
CAPÍTULO 3 TERCERO. ESTUDIO PANORÁMICO DE LOS DELITOS INFORMÁTICOS. 205
3.1 DERECHO PANORÁMICO ESTATAL 205
3.2 DERECHO PANORÁMICO EN AMÉRICA SOBRE LOS DELITOS INFORMÁTICOS 237
3.3DERECHO PANORÁMICO INTERNACIONAL SOBRE LOS DELITOS INFORMÁTICOS 263
3.4 ORGANISMOS INTERNACIONALES 282
3.5 ORGANIZACIONES NO GUBERNAMENTALES 285
CAPÍTULO CUARTO. LA INCORPORACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL DE MICHOACÁN. 288
4.1 PLANTEAMIENTO DE LA INVESTIGACIÓN 288
4.2 COMPROBACIÓN DE LA HIPÓTESIS 289
4.3 PROPUESTAS 291
CONCLUSIONES 299
GLOSARIO DE ABREVIATURAS PARA LAS NOTAS AL PIE DE PÁGINA 302
GLOSARIO DE TÉRMINOS 303
FUENTES DE INFORMACIÓN Y DE CONSULTA 330
BIBLIOGRAFÍA 330
DICCIONARIOS. 338
LEGISLACIÓN FEDERAL 339
LEGISLACION ESTATAL 340
FUENTES DE INFORMACIÓN ELECTRÓNICAS 342

RESUMEN

Esta tesis, es un análisis dogmático Jurídico Penal, examinaremos jurídicamente novedosas figuras penales; para esto se consulto prestigiados tratadistas, de los cuales plasmaremos sus teorías en los delitos informáticos, tanto en las legislaciones Federales como en la de los diversos Estados. Vincularemos la Informática con diversas actividades humanas tal como la medicina, la biología, la genética, entre muchas otras, así como la importancia con el Derecho y sus novedosas ramas como lo son: el derecho informático, la informática jurídica, el derecho a la información cibernética jurídica y su vinculación con otras ramas como con el derecho constitucional, el derecho civil, el derecho procesal civil, el derecho de autor, el derecho a la información, el derecho bancario y, sobretodo, el derecho penal, que es el plano de análisis de ésta tesis de grado, y es en donde se encuentran los delitos informáticos. Desarrollamos una descripción de la naturaleza de los delitos informáticos y del marco en que se encuentra interrelacionado con nuestras figuras delictivas, en donde se establecerán los bienes jurídicos que el estado tutela y por medio de que legislaciones lo logra: como la Constitución Política de los Estados Unidos Mexicanos, las leyes secundarias a saber: la ley federal del derecho de autor, la ley de propiedad industrial, la ley de transparencia y acceso a la información pública gubernamental, los códigos civiles; penales federales y estatales, los códigos procesales civiles y penales federales y estatales. Las legislaciones de los estados que analizan ya los delitos informáticos y que servirán de análisis para la propuesta de la incorporación de los delitos informáticos a nuestra regulación penal del Estado. Estudiaremos el tipo de delincuente que realiza la conducta antijurídica, descubriremos la importancia de la prevención del delito informático en nuestro país, así como la supervisión de las policías cibernéticas. En México el problema es la Delincuencia Organizada, y estos delitos se cometen por falta de una regulación adecuada, y por no contar con los recursos económicos que ellos tienen, pues son estos quienes explotan los desarrollos tecnológicos, en la trata de blancas, la explotación sexual, el turismo sexual y otros. Es vital que nuestros legisladores y los impartidores de justicia se encuentren cada vez más actualizados en este tipo de temas para dar seguridad jurídica a los gobernados. Compararemos a México y sus regulaciones federales y locales, y compararemos a otros países, respecto de los delitos Informáticos, cuáles han sido sus tratamientos y su efectividad. **Palabra clave**: Delito Informático, Delincuencia Organizada, Policía Informática.

ABSTRACT

This thesis is a dogmatic criminal legal analysis, by means of which we can then understand novel legally criminal figures, for which it was consulted to prestigious writers, which will shape their theories according to the computer crime, both in the Federal legislation such as the various States, with emphasis on the state. In the same way we will link the Computing with various human activities such as medicine, biology, genetics and many others, as well as the importance to the right, and his innovative branches as they are: the cyber law, the legal informatics, the right to the cybernetic information and legal links with other branches such as with the constitutional law, civil law, the copyright, the right to information, the banking law, and especially the criminal law, which is the level of analysis of this thesis, and it is in where is located the cybercrime. We develop a detailed description of the nature Of the computer crime and the framework that is interlinked with our criminal figures, where will be the legal property is state guardianship and protects, and by means of which laws it succeeds as it is the Constitution of the United Mexican States, secondary laws or regulations as are: the federal law of copyright, the industrial property law, the law of transparency and public access to government information, as well as the civil and penal codes federal and state civil procedural codes and federal and state criminal and the laws of the States that already analyzed the computer crime that we can serve as an analysis for the proposal of the incorporation of computer crime to our regulation of criminal law of the State. We check the offender that performs the unlawful behavior, and we will discover the importance that must have the prevention of computer crime in our country as well as the significance of their supervision the cyber police. We must not neglect that the current Mexico one of the big problems are the Organized Crime, and are precisely this kind of criminals who perform these offenses referred to in our analysis that to find that there are no regulations adequate or accurate or that has the economic resources such as the criminals are the most exploited these technological developments such as the trafficking in women, sexual exploitation, etc. In such virtue is necessary that our legislators, our judges are increasingly current on this kind of topics to provide more legal certainty for all the governed. Mexico will compare to its various local and federal regulations, and similarly with respect to other countries, for Computer crimes, and what have been their treatments and their effectiveness. **Keyword:** cybercrime, Organized Crime, cyber police.

INTRODUCCIÓN

En nuestro primer capítulo analizaremos aspectos fundamentales sobre la electrónica, la informática y la cibernética, explicaremos los componentes de la computadora; como son, el hardware, el monitor, cpu, teclado, mousse, etc; y, el software, que son todos los paquetes de programas para la computadora; discerniremos la importancia y la evolución del internet, así como los servicios que ofrece; como el correo electrónico, la información en línea y otros, se hará énfasis en la informática jurídica y su utilidad, en el mismo capítulo analizaremos las diversas regulaciones nacionales que contemplan los delitos informáticos.

En el capítulo dos ahondaremos en los sujetos que intervienen en el delito informático, los tipos de delincuentes que cometen este ilícito y las características de este tipo de delitos, haciendo énfasis en los delitos conocidos por las Naciones Unidas.

El capítulo tres es la parte toral de la presente tesis de grado, puesto que señalaremos qué bienes jurídicos se protegen en el Delito informático como son: el Derecho a la intimidad y la confidencialidad, el derecho a la información, el derecho al patrimonio y ahora uno de los más importantes el derecho a la seguridad nacional.

En el capítulo tres resaltaremos las legislaciones nacionales que contemplan los delitos informáticos, de igual forma nos acercaremos a algunas legislaciones en América Latina que también los contempla y se ampliara un poco más hacia el ámbito Internacional.

En el capítulo cuarto plantearemos nuestra investigación, basándonos en la necesidad de la protección de la información sensible que son el nombre, el domicilio, el origen racial, la preferencia sexual, las creencias religiosas; información que no puede, ni debe, ser procesada electrónicamente sin restricciones; y, por el otro lado, el manejo y registro de la información pública, cómo debe de ser clasificada y bajo qué criterios, lo anterior para proteger la seguridad pública, la vida de las personas, de su familia o patrimonio, por lo cual no deberá registrarse, ni serán obligados a proporcionar datos, tanto a personas físicas como morales.

La incorporación de los delitos informáticos al Código Penal del Estado de Michoacán. Sobre todo en algunos rubros no pretende el aumento de sanciones privativas de libertad, porque es conocido por todos nosotros que el aumento de las penas no desalienta la comisión del delito; lo que es la prevención general, estos delitos son facilísimos de cometer para los Hackers y los Crackers y muy difíciles de descubrir. Muchos de estos delitos son cometidos mediante la manipulación de los equipos de cómputo y son normalmente en acciones de

oportunidad del sujeto activo, lo que se intentará con la propuesta es la reparación del daño (justicia restaurativa) sobre todo cuando sean afectaciones patrimoniales, haciendo sabedor al delincuente que la reparación del daño que será indudablemente mayor, que el beneficio que haya obtenido de su conducta, para lograr que se limite, o que lo piense un poco más, antes de cometerla.

Otro aspecto relevante es la actualización a algunos delitos ya contemplados en nuestro código penal que ya se vinculan directamente con los delitos informáticos, como son la pornografía infantil y el turismo sexual, así como la importancia de tener una policía especializada en informática para la prevención y el combate de este tipo de ilícitos.

CAPÍTULO PRIMERO. ANTECEDENTES SOBRE LA INFORMÁTICA SUS CONCEPTOS Y SUS MÚLTIPLES CAMPOS DE ACCIÓN.

1.1 ANTECEDENTES DE LA INFORMÁTICA

En este apartado se analizaran todos los antecedentes y varias de las definiciones en el mundo y en México de conceptos importantes tales como la informática, la electrónica, la cibernética, el internet. La informática es una ciencia como el Derecho, para una mejor comprensión de los delitos informáticos.

1.1.1 HISTORIA DE LAS COMPUTADORAS

Durante siglos el hombre ha investigado las diversas formas para facilitar y simplificar su vida ya sea con herramientas o maquinarias, la historia de los aparatos para calcular y computar remonta a miles de años atrás.

El primer aparato de este estilo que existió fue y es el ábaco con una antigüedad de más de 5,000 años ya de origen perdido en el tiempo apareció en varias culturas. El código de Hammurabi da a conocer referencias del uso de este inteligente invento tanto en contratos, bonos, recibos, inventarios y transacciones de compra- venta.

La palabra "ábaco" es una palabra latina del griego "abax" o "abakon", que significa "superficie plana" o "tabla". Es posible que sea originado de la palabra semítica Abaq que significa "polvo". En China fue conocido como Suan Pan, en Japonés Soroban, en Corea Tschu Pan, en Vietnam Ban Tuan o Ban Tien, en Rusia Schoty, en Turquía Coulba y en Armenia Choreb.

Leonardo da Vinci (Italia, 15 de abril de 1452- Francia, 2 de mayo de 1519) trazó las ideas para una sumadora mecánica, había hecho anotaciones y diagramas sobre una maquina calculadora que mantenía una relación de 10:1 en sus ruedas registradoras de 13 dígitos.

Aún después de este ingenioso invento, persistían problemas en la realización de ciertas operaciones, por lo que John Napier (Edimburgo, 1550- 4 de abril de 1617) creó la Tabla de Logaritmos con lo que permitió realizar múltiples y divisiones de manera sencilla y rápida paro

aún con sus problemas por lo que fue inventada la Regla de cálculo, aparato más sencillo y ágil de usar pero muy inexacto a través de mediciones de longitudes entre dos reglas. Durante más de 200 años, la regla de cálculo es perfeccionada, transformándose en una calculadora de bolsillo, extremadamente móvil.

Blas Pascal (19 de junio de 1623- 19 de agosto de 1662), a los 18 años de edad creó una máquina capaz de realizar operaciones mediante un mecanismo de ruedas dentadas basadas en las ideas de Leonardo da Vinci, *"la cual fue conocida como la primer máquina calculadora de la historia, también desarrolló la teoría de las probabilidades, piedra angular de las matemáticas modernas. Con las limitaciones de la Pascalina a sumas y restas, Gottfried W. von Leibnitz mejoró esta máquina con la inserción de un cilindro con lo cual permitió que la Pascalina pudiera multiplicar dividir e incluso realizar raíces cuadradas".*[1]

Con la llegada de las máquinas de telar automáticas por Joseph Jackard en 1801 mediante tarjetas perforadas que guiaba a la maquinaria a realizar el mismo modelo una y otra vez sin perder detalle entre sí, siendo éste el inicio del sistema de las tarjetas perforadas y de automatización, con lo que permitió controlar por primera vez una máquina con instrucciones codificadas. Para 1823 Charles Babbage, matemático inglés y científico de la computación, *"con soporte del gobierno Inglés ideo una máquina denominada Maquina Diferencial capaz de ejecutar diversos tipos de operaciones, almacenar información y resolver todo tipo de problemas además de entregar el resultado impreso, pero siendo muy ambicioso para su época esta máquina jamás pudo terminarse por causas mecánicas causando cambio de diseño sin poder concordar la idea original y la terminación del apoyo del gobierno inglés*".[2]

Años después Charles Babbage ideó su Maquina Analítica, con lo que se podía idear operaciones más complejas de manera rápida además de guardar datos en un dispositivo interno tomando la idea de las tarjetas perforadas, siendo esta la base para la creación de las computadoras, pero aún así no pudo terminarse.

Los primeros y verdaderos inicios en lo que hoy conocemos como computadoras se debe a Herman Hollerith, miembro del cenco de los Estados Unidos de Norte América que

[1] Véase "La Historia de la Computación", 4 de Enero del 2013, h*ttp://www.cad.com.mx/historia_de_la_computacion.htm.*
[2] Véase "El Rincón Universitario", 4 de Enero de 2013, *http://www.emas.co.cl/categorias/informatica/historiacomp.htm.*

basado en la idea de las tarjetas perforadas realizó una máquina la cual podía guardar de manera automática el registro de las personas censadas mediante perforaciones en los rasgos de las personas conociéndose como Fotografías perforadas.

El primer paso se dio entre 1939 y 1944 con la subvención de IBM (Internacional Business Machines) que significa (máquinas de negocios internacionales) la Universidad de Harvard creó la Mark I de 16 metros de largo y 2,5 metros de alto, contenía un aproximado de 800.000 piezas y más de 800 Km. "*De cables eléctricos, la cual empleaba señales electromagnéticas para desplazar las partes mecánicas, su programación dependía de la idea inicial de las máquinas analíticas mediante una cinta perforada, esta máquina podía hacer cualquier tipo de operaciones aunque de una manera relativamente lenta debido a la complejidad de la maquinaria interna*".[3]

Dos años después fue creada la ENIAC (Electronic Numerical Integrator And Computer) por J.P.Eckert y J.W.Mauchly en la Universidad de Pensilvania Estados Unidos, *"conocida como la primer computadora electrónica de la historia, pesaba 30 toneladas y ocupaba un espacio de 450 m2, llenaba un cuarto de 6 metros por 12 metros y contenía 18.000 bulbos, tenía que programarse manualmente conectándola a 3 tableros que contenían más de 6000 interruptores. La ENIAC operaba con "uno decimal" y notablemente superior la MARK I, dando así el principio de una nueva era abarcando periodos determinados basados en las características del sistema físico o lógico conocidas como Generaciones dividiéndose en las siguientes*[4]:

La primer generación: Construidas entre 1950 y 1960 conocidas como las primeras máquinas comerciales, las cuales su estructura básica consistía con la llamada válvula al vació. Lo que facilito su funcionamiento y era capaz de realizar mil operaciones por segundo y almacenar hasta 20,000 posiciones.

La segunda generación: Construidas entre 1960 y 1965 su principal característica consistía en la introducción de elementos electrónicos básicos como el transistor el cual establecía el paso de corriente entre dos puntos, este tipo de tecnología marcó una gran pauta

[3] Véase "La Historia que llevo a construir la Primera Computadora", 2 de Enero del 2013, *http://www.monografias.com/trabajos14/histcomput/histcomput2.shtml#G*

[4] Véase "El Rincón Universitario", 4 de Enero de 2013, *http://www.emas.co.cl/categorias/informatica/historiacomp.htm*

en la creación de computadoras revolucionando la industria con el ahorro de energía y espacio además de la velocidad y rapidez de cálculo.

La tercera generación: Construidas entre 1965 a 1975 su funcionamiento y contracción se basaba en el uso de los circuitos integrados el cual podía abarcar hasta 20,000 componentes en 25 m2, lo que permitía que ésta pudiera abarcar menos espacio a comparación de sus antecesoras.

La cuarta generación: Construidas a partir de 1975 hasta nuestros días, se caracteriza esta generación por la integración de 60,000 componentes en un circuito integrado de 25 mm2, la aparición del microprocesador, la contracción de computadoras personales y microcomputadoras lo que dio origen a la expansión de las computadoras por el mundo, y la especialización de las aplicaciones de la informática lo que trajo consigo la llamada "inteligencia artificial", telecomunicaciones, tratamiento electrónico de las imágenes y base de datos.

La quinta generación: Fue un proyecto lanzado por Japón en los años 70s con el fin de elaborar computadoras con inteligencia artificial, un procesamiento paralelo y un nivel propio de lenguaje de máquina, el proyecto duró diez años sin poderse lograr.

1.2 CONCEPTOS DE LA ELECTRÓNICA, INFORMÁTICA Y CIBERNÉTICA

1.2.1 LA ELECTRÓNICA

Para poder entender la oposición esencial entre un delito informático y los conocidos como los delitos electrónicos, es necesario entender lo que es la Electrónica y qué es la informática, que consiste en: *"Parte de la ciencia que estudia los fenómenos que intervienen electrones en estado libre"*.[5] Lo cual prácticamente no dice nada, por lo que la electrónica como técnica: *"Es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacio, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos"*.[6]

[5] Diccionario de la Lengua Española**,** Editorial Planeta, México 1990, t 3, p. 461.
[6] Diccionario de la Lengua Española, Editorial Real Academia Española, Vigésimo Segunda Edición, España 2001, t 4, p. 590.

Para entender de una manera fácil en su funcionamiento dentro de un aparato electrónico se tiene que tomar en cuenta que el flujo de estos electrones genera corriente eléctrica y esta a su vez usada en dispositivos cambian la energía electrónica en calor, luz o movimiento, a lo que se conoce como Eléctrica, pero usada en dispositivos provistos de inteligencia surge lo que es una radio, una televisión y una computadora es conocida como Electrónica.

1.2.2 LA INFORMÁTICA

Siendo que los aparatos informáticos son electrónicos pero no necesariamente todos los aparatos electrónicos son informáticos, como el ejemplo de que una licuadora a comparación de una computadora. Ya siendo parte esencial el flujo de corriente eléctrica para transformarlo en otro tipo de energía de ambos, la palabra clave es el procesamiento de información, dando origen a la informática, siendo esta: *"una rama del saber humano que se ocupa de todo lo relacionado con las computadoras, su comportamiento, su diseño y desarrollo de todo tipo de programas de computadoras (desde los sistemas operativos hasta los más modestos programas de aplicación) operación y uso de las computadoras"*.[7]

Es una rama de la ingeniería que estudia el tratamiento de la información a través del uso de maquinas automáticas. Proviene del francés INFORMATIQUE que a su vez por la conjunción de las palabras información y AUTOMATIQUE, para dar idea de la automatización que se logra con los sistemas computacionales.

La informática es un extenso campo que incluye los fundamentos teóricos, el diseño, la programación y el uso de las computadoras (ordenadores) como instrumento de solución de problemas.

Esto puede ser comprendido como la interpretación y procesamiento lógico de los impulsos eléctricos de manera ordenada, por ejemplo, los cassettes, éstos poseen las cintas magnéticas, el cual su funcionamiento básicamente consistía en que a través de esta cinta plástica quedaba un registro magnético entre una combinación lógica y ordenada de cargas positivas y negativas por así decirlo, que en el tema de un audio cassettes estaban distribuidos

[7] Diccionario de Informática y Telecomunicaciones, Inglés-Español, Editorial Ariel S.A, Barcelona España 2001, p. 131.

según las vibraciones generadas por el sonido pero en el caso de dispositivos informáticos como lo son los disquetes o discos flexibles esta relación ordenada de cargas son comprendidos como ceros y unos el lenguaje vinario; están procesadas y comprendidas lógicas y matemáticamente a través de una computadora permitiendo reproducir o guardar información.

1.2.3 LA CIBERNÉTICA.

Cibernética: *"Del griego kuBEpvnTIkn: Piloto o el arte de pilotear un navío, aunque Platón la utilizo en la Republica con el significado de Arte de dirigir a los hombres o Arte de gobernar"*.[8]

Las investigaciones con propósitos militares a partir de la segunda Guerra Mundial propiciaron la creación del concepto de la Cibernética Moderna: como una ciencia de la comunicación y el control.

Otra forma de comprender a la Cibernética actual es como: *"Estudio de las analogías entre los sistemas de control y de comunicación de los seres vivos y los de las maquinas y en particular, el de las aplicaciones de los mecanismos de regulación biológicas a las tecnológicas"*.[9]

1.2.3.1 ORÍGENES DE LA CIBERNÉTICA

En 1948 el matemático norteamericano Norbert Wiener (1894-1964) en su obra *"Cibernética o el control y comunicación en animales y maquinas (Cybernetics, or control and communication in the animal and machina) publicada en 1948, el cual empleo el termino para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina"*.[10]

1.2.3.2 DIFERENCIA ENTRE CIBERNÉTICA Y LA INFORMÁTICA.

Un punto importante es resaltar la diferencia que existe entre la informática y la Cibernética que vistos de cierta manera parecerían que son similares, pero aunque guardan una relación entres las partes que lo componen no son iguales.

---

[8] Mateos Muñoz, Agustín, "*Compendio de Etimologías Greco-Latinas del Español*", Editorial Esfinge, Cuadragésima Sexta Edición, México 2007, p. 299.
[9] Diccionario de la Lengua Española, Ob. Cit, t 3, p. 370.
[10] Véase a "Norbert Wiener y el Origen de la Cibernética", 14 de Enero del 2013, *http://www.infoamerica.org/documentos_pdf/wiener2.pdf*.

La Cibernética es la ciencia que trata de explicar y dar solución a eventos de control y comunicación ya sean fenómenos acontecidos en la naturaleza, sociedad o humanos, de tal manera la informática busca desarrollar máquinas capaces de "Inteligencia Artificial", simular actividades y capacidades humanas como la robótica, la búsqueda de solución de problemas y la toma de decisiones por sí mismas, conocido como Heurística o Método Heurístico.

1.2.4 EL ORDENADOR Y SUS COMPONENTES

El concepto ordenador fue usado por el matemático Húngaro- Estadounidense John Von Newman (1903-1957) con el fin de simplificar su propia maquina que podía realizar cálculos.

La Computadora es: *"Una máquina electrónica análoga y digital, dotado de una memoria de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas"*.[11]

Entendido de otra manera una computadora es: *"Un dispositivo electrónico complejo que puede ser programado para recibir, almacenar, procesar, transmitir y presentar"*.[12]

Esta se compone de dos elementos esenciales, el SOFTWARE y el HARDWARE, parte importante para una computadora y relacionadas entre sí ya que una no puede existir sin la otra.

El Hardware son los componentes físicos y materiales, en conjunto o separados, electrónicos, electromecánicos o mixtos, que compone el equipo lógico e informático en una computadora.

El Software es la parte intangible de una computadora como un conjunto de instrucciones con las que el usuario y el sistema informativo interactúan para realizar determinadas tareas.

Las partes que componen a una computadora se dividen en 3:

[11] Diccionario de Informática y Telecomunicaciones, Inglés-Español, Editorial Ariel S.A, Barcelona España 2001, p. 412.
[12] Diccionario de Informática y Telecomunicaciones, Ob. Cit, p. 130.

1) Unidades de entrada.
2) Unidades de salida
3) Unidades de procesamiento, Almacenamiento o Memoria.

La unidad de Entrada. Esta constituida de todos aquellos dispositivos con los cuales se permite ingresar datos e información además del manejo de programas informáticos, estos se componen de: el teclado, el mouse (ratón), tablero digitalizado, lector de discos compactos (CD ROM, DVD), sistemas de lectores de tarjeta, unidades de almacenamiento (memorias USB Flash), reconocimiento de voz y unidades de disco.

Las unidades de salida son todos los dispositivos físicos en los cuales permite representar la información susceptible a ser apreciados, estos son pantallas, bocinas, impresoras de papel en tres dimensiones.

Las unidades de procesamiento, Almacenamiento o Memoria. Es aquella en la que la información es almacenada analizada y procesada, consisten en: discos duros, (Hard Disck Drive) denominado disco duro, procesadores (micro procesadores), unidades de almacenamiento (tarjetas de memoria, memorias USB flash o SD).

Dentro de la capacitación de almacenamiento existen dos tipos de memoria la primera llamada RAM (Random Acceses Memory) cuya traducción es (acceso de memoria aleatoria) la cual consta de pequeñas celdas en un chip que almacenan de forma temporal gran parte de la información, entre mayor memoria RAM tenga una computadora mayor velocidad operará. La otra memoria es la ROM (Read Only Memory) cuya traducción es (memoria sólo de lectura), consta en memoria semiconductora de lectura utilizada para almacenar datos que nunca necesitan modificarse.

1.2.5 EL INTERNET

Para poder entender los delitos informáticos es necesario poder entender lo que es el internet, que es un conjunto de servidores conectados entre sí mediante un sistema maestro de computadoras dentro de una red alrededor de todo el mundo.

1.2.5.1 HISTORIA DE LA INTERNET EN EL MUNDO

La internet fue concebido por el Ministerio de Defensa de los Estados Unidos de América con el fin de lograr crear una red de computadoras interconectadas que no dependiera de una computadora central con el fin de que en ataques la información no comprometida se encontrara protegida en su totalidad o en parte, así como en la funcionalidad de la red que se vería comprometida al destruir el servidor central.

"En 1960 empezó a desarrollarse un sistema de red en que las computadoras interconectadas no dependieran de un servidor central sino que cada computadora actuase de manera interdependiente de las otras, con lo que nación la idea de ARPANET".[13] (Advanced Research Projects Agency Network). *"Con lo cual para el funcionamiento de esta red fue necesario la creación de procesadores especiales denominados Procesadores de Masaje de Interfaz (IMP en sus siglas en inglés) el cual el primer procesador de este tipo entro en funcionamiento el 1 de Agosto de 1969 en la Universidad de California de los Ángeles E.U.A, con una computadora Honetwell 516 con una memoria de 12 MB de memoria".*[14] *"Extendiéndose a otras Universidades del País dando origen a ARPANET. Para 1972 se habían instalado 37 Procesadores de Mensaje de Interfaz. ARPANET funcionaba con un programa denominado Network Control Protocol (NPC)".*[15] Facilitando su uso debido a que era compatible con diversas computadoras y programas operativos creciendo de tal forma que los propósitos militares del ministerio de defensa fueron cambiados por los fines científicos y educativos de las Universidades en los que se encontraba ya instalado.

Para 1980 el NPC fue sustituido por TCP/IP un programa más eficiente el cual convertía la información en pequeños paquetes los cuales pueden ser enviados a diversos puntos con base a su dirección a través de diferentes puntos de enlace de internet y la computadora de destino, en este mismo año ARPANET se desligó por completo de sus objetivos militares a los que fue diseñado.

---

[13] Rojas Armandi, Víctor Manuel, "*El Uso de la Internet en el Derecho*", Segunda Edición, Editorial Oxford, México 2001, p. 2.

[14] Ídem.

[15] Véase "La Historia de Arpanet", 15 de Enero del 2013, *http://es.wikipedia.org/w/index.php?title=Internet&oldid=67768692*.

"En 1986 se fundó la NSFNET (National Science Foundation´s Network) financiada por el gobierno de los Estados Unidos de América creando diferentes líneas de enlace para internet facilitando la transferencia de datos dando lugar a la expansión de la internet fuera del país, para 1995 NSFNET internet crear una política de uso científico y no comercial para la internet lo cual no fue aplicado debido a la privatización de la internet expendiendo su uso a niveles comerciales".[16]

1.2.5.2 HISTORIA DE LA INTERNET EN MÉXICO

Los Orígenes de la internet en México se remontan a 1986 cuando el Tecnológico de Monterrey campus Monterrey que por medio de la red BINET ya recibía información, logrando para el 15 de junio de 1987 la primera conexión permanente al mismo sistema. En octubre de 1986 se integró al sistema BITNET en la Universidad Nacional Autónoma de México. *"El 28 de febrero de 1989 el Tecnológico de Monterrey campus Monterrey se convirtió en la primera institución Mexicana que logro establecer un enlace de internet mediante una red analógica de cinco hilos a una velocidad de 9600 bits por segundo, este acceso a internet se estableció mediante un enlace a la escuela de medicina de la Universidad de Texas, en San Antonio E.U.A., para 1989 ya se disponían de tres líneas de acceso y estableció el primer nodo de internet en México y se dispuso el primer nombre de servidor para el .mx".*[17]

Una segunda conexión establecida con éxito en México fue creado por la Universidad Nacional Autónoma de México mediante el acceso a Internet entre el Instituto de Astronomía en la ciudad de México y (NCAR) el Centro Nacional de Investigación Atmosférica EE.UU. vía satelital a 56 kbp.

La tercera institución en conseguir conexión a internet fue el Tecnológico de Monterrey campus estado de México y a finales de los 80`s e inicios de los 90`s las principales instituciones educativas en el país adoptaron medidas para establecer alguna ruta de acceso hacia las redes de información electrónica, con lo que surgieron tres tendencias:

---

[16] Rojas Armandi, Víctor Manuel, Ob. Cit, p. 3.

[17] Gutiérrez Cortés, Fernando y López, Carlos Enrique "Una Década de Internet en México", Revista Mexicana de Comunicación, núm. 56, Octubre-Diciembre 1998, 16 de Enero del 2013, *http://www.cem.itesm/dacs/buendia/rmc56/internet.html.*

a) La primera consistió en todas aquellas instituciones educativas que se afiliaron y lograron establecer un acceso a internet a través de la Universidad Nacional Autónoma de México o el Tecnológico de Monterrey, los que establecieron un enlace con el ITESM (Instituto Tecnológico de Estudios Superiores en Monterrey), fueron la Universidad de las Américas en Cholula Puebla; el ITESO (Instituto Tecnológico y Estudios Superiores de Occidente) en Guadalajara Jalisco, estableciendo servicios de correo electrónico, transferencia de datos FTP y transferencia a distancia a una velocidad de 9600 bits por segundo, con el paso del tiempo se afiliaron al acceso de internet del ITAM (Instituto Tecnológico Autónomo de México) fueron el Colegio de postgrados de la Universidad de Chilpancingo en el Estado de México, el centro de Investigación de Química Aplicada en Saltillo Coahuila y el Laboratorio Nacional de informática Avanzada en Xalapa y la Universidad de Guadalajara pudo conectarse a través de la UNAM (Universidad Nacional Autónoma de México).

b) Los segundos fueron aquellas universidades que pudieron establecer una conexión a internet mediante una academia de los Estados Unidos, en la cual se encontraba la Universidad de Guadalajara enlazada con la Universidad de California en Los Ángeles mediante una línea privada de cuatro hilos a una velocidad de 9600 bits por segundo.

C) Los terceros fueron aquellas universidades que se afiliaron a un sistema alternativo de redes de información electrónica como el Tecnológico de Mexicali con el BESTNET, pero con los adelantos en las tecnologías no pasó mucho tiempo en que cambiara sus sistemas a otras redes por necesidad.

Comenzando los 90`s fue creado el organismo RED-MEX constituido por diversas instituciones académicas que se dedicaba a discutir políticas, estatutos y procedimientos con el fin de reglamentar el desarrollo de las redes de comunicación electrónica en México.

"El 20 de enero de 1992 en la universidad de Guadalajara y por iniciativa del ITESM Universidad de las Américas ITESO, Colegio de Postgrados, LANIA, CIQA, Universidad de Guanajuato, Universidad

de Veracruz, Instituto de Ecología, Universidad Iberoamericana e Instituto de Mexicali, se crea MEX-net, el cual se encargaría de decodificar, propiciar y contribuir en el desarrollo de internet en México". [18]

Durante 1983 y 1993 el uso de la internet era exclusivamente con fines académicos y de investigación mediante las principales instituciones de educación superior y centros de investigación y que operaron como únicos proveedores de acceso a internet, con lo que el 18 de enero de 1993 el (CONACYT) Consejo Nacional de Ciencia y Tecnología fue la primer institución pública en conseguir un enlace a Internet a través del Centro nacional de Investigación Atmosférica en E.U.A. y en este mismo año la Universidad Autónoma Metropolitana y el Instituto Tecnológico Autónomo de México, lograron intercambiar información entre dos redes diferentes.

Para 1994 se logró fusionar las redes de MEX-net y de CONACYT con lo que surgió la Red Tecnológica nacional que alcanzó un enlace de 2 Mbps y en este mismo año con el surgimiento de la (WWW) iniciaron los usos comerciales de la Internet y la elaboración de los primeros dominios (.mx) y (.edu .mx), y para los finales de este mismo año bajo el dominio (.mx) estaban declaradas 44 instituciones académicas, 5 empresas en (.com.mx9 y una institución bajo (.gob .mx), se habían asignado 150 direcciones de IP las cuales 50 eran clase B y 100 clase C y se creó un BackBone nacional incorporando diversas instituciones educativas y las primeras empresas mexicanas interesadas en Internet.

"En 1995 el número de servidores (WWW) aumento 160% y surgió la segunda etapa de desarrollo de la Internet en México, siendo para octubre del mismo año que los dominios bajo (.mx) ascendió a 100 dejando por detrás a los dominios bajo (.edu .mx) con lo que un mes después se anunció la elaboración del Centro de Información de Redes de México (NIC-México) la cual era la encargada de administrar y coordinar los recursos de la Internet en México".[19]

Actualmente el ITESM campus Monterrey y NIC-México son los responsables de asignar y administrar los nombres de los dominios ubicados bajo la designación (.mx), la UNAM, IPN y el ITESM contribuyeron en establecer los fundamentos de una cultura en la

[18] Véase Sociedad Internet de México, "Historia de la Internet En México", 17 de Enero del 2013, *http://www.isocmex.org.mx/historia.html.*

[19] Véase Corporativo Nic-México, "Historia de Nic-México", 17de Enero del 2013, *http://www.nic.mx/es/NicMéxico.Historia.*

red además de contribuir en la capacitación en el desarrollo de sitios (WWW) del PRI, PRD y PAN, en la seguridad de computadoras para empresas con el fin de disminuir costos. *"Además, siete de las principales instituciones educativas del país se han encargado de promover y coordinar (INTERNET 2), construido con 202 Universidades en colaboración con las industrias privadas y el gobierno, con fines científicos y tecnológicos en el país donde la UNAM es el Centro de Operaciones de la Red Nacional de INTERNET 2 cuya tarea es asegurar la alta disponibilidad de la red y el ágil reconocimiento de fallas y degradación del servicio*".[20]

1.2.5.3 SERVICIOS DEL INTERNET

Al convertirse la Internet en un sistema abierto, éste realiza dos tareas importantes la primera como medio de comunicación y la segunda mediante la información.

COMO MEDIO DE COMUNICACIÓN, la red entre computadoras permite la comunicación entre sí y entre los usuarios realizada mediante cable telefónico o conexión por línea de velocidad o banda ancha DSL, debido a esto cualquier computadora puede conectarse a Internet sólo debe contar con el respectivo MODEM y un servidor de un proveedor de internet el cual debe tener entrada a la espina dorsal del mismo Internet (backbone). Los medios de comunicación más comunes en la Internet se localizan en el Correo Electrónico (e-mail), la comunicación a través de foros de discusión, servidores de lista y mensajeros instantáneos.

El correo electrónico. Permite el libre intercambio de información y datos a través de un servicio de red por medio de sistemas de comunicación electrónicos, comparado con el correo ordinario, es más barato y rápido debido a que en cuestión de segundos pueden ser enviados datos e información, otra ventaja del correo electrónico a comparación de los medios de comunicación convencionales como el teléfono radica en que este necesita relación directa entre personas, el correo electrónico puede ser enviada la información y ser revisado en otro momento, a diferencia con el Fax que éste necesita que el documento tiene que ser impreso y en caso de corrección deberá ser escaneado o en su caso mecanografiado y corregirlo, el correo electrónico por otro lado los datos e información transferida puede ser modificada a través de un procesador de palabras (Word, TXT).

[20] Téllez Valdés, Julio, *"Derecho Informático"*, Tercera Edición, Editorial Mc-Graw Hill, México 2003, p. 85.

COMO COMUNICACIÓN MEDIANTE FOROS DE DISCUSIÓN, se lleva a cabo a través de páginas especialistas en el que se sostiene un contacto directo entre las personas á través de pregunta y respuesta.

MENSAJERÍA INSTANTÁNEA, esta comunicación puede ser considerada como de las más eficientes y rápidas en la Internet, depende de un servidor y programa especializado que permite entablar una conversación escrita (Chat) directa con otro usuario, a comparación con el teléfono, los mensajeros instantáneos comparten las mismas cualidades entre sí como la comunicación directa entre personas que poseen el mismo servicio pero a diferencia los mensajeros instantáneos en páginas Web permiten establecer y sostener conversación con personas desconocidas.

COMO MEDIO DE INFORMACIÓN, la Internet se considera como una gran biblioteca por su extenso contenido de documentos considerado como el más inmenso y completo del mundo en el cual cualquier persona tiene acceso desde cualquier terminal y desde cualquier lugar del mundo. A diferencia de una biblioteca las autoridades de la misma controlan el manejo de la adquisición de nuevos libros o documentos, en la Internet los usuarios pueden introducir sus documentos de manera libre, lo que justifica el aumento del contenido de la información disponible, pero el principal problema radica en la veracidad der alguna de esta información derivada de la libre contribución de los usuarios.

La información en la Internet pasa de una computadora a otra sin saber la ruta que esta deberá seguir con lo cual es imposible poner cuotas a su uso por la información consultadas, por tal razón el costo del uso de la Internet se dividen entre todos los usuarios, de tal forma solo son impuestas cuotas mínimas a los usuarios a través de los servidores de acceso a internet.

1.2.5.4 ORGANIZACIÓN DE LA INTERNET

Consta básicamente de una organización no jerarquizada y que todas las computadoras y sistemas de redes con capacidad de entrada a la información así como de los servicios disponibles en internet, toda esta información y servicio no se encuentran depositados en una computadora o red determinada sino solo transmitidas entre varias

computadoras. Tampoco es posible perder la información debido a que siempre es posible encontrar otra ruta para acceder a la información perdida.

Una de las características importantes de la Internet es la Autorregulación, consta de un programa denominado IP con los que funciona cada computadora que a su vez enlazada entre sí, la información es dividida en pequeños bloques los cuales son enviados por canales diferentes que al final son reunidos y armados en las computadoras receptoras, con lo que no existe una comunicación directa entre las computadoras a diferencia de la línea telefónica en la que existe un servidor central en la que dependen las comunicaciones entre teléfonos, pero donde la comunicación es directa entre las partes.

1.2.5.5 DENOMINACIÓN

Cada servicio de información cuenta con sus propias direcciones con el fin de entrar de manera fácil y rápida a través de la Internet, *"cada dirección recibe el nombre de dominios. (WWW, World Wide Web) en sus siglas en inglés, creado en 1989 por las investigaciones del Sir Timothy "Tim" John Berners-Lee ante el CERN (Centro Europeo para la investigación Nuclear), es un sistema que permite extraer elementos de información llamados "documentos" o "páginas web", los cuales necesitan de un programa especial para poder ser leídas, estos programas se conocen como exploradores o navegadores ejemplo: Amya (World Wide Web Consortium), internet Explores (Microsoft), Netscape Navigator (Netscape Communications), Opera (Opera Software)"*[21].

La funcionalidad elemental de la Web se basa en tres estándares básicos:

1. (URL), Localizador Uniforme de Recursos, que detalla a cada página de información se asocia a una única y en dónde encontrarla.
2. (HTTP), Protocolo de transferencia de Hipertexto que especifica cómo el navegador y el servidor intercambian información en forma de peticiones y respuestas.
3. (HTML), Lenguaje de Marcación de Hipertextos un método para codificar la información de los documentos y sus enlaces

[21] Pozo, Juan R, "Breve Historia de la World Wide Web", 21 de Enero del 2013, *http://html.conclase.net/articulos/historia.*

Puede señalar a una (web) como una página, sitio o agregado de sitios que abastecen información por los medios explicados, o a la (web), que es la enorme e interconectada red disponible prácticamente en todos los sitios de la Internet, ejemplo: servicio: //nombre del sistema. Dominio. Nivel más alto. Código o país/ ruta/ archivo; Facultad de Derecho UNAM: *http://www.Derecho.unam.mx*

Una dirección de Internet puede tener más de una sólo sección, un ejemplo es la dirección de la enciclopedia Wikipedia: WIKIPEDIA Enciclopedia libre: *http://es.wikipedia.org/wik/portada*

El nivel de dominio más alto es parte importante en una dirección debido a que menciona el tipo de organización a la que pertenece el dominio, ejemplo de las más comunes:

.com	Organización Comerciales
.edu	Universidades y otras Instituciones de Enseñanza
.gob	Organizaciones Estatales
.net	Sistema de la Red y Administración de Internet
.org	Otras Organizaciones

Otra parte de la dirección en especial para los portales externamente de los Estados Unidos es el manejo de códigos referentes al país de origen por ejemplo:

Portal	País	Portal	País	Portal	País	Portal	País
.at	Austria	.dk	Dinamarca	.in	India	.pl	Polonia
.au	Australia	.es	España	.it	Italia	.pt	Portugal
.be	Bélgica	.eu	Unión Europea	.jp	Japón	.ro	Rumania
.br	Brasil	.fr	Francia	.kr	Corea	.se	Suecia
.ca	Canadá	.gr	Grecia	.lu	Luxemburgo	.sk	Eslovaquia
.ch	Suiza	.hk	Hong Kong	.mx	México	.sl	Eslovenia
.cn	China	.hu	Hungría	.nl	Holanda	.tr	Turquía
.cz	Republica Checa	.ie	Irlanda	.no	Noruega	.us	E.U.A
.de	Alemania	.il	Israel	.nz	Nueva Zelanda	.uk	Gran Bretaña

1.2.5.6 DIRECCIÓN DE CORREO ELECTRÓNICO (e-mail)

Contiene el nombre del usuario seleccionado por el mismo usuario o el prestador del servicio del correo, después se pone el símbolo @ (arroba) que en inglés significa "en", por último el nombre del servidor, el domicilio y el nivel más elevado si es que éste lo tuviera, por ejemplo: Usuario @ servidor. Nivel más levado. Código del País.

1.3. CAMPOS DE ACCIÓN DE LA INFORMÁTICA

La información se ha utilizado en todas las ciencias, disciplinas y artes de la humanidad sirviéndoles para alcanzar sus objetivos, a continuación haré referencia de algunas de ellas.

1.3.1. LA INFORMÁTICA EN LAS CIENCIAS NATURALES

En los últimos años con el incremento de la computación y la Internet se ha generalizado su uso en diferentes áreas del conocimiento humano y es difícil encontrar una rama de la ciencia en donde no se haga el uso de la informática en cualquier sentido y la invasión de las computadoras en todas las actividades del ser humano que ha traído como consecuencia beneficios que en otras épocas se consideraban sólo dentro de la imaginación humana.

1.3.1.1 LA INFORMÁTICA EN LA MEDICINA, EN LA BIOLOGÍA Y EN LA GENÉTICA.

LA MEDICINA

Ha sido de las más beneficiadas por la informática, facilitando los procesos de investigación y el control en cada paciente, tratamiento de datos históricos y experiencias sintomáticas y con ello la creación de máquinas capaces de analizar y realizar diagnósticos certeros, además de realizar intervenciones quirúrgicas o asistencia a distancia mediante la robótica y la Internet.

LA BIOLOGÍA

Es *"La Ciencia que trata de los seres vivos"*.[22] Actualmente tiene un enfoque sistemático y los beneficios de las nuevas tecnologías han sido gigantes y complicadas de mencionar todas a la vez, tanto que han abarcado beneficios en el almacenamiento y tratamiento de información, comunicación y experimentación mediante la simulación virtual.

[22] Diccionario de la Lengua Española, Ob. Cit, t 3, p. 216.

LA GENÉTICA

Iniciada en los años 70´s con las primeras investigaciones sobre la información genética de los organismos, ha generado un incremento en la información cuantitativa que ha sido posible manejar y decodificar tal información, dando como resultados el desciframiento y entendimiento de las secuencias genéticas enteras o parciales de organismos, con lo que en esa misma época se decidió crear los primeros bancos de datos públicos sobre información genética. *"El primero en surgir fue Laboratorio Europeo de Biología a Molecular (European Molecular Biology Laboratory). En julio de 1974 con un tratado intergubernamental de nueve países europeos más Israel y que para el año 2006 sumaban ya 19 países miembros, con sede en Hiedelberg Alemania, cuenta con 4 sub-sedes conectadas entre sí vía Internet las cuales son: Hinxton en Reino Unido, Grenoble en Francia bajo con el Instituto de Bioinformática Europeo, Hamburgo en Alemania y Monterotondo Italia. Sus Investigaciones abarcan el análisis experimental de la organización Biología molecular de los organismos, Biología Computacional y la Biología de sistemas, todo esto apoyado por el desarrollo que permite un avance a las tecnologías disponibles para la comunidad científica y la red incorporada entre ellas. Uno de los principales logros de esta institución fue en 1995 al ser el primero en analizar y descifrar el código genético de la mosca de la fruta por Christiane Nusslein-Vollhard y Erich Wieschaus lo cual les concedieron el premio Nobel de Medicina en ese mismo año".* [23]

"Otro segundo centro en surgir con estos mismos propósitos fuel Elgen Bank en los E.U.A. que en 1987 se transformó en el International Nucleotide Sequence Data base Collaboration. El propósito de todas estas bases de datos es mantenerla a disposición de las instituciones educativas y el público en general de la manera más rápida en la que sea posible, ésta colección de datos se considera que ya ha superado los 100 Gigabytes (cien millones de bites) y se siguen sumando por mes más de 3 millones de secuencias genéticas nuevas". [24]

[23] Véase EMBL Heidelberg**,** "European Molecular Biology Laboratory", 22 de Enero del 2013, *http://www.emblheidelberg.de/*

[24] Véase "International Nucleotide Sequence Database Collaboration", 23 de Enero del 2013, *http://www.ncbi.nlm.nih.gov/genbank/collab/country.*

1.3.1.2 LA INFORMÁTICA EN LA QUÍMICA Y FÍSICA

Estas dos ciencias han evolucionado de manera significativa con la llegada de la informática a sus campos de estudio haciendo que éstas puedan ser presentadas de manera rápida y certera, realizando cálculos y simulaciones nunca antes imaginaba que antes eran tardadas o en muchas ocasiones imposibles de hacer para unas sola persona, además de que con la llegada de los medios electrónicos han surgido nuevas ramas en estas ciencias como la Física o Química Cuántica donde interviene la información para simular lo sucedido en el reino de lo inimaginable.

1.3.2 LA INFORMÁTICA EN LAS CIENCIAS SOCIALES

Con la llegada de la informática y con el internet han evolucionado los campos de estudios y el uso de la informática como herramienta crucial para sus actividades que han creado nuevos conocimientos para diversas ciencias sociales, tales como las que a continuación se mencionan:

1.3.2.1 LA INFORMÁTICA EN LA ECONOMÍA Y ADMINISTRACIÓN

La informática dentro der la Administración y la Economía ha tenido una gran aceptación causando que en todas sus ramas han generado beneficios en la realización de cálculos administrativos, contables y financieros; control de inversiones, nóminas: automatización y evaluación de proyectos; operaciones comerciales, financieras mediante redes y la automatización de las bolsas de valores del mundo.

1.3.2.2 LA INFORMÁTICA EN EL DISEÑO, INGENIERÍAS Y MANUFACTURAS

En cuanto a la informática con esas áreas ha traído automatización de procesos, facilidad en las actividades lo que trae como consecuencia que la aplicación de la informática en las diferentes fases de la producción lo que permite la producción en masa y a la vez reducir costos.

1.3.2.3 LA INFORMÁTICA EN LA EDUCACIÓN

La informática puede influir en la manera en que las cosas pueden ser enseñadas y aprendidas, por lo que el uso de la tecnología puede ser destinada con fines didácticos en las instituciones educativas, esto es conocido como Informática Educativa.

Tenemos que recordar que los objetivos de un sistema educativo es el desarrollo del alumno en su expresión oral y escrita, comprensión de lectura, capacitación para argumentar y entender; en un segundo plano el alumno deberá aprender a desarrollar un razonamiento lógico-matemático para la solución de problemas y desarrollar su potencial artístico, todo esto con el fin de que empleé sus conocimientos para entender el mundo y con ello para transformarlo preparando a los alumnos para que al salir de las instituciones educativas sean personas preparadas como ciudadanos consientes de la realidad y preparados para enfrentarla.

Con la entrada de los medios electrónicos para la educación se da un cambio en la forma de enseñanza debido a que presenta ventajas significativas en comparación a los medios de la enseñanza tradicional. El alumno presenta mayor atención ante la forma en que se presenta la información, menos aburrida o tediosa y más dinámica, y trae como consecuencia el aprendizaje y la enseñanza de manera fácil y rápida, se proporciona información detallada debido que en los recursos educativos como la Multimedia, como su nombre dice se presenta la combinación de textos, medios audiovisuales, medios interactivos, animaciones, audio, video analógico o video digital; las cuales no podrían ser presentadas en muchos casos por medios tradicionales o en aulas convencionales; ahorro de tiempo y recursos para el proceso de aprendizaje y enseñanza, los alumnos pueden aprender por su cuenta y en casa después de las horas de clases para complementar sus estudios.

Los medios actuales de la informática Educativa que facilita el aprendizaje se presentan de muchas formas entre las cuales encuentran como las básicas:

- Simulación informática.
- Juegos interactivos con contenido educativo.
- Recursos multimedia.
- Bibliotecas virtuales y libros electrónicos (e-books).

Aunque estos medios han sido en muchos casos analizados y en muchos de ellas presentan un verdadero método de enseñanza práctica que han mostrado resultados positivos, no muchas personas lo consideran un medio de enseñanza real, sino como un atajo tramposo a la educación o un sustituto al trabajo docente, con lo que prefieren inclinarse a los anteriores métodos de enseñanza con lo que privan a los alumnos de estas tecnologías, creciendo la brecha de lo que se conoce como Analfabetismo Tecnológico.

Uno de los serios problemas que se enfrentan muchas instituciones educativas es la presión que se ejerce con la apertura de los mercados lo que trae como consecuencia que los padres de familia presionen a las instituciones educativas a adquirir equipos de cómputo evitando atrasarse en la ola tecnológica y éstas al no perder alumnos y prestigio adquieren equipos de cómputo y audio visuales a toda costa y no se enrocan en la calidad educativa sólo en la cantidad, presentando a los alumnos deficiencias en su aprendizaje al seguir esta tendencia tecnológica. Con lo que las instituciones educativas se tienen que enfocar en tres puntos importantes:

EQUIPOS DE CÓMPUTO. En ocasiones por adquirir prestigio y alumnos las instituciones educativas adquieren sistemas de cómputo sólo para satisfacer las exigencias del mercado y no se enfocan en la calidad de los sistemas, en muchos casos se adquieren sistemas de cómputo ya sean muy básicos o muy complejos de manejar para los alumnos y profesores, por lo que las instituciones educativas se tienen que preocupar por adquirir equipo de cómputo especializado y compatible con la mayoría de los programas especializados en la educación o equipos adicionales para la enseñanza y aprendizaje.

SISTEMAS OPERATIVOS. En muchas ocasiones no se toma en cuenta este factor debido a que se cree que los sistemas operativos incorporados en los sistemas de cómputo son óptimos y en muchos casos éstos no son compatibles con programas o equipos educativos enfocados para la enseñanza, además de presentar complicaciones para los alumnos y profesores para realizar estos fines; por ejemplo en los equipos de cómputo convencionales se incluyen sistemas operativos básicos enfocados a las necesidades de las personas como navegadores y uno de la Internet, procesadores de textos e imagen, así como reproductores multimedia, que en muchas ocasiones no son compatibles con fines didácticos que se les

quiere dar a la informática como herramienta y en muchas ocasiones están de más en los equipos informáticos. Lo que las Instituciones educativas tienen que tener cuidado y adquirir sistemas operativos especializados en satisfacer sus necesidades tanto administrativas como educativas.

LOS PROGRAMAS (SOFTWARE). Muchas Instituciones educativas optan por adquirir Enciclopedias Generales en Discos Compactos (CD) y se piensa que con eso es suficiente o bien adquiere programas considerados educativos, los cuales no son enfocados en la red correspondiente a la de los alumnos o a la calidad y cantidad de enseñanza a tratar, y toda institución educativa tiene que ser cuidadosa en adquirir programas especializados en los temas para grado y edad de los alumnos con el fin de optimizar el aprendizaje. Otro problema que en muchas instituciones educativas sólo se enfocan a la enseñanza del uso de la computadora y del sistema básico que éstas ofrecen con lo que para ellas mantiene su prestigio pero no se optimiza a la informática como la herramienta dedicada en la que se pretende convertir.

1.3.2.3 LA INFORMÁTICA Y LA GUERRA

En los conflictos bélicos, siempre se ha buscado conseguir la superioridad de cualquier tipo en contra del enemigo y con ello han surgido los mayores avances en la tecnología e informática ya sea en el campo de las comunicaciones o en general en cualquier área de las ciencias humanas. La industria militar utiliza la informática, como medio de almacenamiento y procesamiento de datos, inteligencia artificial de combate, estrategia y toma rápida de decisiones así como control y seguridad.

1.3.3 LA INFORMÁTICA EN EL DERECHO

Como hemos visto los recientes adelantos tecnológicos en las ciencias tanto sociales como naturales han generado un gran cambio en forma y su esencia, haciéndolas más fáciles de realizar y como consecuencia logrando grandes avances en sus respectivos campos de estudio, por lo que el Derecho no bebe permanecer ajeno a estos adelantos tecnológicos t responden a los nuevos y complejos problemas que se le plantean.

La ciencia del Derecho no puede dejar pasar esta oportunidad y la relación existente entre la Informática y el Derecho no puede ser analizado sólo desde un punto de vista ya que la informática representa un gran campo de técnicas y conocimientos en la actualidad, y que también debemos tomar en cuenta que ésta no se quedará estancada y en un futuro seguir creciendo.

También hay que tomar en cuenta que los constantes problemas que surgen con las nuevas tecnologías a estudiar no siempre son tan novedosos, sino son problemas ya existentes, sólo realizados de nuevas formas con las tecnologías, con lo que se han creado otras ramas o denominaciones para poder dar solución y entendimiento a estos problemas y si duda a los beneficios como las siguientes:

1.3.3.1 DERECHO INFORMÁTICO

Se puede hablar de los primeros señalamientos respecto del Derecho Informático más claro en la obra de Norbert Wiener *"denominada Cibernética y Sociedad (The Human Use of Human Beings: Cybernetics and Society) que, en su Capítulo IV, hace referencia a la influencia de la cibernética con los fenómenos sociales incluyendo al Derecho y esta relación se da a través de la comunicación".* [25]

Entendemos al Derecho en su forma más pura y simple como: *"El conjunto de normas jurídicas que tienen por objeto regular la conducta humana. Y a la Informática como un: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".* [26]

Por lo tanto se podría entender en este caso que el derecho Informático, está enfocado únicamente a una protección de los datos informáticos o la información concentrada en medios magnéticos o digitales, tenemos que recordar, que anteriormente la informática fue enfocada originalmente a los cálculos matemáticos, pero después ésta se enfocó también en el campo de la lingüística, lo que trajo consigo nuevos cambios y ventajas, sin contar los nuevos problemas que surgieron con este adelanto.

---

[25] Wiener, Norbert, *"The Human Use of Human Beings: Cybernetics and Society"*, 24 de Enero del 2013, *http://biblioteca.universia.net/html_bura/ficha/params/titlethehumanuseofhumanbeingscyberneticsandsocietyn/id/37815461.html*

[26] Diccionario de la Lengua Española, Editorial Real Academia Española, Vigésimo Segunda Edición, España 2001, t 6, p. 863.

1.3.3.2 DERECHO A LA INFORMÁTICA Y A LA INFORMACIÓN

Bajo este tenor el Tratadista Argentino Carlos M. Corres denomina: *"Derecho a la Información, en obra el Derecho Informático como: La Teoría Jurídica de la Información"*.[27] Donde en 1987 *"basado en las teorías francesas de esa época en especial de Pirre Catála, donde ya tiene marcado un objeto de estudio, el cual es la información como una mercancía, en donde Pierre Catála sostiene que ésta Información tiene un valor patrimonial y éste es susceptible de apropiación. Y se hace la distinción de Derecho sobre la Información y Derecho a la Información, donde el primero señala a la información referente a datos personales las cuales únicamente concierten a ellos mismos, y que son objeto de protección y el segundo que se contrapone con el primero donde se da acceso libre a información pública desde que ésta se haga pública"*.[28]

Surge el problema de ubicar al Derecho Informático, en el derecho Público o Privado; en especial en Francia es un derecho público regulado por leyes especiales desde la Ley de Comunicación del 9 de Enero de 1978, aunque en esa época y basada en la protección única de datos, este Derecho estaba más orientado a un Derecho Privado.

El tratadista Argentino Herminio Tomás Azpilicueta, en su obra Derecho Informático, señala que: *"el derecho informático puede estar ubicado dentro del Derecho Civil y Comercial sin problema alguno bajo los principios tradicionales de la responsabilidad civil, contractual y delincuencial, bajo el derecho Administrativo debido a la materia técnica del mercado público en la informática, dentro del Derecho Internacional debido a las determinaciones de jurisdicciones aplicables a los contratos internacionales, así como en el Derecho de Comercio Exterior bajo estas mismas causas. Otras ramas en las que señala son el Derecho de Trabajo, Derecho Fiscal y el Derecho Procesal"*[29].

La relación del Derecho y la Informática así como los avances continuos en las tecnologías ha impactado cada una de las ramas del Derecho desde extraordinarios beneficios hasta nuevos retos, por lo que se le puede decir que el Derecho Informático es interdisciplinario, por lo que puede ser ubicada en una sola rama del Derecho exclusivamente.

---

[27] Correa, Carlos, *"Derecho Informático"*, Editorial Desalma, Buenos Aires Argentina 1999, p. 287.
[28] Ibídem, p. 288 y 289.
[29] Azpilcueta Hermilio, Tomas, *"Derecho Informático",* Editorial Abelardo-Perrot, Buenos Aires Argentina 1996, p. 55.

Este término ha venido evolucionando junto con las nuevas tecnologías hasta llegar a la definición dada por el Jurista Julio Téllez Valdez sobre Derecho Informático el cual dice: *"Es una rama de las ciencias jurídicas que consideran a la informática como instrumento y objeto de estudio. Que donde ya existe una interacción del Derecho y la Informática desde dos puntos, un primer punto como la Informática Jurídica y el segundo del Derecho de la Informática*.[30]

1.3.3.3 LA INFORMÁTICA JURÍDICA

Surge en el momento en que la Informática es utilizada con fines lingüísticos, el primer esfuerzo realizado fue en 1959 en la Universidad de Pennsylvania en el Healt Law Center donde fueron colocados en medios magnéticos ordenamientos legales, logrando su éxito al ser el primer sistema legal automatizado en búsqueda de información, mostrado por primera vez en 1960 ante la Barra de la Asociación Americana de Abogados y rediseñado para fines comerciales para la Corporación de sistemas Aspen, en 1966 se inició un sistema interno de recuperación de datos legales y para 1968 se habían computarizado los ordenamientos de cincuenta estados de los Estados Unidos de América.

La informática jurídica es la técnica que tiene por objeto la aplicación de la Informática para el procesamiento de información Jurídica, el jurisconsulto Julio Téllez Valdez la define como: *"La técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicable a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación"*.[31]

1.3.3.4 LA INFORMÁTICA APLICADA AL DERECHO

Muchas ciencias han visto que las aplicaciones de los adelantos tecnológicos le traen grandes e incontables beneficios generando eficiencia y rapidez, así como ahorro de tiempo y recursos y no pasará mucho tiempo en que los juristas utilicen estas herramientas a favor del derecho que son ramas de la informática Jurídica.

[30] Téllez Valdés, Julio, *"Derecho Informático"*, Tercera Edición, Editorial Mc-Graw Hill, México 2003, p. 17.
[31] Ibídem, p. 19.

Durante sus inicios la informática jurídica como ya se había mencionado enfocaba sus esfuerzos en el procesamiento de información jurídica, esto se le conoce como Informática Jurídica Documentaria con lo que podía abarcar tanto leyes, jurisprudencia y doctrinas, hasta actos jurídicos, con lo que ha llevado a un mejoramiento del fenómeno jurídico, como una compilación.

"Anteriormente la Informática Jurídica estaba separada de las aplicaciones de la Informática en derecho como lo señaló el tratadista Hermilio Tomás Azplicueta en su obra, pero con los adelantos tecnológicos ya no es posible mantenerlos separados. La informática jurídica de gestión dentro de la Informática aplicada al Derecho, consistía en aplicar cada uno de los principios informáticos a toda actividad jurídica y ésta a su vez la clasificaba en tres grupos": [32]

1.-INFORMÁTICA REGISTRAL: Consiste en la rapidez y facilidad de accesibilidad a registros públicos en especial, dando como ventajas del recuperar dichos registros de papel utilizado y facilitar los trámites.

2.-INFORMATICA OPERACIONAL: Consiste en facilitar las actividades en las áreas públicas como lo son los juzgados y en el área privada como los consorcios de abogados, permitiendo que las máquinas lleven todas las actividades, el control de asuntos y pleitos, contabilidad y registros.

3.- INFORMÁTICA DESICIONAL: el autor Hermilio Tomás Azplicueta *"la considera la más difícil de comprender debido a que no se busca una "Juscibernética" y no pasar a una automatización de las decisiones, sino en que la misma información proporcione facilidades para evitar trabajo repetitivo al momento de redacción de escritos por medio de formatos pre impresos donde exclusivamente se cambian datos variables, permitiendo al Juzgador ahorro de tiempo y continuar llevando sus labores decisorias"*.[33]

4.-INFORMÁTICA JURÍDICA DE AYUDA A LA DECISIÓN: En este caso los ordenadores facilitan la información adecuada para la toma de decisiones mediante el

[32] Azpilcueta Hermilio, Tomás, Ob. Cit, p. 56.
[33] Ídem

tratamiento y recuperación de información jurídica, siendo ésta la parte fundamental de la informática jurídica.

"Otra forma en la que puede ser clasificada la información jurídica es".[34]

1. INFORMÁTICA JURÍDICA DOCUMENTARÍA: *"Tiene por objeto la creación de bancos de datos jurídicos referentes a todas las fuentes del Derecho excluyendo a la costumbre, para su procesamiento y con fines de consulta en el futuro".*[35]

2. INFORMÁTICA JURÍDICA DE CONTROL-GESTIÓN: *"Enfocada en los campos jurídico-Administrativo, judicial registral y en despachos de Abogados. Dentro los que encontramos los siguientes"*:[36]

EN LA ADMINISTRACIÓN PÚBLICA: Debido al crecimiento demográfico y económico la Administración Pública ha sido orillada al uso de estas nuevas tecnologías para mejorar la estructura jurídico Administrativo y los sistemas de operación, con el fin de agilizar los trámites, disminuir la burocracia y la corrupción.

EN LOS ÓRGANOS JURISDICCIONALES: Con un enorme desarrollo en la automatización de los órganos jurisdiccionales conocido como: *"Informática Judicial, por ejemplo: la formulación agendaria de Jueces y Magistrados, redacción automatizada de textos jurídicos a manera de sentencias, la aceptación registro e indicación del número y juzgado y verificar si hay o no conexidad de la causa, pueden seguirse las diferentes fases del proceso y el estado del juicio en un momento en el futuro dejar de asistir a tribunales y ser consultables por vía telemática.* [37]

En los campos de Administración de justicia se permite que ésta sea rápida, expedita, particularizada y gratuita.

EN LOS DESPACHOS Y NOTARÍAS: Mediante el uso de sistemas computacionales se permite la automatización de oficinas, despachos y Notarías en diversas labores como el control de asuntos, honorarios, verificación de escritos y funciones

[34] Téllez Valdés, Julio, Ob. Cit, p. 28.
[35] Fix Zamudio, Héctor, *"Metodología, Docencia e Investigación Jurídicas"*, Décimo Primera Edición, Editorial Porrúa, México DF, 2003, p. 431.
[36] Ídem
[37] Téllez Valdés, Julio, Ibídem, p. 35.

documentarias de consulta, con lo que permite a los abogados enfocarse a actividades jurídicas de contenido creativo, crítico e interpretativo.

3. SISTEMAS EXPERTOS LEGALES O META-DOCUMENTARIA: Donde tras los fines documentarios de la Informática Jurídica, el sistema experto sirve con el fin de solucionar problemas con el uso de razonamientos implementados en una computadora, en lo que lo divide en 5 puntos para su fácil explicación:

a) INFORMÁTICA JURÍDICA DECISIONAL: Consiste en que los mismos medios informáticos le proporcionen a los Juristas ayuda en la toma de decisiones y no que un sistema tome las mismas por sí, aunque también hace referencia de la posibilidad de que un futuro que los mismos sistemas informáticos a través de sistemas expertos y la inteligencia Artificial.

b) EDUCACIÓN: *"Los crecientes avances en la Tecnología de la información y comunicación puede proporcionar mejoras en la educación tanto en aprendizaje de conocimiento como en experiencias Jurídicas facilitando las labores docentes y el aprendizaje"*.[38]

c) INVESTIGACIÓN O INFORMÁTICA JURÍDICA ANALÍTICA: Consta de las elementos matemáticos para aumentar las posibilidades de resultados, pero sin éxito por la complejidad y la ausencia de resultados exitosos. Este tipo de Informática usa las computadoras para poner a prueba las hipótesis y teorías.

d) PREVISIÓN: Con gran funcionalidad en países con sistemas jurídicos romano-germánico como el Mexicano, donde a través de un estudio de diversos factores pueden ser tomadas diferentes decisiones aún con la más mínima variable, un ejemplo de este proceso son las Jurisprudencias en materia penal de muchos Estados, donde para inferir del expediente y los antecedentes de los delincuentes analizando los antecedentes, medios profesionales, familiares, económicos, etc.

e) REDACCIÓN: Consiste en la ayuda y la corrección en la redacción de textos en especial legislativos, durante la creación mediante un programa especializado enfocado en la

[38] Fix Zamudio, Héctor, Ob. Cit, p. 432.

lógica interna del texto facilitando la comprensión coherencia y armonización de los textos. También puede ser usado en la enseñanza Jurídica por computadoras en el que se debe de reconstruir un texto jurídico mediante un sistema de interrogación con diferentes valores con el fin de asimilar la estructura de un texto.

Con lo anterior se puede resumir la Informática Jurídica se divide en tres ramas:

LA INFORMÁTICA JURÍDICA DOCUMENTARIA

Es la aplicación de métodos y técnicas de la informática en los textos jurídicos a bancos de datos, así como su procesamiento, que para poderlo lograr es necesario la recolección, organización, almacenamiento, recuperación, interpretación, identificación y el uso del documento Jurídico. Para poder lograr la Informática Jurídica es necesario considerar tres aspectos:

a) La aplicación de un método de análisis, recuperación y tratamiento de la información, de los cuales existen tres sistemas comunes para el análisis de la información jurídica: 1. Indexaconección, en el cual crea una lista y calificando e individualizando la información designado por una o varias palabras o claves numéricas lo que permite su fácil ubicación y consulta; 2.- Full-text: que consiste en el almacenamiento del texto en su totalidad en las máquinas; 3.- Abstract: consiste en almacenar los textos complejos de forma lógica a través de restrictores de distancia en el cual puede ser organizado y consultado con mayor facilidad.
b) La información de banco de datos mensuales, sistematizados, sectorizados o integrales.
c) La utilización de los lenguajes o mecanismos de recuperación de información.

INFORMÁTICA JURÍDICA DE GESTIÓN:

Consiste en todas las facilidades que proporcionan los sistemas informáticos en la organización, administración y control de la información, documentos, expedientes y libros jurídicos mediante programas o sistemas de clasificación, utilizado en el área pública y privada, utilizada en el seguimiento de trámites y procesos, el uso rápido de registros contenidos en base de datos, facilitar actuaciones y actividades administrativas.

INFORMÁTICA JURÍDICA DE APOYO EN LA DECISIÓN:

Consiste en la interacción hombre-máquina para la toma de decisiones jurídicas y el aprendizaje del Derecho, por medio de proporcionar banco de datos con hechos experiencias e información jurídica. Además de facilitar el trabajo mediante el proporcionamiento de elementos considerados repetitivos y tediosos con lo que permite enfocar a los juristas a realizar trabajo creativo en el campo del Derecho.

LA INTERNET Y EL DERECHO:

Con la llegada de la internet diferentes ramas de las ciencias naturales y sociales han visto una oportunidad de mejoramiento en sus campos ya sea como consulta, investigación y comunicación acortando tiempos y facilitando trabajos. La ciencia del Derecho debe aprovechar este medio para obtener grandes beneficios los cuales pueden enfocarse a los siguientes 3 campos: la comunicación, la información y el aspecto laboral.

EN EL CAMPO DE LA COMUNICACIÓN. Con otros seres humanos resulta importante basado en toda tecnología que permite mejorarla y simplificarla. La Internet proporciona en materia de comunicaciones al Derecho una amplia gama de posibilidades que es difícil no aprovechar.

CORREO ELECTRÓNICO (E-MAIL). Es un servicio de mensajería electrónica que permite un libre intercambio de información y datos entre las computadoras conectadas, en el caso de redes privadas este servicio puede ser usado exclusivamente a los equipos conectados a esta misma red con lo que no permitirá la entrada de cualquier otro correo electrónico de otro tipo de red. El servicio de correo electrónico consta de servidores que ofrecen este servicio utilizando la Internet como medio de envió con lo que permite que cualquier correo puede ser recibido por cualquier servidor por cualquier computadora siempre que sean compatibles; la gran ventaja que presenta el correo electrónico es la posibilidad que ofrece para poder enviar Documentos Adjuntos al correo (Attached) y éste ser enviado de manera instantánea en cualquier parte del mundo de manera más segura hacia cierto punto, la disminución de costos, debido que es más económico enviar un correo electrónico que hacer una llamada telefónica, enviar un Fax o el costo de correo común, en especial si esta es

realizada en diferentes partes del mundo. Otra ventaja es el ahorro de tiempo y trabajo debido a que el correo electrónico es un envió instantáneo, que a diferencia de un correo tradicional es necesario que la carta sea redactada, impresa, firmarse, colocarse en sobre y ser depositada en el buzón o en su caso ser enviada por fax, con lo que lleva gasto de tiempo y trabajo; otra ventaja del correo electrónico, es que el correo es depositado en un buzón virtual ya sea del servidor o de programas especializados con lo que permite que no se necesita estar disponible para recibirlo y ser revisado en cualquier momento, o en su caso para viajes puede ser revisado en cualquier computadora con acceso a Internet o a dispositivos móviles inalámbricos.

Este medio presente riesgos en la seguridad que aún hace que muchas personas no puedan confiar en este sistema al 100% debido a que el correo al ser enviado tiene que ser fragmentado y enviado por diferentes rutas que al final serán rearmados, pero esta unión se lleva a cabo por diferentes puntos que supone que puede ser visto o modificado en cualquiera de estos puntos, lo que reitera un serio problema en especial en el caso del secreto profesional. Otro riesgo que presenta el correo electrónico es que como en los medios tradicionales como lo son: el fax, las cartas, las llamadas telefónicas las cuales pueden ser conocidas por personas ajenas y sin la autorización con la intervención de llamadas telefónicas, robo de correo y documentos; el correo electrónico también se encuentra sujeto a este tipo de riesgos las cuales se pueden reducir al máximo tomando medidas de seguridad adecuadas.

Estas medidas de seguridad pueden ser técnicas o no, con diferentes grados de dificultad ya que, en primer lugar se tiene que el correo electrónico para poder ser enviado tiene que ser fragmentado y ser unido en diferentes o puntos hasta llegar al destinatario con lo que se está en riesgo de que los correos sean vistos, lo que puede ser considerado como medida de seguridad al respecto es contratar a un proveedor del servicio seguro y conocido, tomando en cuenta que proporciona este tipo de seguridad contra filtraciones de información y ataques externos; otra medida de seguridad es la codificación de mensajes mediante programas especiales, el problema que conlleva este tipo de medidas de seguridad consiste en que los programas no son fáciles de conseguir, el costo, necesidad de conocimientos básicos sobre codificación y la compatibilidad de programas con el destinatario. En el caso de redes privadas no existen mayores riesgos debido a una comunicación directa entre equipos.

Otro de los problemas que trae consigo el correo electrónico es el acceso no autorizado, con lo que pueden ser prevenidos relativamente de manera fácil, ya que primero es mantener una contraseña a salvo, nunca ser revelada a personas extrañas, no dejar guardada en las cuentas de correo electrónico en equipos propios o extraños, en caso de anotarla mantenerla en un lugar seguro y desconocido para las demás personas. Para el caso de contar con acceso a correos electrónicos en equipos personales y evitar sustracciones de información, las medidas de seguridad a seguir son básicamente en mantener apagados los dispositivos de comunicación inalámbrica cuando estos no son utilizados y contar con programas denominados antivirus siempre activos y actualizados.

Tomando en cuenta estas medidas de seguridad los juristas pueden tomar esta herramienta de comunicación como parte de su vida profesional, con lo que les permitirá un ahorro significativo de tiempo, dinero y trabajo, además, de mejorar su calidad de trabajo jurídico. Los principales servidores de correo electrónico en México y en el mundo de manera gratuita y segura a considerar son:

- www.google.com
- www.hotmail.com
- www.prodigy.com.mx
- www.terra.com.mx
- www.yahoo.com

MENSAJERÍA INSTANTÁNEA O CHAT

Como otro de los servicios que ofrece la Internet, éste permite una comunicación directa a través de programas especializados que se conectan entre los usuarios compatibles, que poseen el mismo servicio o mediante ciberespacios especializados ofrecidos por compañías en la Internet en cualquier parte del mundo; este medio permite establecer conversaciones en tiempo real entre dos o más personas a la vez mediante comunicación escrita "chat", hablada o mediante video o conferencia, con lo que representa ahorro de dinero a comparación con el teléfono en especial en llamadas de larga distancia, además, interactuar a la vez con un mayor

número de personas en una conversación telefónica normal y ahorro de tiempo debido a que no es necesario desplazarse a otros lugares con el fin de comunicarse con otra persona.

EN EL CAMPO DE LA INFORMACIÓN

La Internet en muchas ocasiones se le ha considerado como la biblioteca más grande del mundo, debido a que desde cualquier parte del mundo puede consultarse cualquier tipos de información en Bibliotecas virtuales o libros electrónicos (e-Books), de manera gratuita o no; la manera en la que se puede acceder a esta información es mediante sistemas de búsqueda de información encontrado en la página de inicio (home page). Las ventajas de la intervención de la Internet como medio de información es básicamente la facilidad que proporciona para acceder a información en cualquier momento y desde cualquier lugar de manera gratuitas si así se dispone; la desventaja consiste en que no todo lo publicado en Internet es cierto o actualizado en a sitios gratuitos, siempre que se tenga que consultar información en la red es necesario realizarlo en lugares conocidos.

La siguiente es una lista de direcciones de servicios generales de información Jurídica:

DIARIO OFICIAL:

http://www.emexico.gob.mx:80/wb2/emex/emexdiariooficialdelafederación

http://www.diariooficialdigital.com/

http://dof.terra.com.mx/

http://www.juridicas.unam.mx/infjur/leg/docleg/fed/indices/

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS:

http://www.info4.juridicas.unam/ijure/fed/9/

http://www.constitucion.gob.mx/

http://mexico.udg.mx/politica/constitucion/index.html

LEYES FEDERALES:

http://www.info4.juridicas.unam/ijure/fed/

http://www.cddhcu.gob.mx/refley/

LEYES DEL DISTRITO FEDERAL:

http://www.df.gob.mx/leyes/

http://info4.juridicas.unam.mx/adprojus/leg/10/default.htm?s=apj

TESIS Y JURISPRUDENCIAS:

http://www.juridicas.unam.mx/infjur/leg/jrs/

http://www.scjn.gob.mx/ius2006/paneltesis.asp

En el campo laboral la Internet a beneficiado al Derecho ya sea en el sector público o privado a distancia, con lo que permite realizar trabajos desde diferentes partes del mundo para un mismo fin, en el sector público y privado se han visto recientes oportunidades de crecimiento en este campo debido a grandes beneficios que trae consigo, entre estos se encuentran: el acceso remoto a sistemas y bases de datos, incremento en la productividad, ahorro en el personal, costos y espacios de oficina; mejor calidad del trabajo, reducción de costos en la gestión de clientes, mejoras en las condiciones de trabajo, permanencia del serbio, velocidad de actuar y calidad de vida.

No sólo en el área privada se ha visto beneficiado el derecho con el trabajo a distancia que trae consigo la Internet, ya que se ha visto la posibilidad de emplear políticas públicas creando un gobierno digital; *"el jurisconsulto Julio Téllez Valdés define un gobierno Digital como el "proyecto de políticas públicas en el que se programan acciones relativas a la eficiencia en la administración pública y sus vínculos con los ciudadanos y empresas".*[39] Con lo que para la defensa de los ciudadanos y empresas se pretenden establecer diferentes medios para la solución de controversias y su

[39] Téllez Valdés, Julio, Ob. Cit, p. 46.

defensa derivado de su relación mediante el uso de la Internet lo que se le denominó "Ciberjusticia".

Los primeros en aparecer en el campo de la "Ciberjusticia" fueron los "Cibertribunales" que funcionan igual que los arbitrajes y surgen de los conflictos surgidos del uso común en Internet ya sea entre público en general o conflictos entre empresa, con lo que les permite a las partes igual que en un arbitraje de elegir entre diversos expertos para proponer soluciones, *"los primeros Cibertribunales en surgir fueron en el año de 1996 en los Estados Unidos de América con la aparición de virtual Magistrate. Con colaboración del cyberspace Law Institute (CLI) y el Nacional Center of Automated Information Research (NCAIR), que ahora se encuentra en la Universidad de Chicago-kent y sus principales objetivos son: establecer el uso de resoluciones establecidas para conflictos que provienen en Internet, proveer de operadores de sistemas informados y neutros para los juicios, proporcionar un medio de solución de controversias, con autonomía para las partes, rápido, económico y accesible; proporcionar asesoría para definir deberes y obligaciones de las partes, estudiar la posibilidad usar el mismo u otros disponibles en la red".* [40]

"Un segundo Cibertribunal es el The Online Ombuds Office. Fue establecido en Junio de 1996 bajo la iniciativa del Center of Information Tecnology and Sioute Resolution de la Universidad de Massachussets, que consiste en un servicio de mediación para la solución de decisiones para personas e instituciones de una actividad en línea, en especial entre los miembros de un grupo de debate, competidores proveedores de acceso a Internet y sus abonados, y los que se relacionen con la propia intelectual". [41]

Otro de los denominados Cibertribunales fue *"el Cyber-Court un proyecto de otra vida creado en septiembre de 1996 y terminado en diciembre de 1999 creado por Center Recherche en Detroit Publique de la Universidad de Montreal, el cual su función era el de moderador en las mediaciones y prestar asistencia técnica o administrativa. Al termino de este fue creado el Resolution".*[42] Que continúo con este mismo trabajo.

Por ahora todos los intentos de un Cibertribunal están esencialmente enfocados a un arbitraje entre las partes por conflictos derivados del uso de servicios en Internet, creados por

[40] Véase "Virtual Magistrate", 4 de Febrero del 2013, *http://www.vmag.org/*
[41] Véase "The Online Ombuds Office", 4 de Febrer del 2013, *http://www.ombuds.org/center/ombuds.html*
[42] Véase "Resolution", 4 de Febrero del 2013, *http:/www.udrpinfo.com/eres/*

particulares; pero cabe la posibilidad que en un futuro exista Cibertribunales creados por el Estado, no únicamente enfocados a litigios creados por la Internet, sino también enfocados a todo tipo de litigio que normalmente un tribunal conocería, aunque en la actualidad y en nuestra realidad es posible revisar las actuaciones, acuerdos, sentencias y estado procesal mediante internet, en un futuro no sólo se puede revisar el estado procesal de los asuntos sino realizar actuaciones de manera telemática sin la necesidad de presentarse físicamente a los tribunales. A pesar de que la existencia de un Cibertribunal en México parezca una idea alejada de la realidad debido a que se tendría que adaptarse nuestro sistema legal, la solución de problemas de índole técnico-jurídico, el fortalecimiento de la confianza de las personas en los medios electrónicos como la Internet y en la justicia mexicana y el afinamiento de ligeros detalles en los asuntos que siendo similares no son únicos entre sí; los Cibertribunales tendrían como ventajas entre otras: el ahorro de tiempo y recursos tanto para el litigante como para el tribunal, en cuanto a evitar el traslado desde un despacho a un juzgado en una ciudad caótica como la nuestra, en especial cuando el asunto no se ha movido o en el caso de realizar actuaciones urgentes e inesperadas, disminuir el tiempo de reacción para emitir una respuesta rápida ante contratiempos desde cualquier parte del mundo, evitar la corrupción, ahorro de recursos que trae la disminución en los costos tanto para los litigantes como para el Estado; pero a su vez esto presenta desventajas para las partes, debido a que la seguridad y honestidad del sistema de una Cibertribunal depende de los conocimientos y honestidad de quien está encargada de la vigilancia y creación de un Cibertribunal o quien hace uso de él, la interacción entre las partes se vería disminuida o eliminada casi en su totalidad. Aunque con la idea de los Cibertribunales no puede ser tomada a la ligera y ser tema de estudio en trabajos posteriores.

1.3.3.5 LA CIBERNÉTICA JURÍDICA

Los avances en la ciencia nos han llevado a un mundo de maravillas tecnológicas que antes nunca pudieron ser imaginadas, con lo que ha llevado a mejorar la calidad de vida de los hombres en todos sus aspectos y aunque parece difícil de creer y de ciencia ficción, la posibilidad de que en una mañana las computadoras puedan tomar decisiones por sí mismas sin simular los pensamientos humanos ni ser manipulada o la necesidad de intervención humana para lograr complejas decisiones conocido como "Inteligencia Artificial".

"Se entiende como (Inteligencia Artificial) el: Desarrollo y utilización de ordenadores con los que se intenta reproducir los procesas de la inteligencia humana".[43] Aunque en los campos de la Inteligencia Artificial está dando sus primeros pasos la idea de que una computadora pueda tomar decisiones jurídicas por sí misma sin la necesidad de intervención humana, e incluso el grado de suplantar jueces y magistrados pueda causar controversia y considerar un tanto impráctico e innecesario.

Para la toma de decisiones jurídicas dependen de muchos elementos y vertientes para buscar una verdad jurídica sólida aún la más mínima decisión requiere de un sinnúmero de elementos que no pueden ser analizados fácilmente, explicados y ser plasmados de manera práctica, aunque se puede hablar de "Sistemas Inteligentes Legales" los cuales no es necesario que la misma computadora tome las decisiones por si, sino que ésta pueda proporcionar auxilio en las tomas de decisiones jurídicas como una herramienta y éstas para un funcionamiento óptimo deben contener requerimientos básicos: una base de conocimientos como banco de datos, un sistema cognoscitivo o mecanismos de inferencias para la estructura de esquemas de razonamiento, elementos que permiten el establecimiento de comunicación entre el sistema y el usuario, que al igual que en otras ciencias estos sistemas expertos funcionan a través de complejas ecuaciones y modelos lógico-matemáticos, para resolver problemas y simulaciones complejas lo que ha llevado a diversos estudios en diversas áreas de las ciencias a realizar complejas emulaciones a procesos que llevarían semanas en resolver por la mente humana, aunque el proceso mental que lleve al planteamiento, razonamiento y solución de problemas es difícil de explicar y describir, además de que necesita determinados factores como el conocimiento, la experiencia y determinadas circunstancias, así como otros factores que pueden ser considerados como subjetivos, para la existencia de un sistema capaz de tomar decisiones sin la necesidad de la intervención o manipulación humana, en especial para el ámbito del Derecho se necesita la existencia de una computadora capaz de resolver y plantear decisiones jurídicas se necesitaría que ésta pudiera obtener conocimientos por sí misma, aprender de errores del pasado en forma de experiencia, así como, de analizar factores que pueden ser considerados como subjetivos para poder llegar a una verdad jurídica, pero no ser descartada ya que loa avances en la tecnología siempre traen sorpresas en el futuro.

[43] Diccionario de la Lengua Española, Ob. Cit, t. 6, p. 873.

1.3.3.6 DERECHO DE LA INFORMÁTICA

Como ya hemos visto las nuevas tecnologías han traído mejoras en todos los campos del Derecho e incluso nuevas formas en las que esta ciencia puede ser vista a partir de ahora, así como ha pasado en otras ciencias del conocimiento humano, pero los nuevos adelantos no podían quedarse al uso exclusivo de los científicos, investigadores y estudiosos de las ciencias, sino también han pasado a ser uso del público en general y en mayor medida del uso comercial, aprovechando sus enormes beneficios tanto como herramientas para adquirir conocimientos, analizar comunicaciones y simplificar la vida humana.

A partir de los años 60`s con el uso de los medios informáticos surgieron mayores relaciones sociales y comérciales entre los pueblos y a partir de ellos surgieron problemas derivados de la expansión de relaciones, con lo que se da nacimiento al Derecho de la informática, pero en esos momentos no era tan estudiada ya que se le deba más importancia a la informática jurídica o en muchas ocasiones junto a ella era estudiado, debido a que todos estaban enfocados y maravillados en los beneficios que traían las Computadoras al mundo del Derecho.

Con lo que atendiendo a esa problemática ha surgido el Derecho de la Informática para poder dar solución a estos conflictos, entendiéndolo como: *"Conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"*.[44] Con lo cual los problemas a enfrentarse en el mundo de la informática e Internet son entre otros:

- La regulación jurídica de los derechos y obligaciones derivados de las relaciones existentes al adquirir, distribuir, explotar y utilización del software y Hardware, protección jurídica de Software considerado como un bien inmaterial.
- Derechos y obligaciones para los creadores, distribuidores y usuarios de base de datos.
- Regulación jurídica derivada de la contratación de bienes y servicios informáticos ya sea dentro de un Estado y fuera de ellos ya sea de manera directa o indirecta.
- Protección de datos personales, surgida de la potencial agresión informática con respecto al procesamiento de estos mismos datos.

[44] Téllez Valdés, Julio, Ob. Cit, p. 61.

- Responsabilidad, derechos y obligaciones surgidos de la transferencia electrónica de fondos o datos, dentro de un país o incluso entre usuarios localizados en diferentes países con diferentes regulaciones jurídicas.
- Validez probatoria de los documentos generados por medios informáticos o incluso de los documentos encontrados en soportes informáticos.
- Regulación jurídica derivada de la relación laboral a través de los medios informáticos a distancia.
- Transacciones comerciales llevadas a través de medios informáticos realizados dentro de un país o fuera de él.
- Los denominados Delitos Informáticos.

Debido a estos problemas que se suscitan en estos campos el primer paso para dar una solución y en especial una regulación y protección es la planificación mediante normas que conforman una política la cual se tiene que acoplar a un fomento del desarrollo industrial en el campo de la informática, contratación gubernamental de servicios y equipos informáticos confiables y seguros, plantación, control, aplicación, difusión y del fenómeno informático.

LA PROTECCIÓN DE BASE DE DATOS.

Actualmente la información ha dejado sus connotaciones pasadas, convirtiéndose en un bien fundamental en un mundo cada vez más apegado a la tecnología la cual se ha convertido como una herramienta de fácil acceso a ella, pero a la vez que éste sea considerado con un bien con valor económico, debido a que en las diferentes fases en el procesamiento de la información implica un costo que es reflejado en precio ante los usuarios, pero en muchos casos la información no tiene cuantía imaginable debido que contar con ella permite tomar decisiones de manera más rápida, certera e informada, generar riquezas superiores al valor mismo de la información, e incluso manipular a las personas y sociedades enteras, bien incluso se menciona que quien tenga el conocimiento tiene el poder.

Las bases de datos han proliferado con la llegada de las nuevas tecnologías en diferentes áreas de la sociedad que en muchos casos son usadas con fines tanto administrativos, de control, académicos e incluso económicos.

Para la creación de base de datos eficientes interfiere diversos procesos que involucra a una gran cantidad de personas especializadas, con lo que éstos se convierten en un producto con costo determinado que muchas veces se ve reflejado en la calidad de la base de datos y según para el fin que esté creada la base de datos esta presentara variados problemas a tratar.

La base de datos en general tiene 3 problemas fundamentales básicos por resolver, el primero el derecho de autor del material almacenado en los bancos de datos, la autorización sobre el uso de sus obras y otorgar la facultad de administrar la base de datos; el segundo es el Derecho originado a los productores de la base de datos por la sistematización y elaboración, el tercero son los derechos y obligaciones derivados entre la relación del creador, distribuidor y usuario, este último al ser consultado y ser adquirido.

El caso de la base de datos con fines académicos han revolucionado a las ciencias debido a la facilidad que conlleva manejar grandes volúmenes de información en corto tiempo, con lo que ha llevado a las computadoras sean consideradas como una herramienta académica por el manejo de base de datos en soportes electrónicos que únicamente pueden ser leídos por los mismos, pero en otros casos las bases de datos sólo pueden ser consultadas de manera "On-line" mediante la Internet o el uso de redes privadas.

Con fines económicos y administrativos las bases de datos han creado una relación de dependencia con las empresas, lo que los hace completamente vulnerables a posibles atentados, que generan daños y pérdidas económicas y que en muchas ocasiones termina en el cierre de la empresa por lo que las bases de datos de este tipo necesitan de 3 tipos de seguridad: la física con concierne a la estructura física que sustenta la base de datos, como lo son soportes magnéticos (diskettes), ópticos (CD ROM) y las mismas computadoras; la lógica que es toda la base de programación necesaria para el correcto funcionamiento de la base de datos; y en especial protección jurídica en cuanto los ataques físico como lógicos de la base de datos.

PROTECCIÓN DE DATOS PERSONALES

La información no es exclusiva de los medios tecnológicos, aunque con ésta tuvo su auge en los años 70`s con el gran almacenamiento de documentos en medios electrónicos, con lo que permitió el rápido manejo y el control de grandes volúmenes de información en menor espacio y debido con el creciente uso de los medios informáticos, permitió que la mayor parte del público, empresas, instituciones públicas crearan su propia información, e incluso de información de tipo personal, los cuales contenían datos personales desde los más básicos como nombre, edad, fecha de nacimiento, domicilio, estado civil, hasta los archivos con datos más complejos como el tipo sanguíneo, nivel y logros académicos, enfermedades o padecimientos pasados o actuales, religión, cuentas bancarias, los cuales pueden ser almacenados en diferentes centros de acopio o banco de datos públicos o privados, incluso en los mismos hogares, que sin la ayuda de la informática el tratamiento de todos estos datos para diferentes personas seria una labor compleja, pero se tiene que recordar que la seguridad de cualquier medio de cómputo así como la buena voluntad humana no son perfectas al 100% y la información personal comprometedora depositada en los bancos de datos es susceptible de caer en manos de terceros y ser susceptible de ser revelada lo que puede generar un sinfín de problemas.

Para poder tratar este asunto, diferentes sistemas jurídicos se han enfocado en resolver, desde la Asamblea de los Derechos Humanos en 1968 se presentaba la preocupación por esta creciente realidad, en el caso de Francia se presentan figuras como los Derechos Humanos, Derechos Personales, Derechos Patrimoniales, Libertades Públicas y privadas con su Ley 78-17 del 6 de Enero de 1878 relativa a la informática, archivos y libertades; en el caso de los Países de Sistemas jurídicos Anglosajones se presentan las figuras de Derecho a la Privacidad, como es el caso de los Estados Unidos que cuenta con su Ley sobre la protección de las Libertades Individuales de la Administración Federal de 1974 y en el caso de España se presentan las figuras jurídicas del Derecho a la Intimidad y al Honor con lo que señala la Constitución Española en su Artículo 18.4: *"La ley limitará el uso de la informática para garantizar el honor y la*

intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus Derechos".[45] Y su ley orgánica de protección de datos de carácter personal del 13 de diciembre de 1999.

En el caso del sistema legal Mexicano aún no se tiene una ley completa y avanzada que pueda proteger los datos personales de manera completa como lo hacen en otros países, los primeros intentos se encuentran en la Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental, pero no llega al nivel de importancia a los objetivos de regular y proteger este delicado problema.

"El primer intento para la protección de datos personales de ámbito internacional fue el convenio 108 para la protección de las personas Respecto al tratamiento Automatizado de los Datos de Carácter Personal del 28 de Enero de 1981 conocido como el Convenio de Estrasburgo por el Consejo Europeo".[46] El cual lo integran 31 países que han firmado este convenio en la actualidad, donde hace mención a los objetivos a seguir, definiciones, ámbitos de aplicación, obligaciones de las partes, derechos, excepciones, sanciones y autoridades; el segundo son las Directivas Europeas 95/49/CE relativa a la protección de las libertades de las personas físicas con respecto a los datos de carácter personal y a la libertad de circulación de esos datos de 24 de Octubre de 1995 de la Comunidad Europea y dentro de los Organismos Internacionales en preocuparse en esto son la OCDE (Organización para la Cooperación y el Desarrollo Económico) con las Líneas Directrices Reguladoras de la Protección de la vida privada y los flujos Transfronterizos de Datos de Carácter personal del 28 de Septiembre de 1980 y la ONU (Organización de las Naciones Unidas) con las líneas Directrices para la reglamentación de los Archivos informatizados de datos de carácter personal de 1989.

TRANSFERENCIA ELECTRÓNICA DE DATOS Y FONDOS

Otro problema al que se enfrentan en la transferencia de datos transfronterizos el cual se debe con el éxito de las telecomunicaciones e informática y la gran necesidad de mantenerse en comunicación entre empresas e incluso entre los particulares, que la cual ha traído grandes

[45] Constitución Española, 8 de Febrero del 2013, *http://www.derechoshumanos.net/constitucion/index.htm?gclid=CKX0iq3l7gCFWrl7Aod73YAeQ*.
[46] Convenio No 108 del Consejo, de 28 de Enero de 1981, de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, 8 de Febrero del 2013, *http://www.apdcat.net/media/246.pdf*

beneficios como el libre intercambio de ideas y opiniones a través del mundo, progreso y crecimiento técnico debido al intercambio de información entre instituciones científicas, progresos económicos con la internacionalización de empresas, pero a su vez contrae problemas sociales y culturales debido a sabotaje en la información o incluso el continuo bombardeo de otras culturas mediante los medios electrónicos puede generar cambios en estos niveles a los cuales no estaban preparados o no son compatibles, crea dependencia tecnológica con el creciente incremento de las tecnologías especializadas en diferentes tareas de la vida humana; y un punto importante es el problema generado por el sabotaje o mala información que puede generar en una frágil economía que depende en muchos casos de la información para su estabilidad.

Con esta transferencia de datos han surgido nuevos problemas en los que el Derecho tiene que enfocarse como lo son: el uso ilícito de datos en el extranjero, intercepción de datos, revelación de información confidencial, control y alteración de documentos fuente, extravío de información, tarifas y régimen fiscales, atentados contra la soberanía de los Estados, regulación de contratos que rodean a la información, propiedad intelectual de la información difundida, seguridad jurídica de las empresas y en muchos casos de los usuarios, con lo cual dio origen el Convenio de Estrasburgo del 28 de enero de 1981 donde también se enfocó en el tratamiento de transferencia de datos transfronterizos aplicable a los países miembros.

Otros beneficios de las telecomunicaciones en la transferencia electrónica de fondos, el cual permite el rápido traspaso de grandes sumas de dinero, lo cual ha sido aprovechado por empresas e instituciones financieras y a menor medida entre particulares, pero este sistema tiene que ser tomado cuidadosamente debido a que es necesario regular la relación de las partes que intervienen en la transferencia de fondos, así como, la transferencia misma, debido que en muchas ocasiones pueden generar el cierre de una empresa o institución financiera en caso de robo sabotaje o alteraciones o incluso el desastre financiero en países enteros.

LA PROTECCIÓN DEL SOFTWARE

A partir del incremento de los medios informático en especial con la llegada de las telecomunicaciones se han visto los fines comerciales y profesionales y desde un punto de vista económico en este momento se ha encontrado así un nicho de mercado en la distribución y

comercialización de programas de cómputo, con lo que se convirtió en la máxima expresión de un producto informático, el cual es capaz de facilitar a un mundo informatizado. Pero éste al ser resultado del intelecto humano además de ser objeto de comercio necesita protección jurídica.

Teniendo en cuenta que la información es un bien intangible ésta es susceptible de apropiación por lo que se le puede considerar como una mercancía autónoma y como tal requiere de regulación y protección jurídica a consecuencia de la relación de derechos y obligaciones, además de la relación resultante entre la información y su creador, así como, de la capacidad de transferencia, usarla, explotarla o incluso recibirla, el cual al ser creación del intelecto del autor él puede disponer de ella en cualquier forma ante terceros.

En tanto a un aspecto técnico, los programas de computadora están diseñados para cumplir lógicamente con determinadas tareas, entre ellos están:

LOS PROGRAMAS FUENTES O SISTEMAS OPERATIVOS: los cuales en muchos casos se encuentran integrados en los equipos de cómputo que tienen por objeto el control y el uso de los diferentes componentes que integran el sistema central de una computadora.

PROGRAMAS OBJETIVOS: Son todos aquellos que tienen la función específica para satisfacer determinadas necesidades de los usuarios.

PROGRAMAS DE APLICACIÓN: Estos se encuentran en equipos externos los cuales para realizar su funcionamiento necesitan de estos programas o incluso para interactuar con equipos de cómputo convencional.

De esto se derivan un sinfín de problemas abordados desde diferentes puntos de vista, el primero desde las empresas, debido a que los programas considerados como un bien económico no se encuentran seguros y pueden ser sustraídos por los competidores desleales o incluso por particulares, por lo que las empresas invierten grandes cantidades de dinero en sobreproducción de programas, señuelos o en muchas ocasiones de programas incompleto e imperfectos; otro problema es el plagio, sabotaje mediante técnicas avanzadas de informática por lo que las empresas invierten grandes sumas de dinero para proteger sus sistemas de

posibles ataques y por último se encuentra decodificación de los programas con el fin de que si llegaran a ser sustraídos estos no pueden ser usados y por lo cual exclusivamente pueden ser descifrados por compañías especializadas o incluso por la misma empresa, lo que tae como consecuencia un incremento costo final en los programas que se ve reflejado en costo a pagar por los consumidores; desde un punto de vista de la relación de la empresa y los usuarios, los problemas que se encuentran son: el uso, alteraciones, explotaciones indebidas hechas por los mismos usuarios u otros no autorizados, así como, el apoderamiento ilícito del mismo mediante la piratería de programas, los cuales para su solución pueden ser abordados desde diferentes ramas del Derecho existentes.

Desde el **Derecho Civil y Mercantil** se encuentra, la problemática derivada de los contratos por el uso correcto y exclusivo de los programas; evitar y controlar la competencia desleal entre productores, distribuidores y usuarios con fines comerciales de los programas de computadora y por último se presenta el enriquecimiento ilícito con el abuso de los programas sin autorización que llevan a un beneficio económico a quien lo practique y a su vez un empobrecimiento del creador del programa de cómputo.

Desde el enfoque del **Derecho Penal,** se encuentran figuras como el robo, fraude, abuso de confianza en otros sistemas jurídicos se encuentran las figuras de los secretos comerciales y secretos de fabricación, desde el punto de la **Propiedad Intelectual** se encuentran aplicables a la protección de programas de computo a los temas de marcas y patentes y la intervención de los **Derechos de Autor** derivado de la propiedad literaria y artística en ciertos programas.

1.3.3.7 CONTRATACIÓN ELECTRÓNICA Y COMERCIO ELECTRÓNICO

Con el creciente uso de la nuevas tecnologías y en especial con la Internet han surgido nuevos problemas derivados de la actividad comercial que se lleva en el mismo, debido a que existía una gran disparidad y en ocasiones abusos desmedidos de parte de los proveedores de los servicios y compras en la Internet y para que esto pueda detenerse debe de existir por parte de los usuarios el conocimiento necesario para evitar esta penosa situación y no ser víctimas de estos abusos a la hora de la contratación de compras y servicios.

Los contratos informáticos son todos aquellos contratos que abarcan transacciones con bienes y servicios mediante la Informática, los objetos de estos contratos son: servicios Informáticos y bienes informáticos que incluyen a los suministros y programas.

Los bienes informáticos en el estricto sentido comprenden todo lo que es el Hardware o equipo de cómputo tanto como interno como externo. Los suministros informáticos comprenden todos aquellos elementos que son conocidos como "Consumibles" en las labores informáticas, éstos se subdividen en:

- Los usados para registros informáticos: que comprenden las diferentes clases de papel y los medios magnéticos.
- Abastecimiento del equipo: como cintas de impresión, tinta y polvo de impresora.
- Auxiliares del equipo: que son los líquidos, cintas toallas equipos limpiadores.

Los servicios informáticos son todos aquellos elementos que intervienen en el auxilio de la actividad informática en la vida diaria, estos servicios informáticos son:

- Los relacionados con los recursos humanos.
- Consultaría y asesoría general.
- Asesoría con los equipos de cómputo y auxiliares.
- Uso de equipos por tiempo.
- Explotación de licencias para programas de cómputo.
- Consulta de base de datos, documentaciones técnicas.
- Mantenimiento de los equipos de cómputo.

En el caso de los contratos electrónicos éstos constan de dos equipos de efectos, los generales que son: el objeto, la duración y rescisión, precio, facturación y pago, garantías y responsabilidades, disposiciones generales, y los elementos específicos que encierran las definiciones técnicas, control de acceso al servicio, asistencia técnica remota o personalizada, secreto y confidencialidad.

En tanto a las partes de un contrato electrónico son: el proveedor del servicio que son los fabricantes distribuidores y vendedores; y los usuarios que pueden ser segundas empresas, entidades públicas y el público en general.

Existen diversos contratos electrónicos que pueden ser aplicados en cuanto al equipo de cómputo, programas de cómputo, servicios informáticos base de datos y documentación los cuales son:

CONTRATO ELECTRÓNICO DE ARRENDAMIENTO

En este contrato esencialmente aplica principalmente en los equipos de cómputo así como accesorios y elementos periféricos de tales equipos, el cual es fundamental fijar el nombre y modelos de los equipos descripción, renta que no necesariamente puede ser mensual, duración término y condiciones del contrato. Además puede contener la opción de compra al final del término del contrato (leasing) en el cual se tiene que señalar el costo del precio de compra, a través del arrendamiento financiero.

En el contrato electrónico de arrendamiento financiero el proveedor se hace responsable de los derechos de autor y propiedad intelectual e industrial e indemnizara daños a terceros, garantizar que los equipos se encuentren en óptimas condiciones y conforme a lo pactado, además de ser responsable por los actos cometidos por los empleados encargados de la Instalación de estos equipos para el usuario.

CONTRATO ELECTRÓNICO DE SERVICIOS ELECTRÓNICOS

Este contrato se asemeja al contrato de prestación de servicios profesionales, que consiste en el servicio que ofrece un profesional a una persona denominada cliente el cual está obligado al pago de una llamada retribución. Las partes en este contrato se le conocen como proveedor el cual es quien presta el servicio y puede ser empresas de donde fue originado el equipo o programa de cómputo o empresas especializadas para estos efectos, y el usuario o cliente quien recibe el servicio, otra especie de este contrato abarca la consulta de datos, documentación técnica, estudios de marcados, administración de datos, seguridad de base de datos y mantenimiento de equipos de cómputo.

CONTRATO ELECTRÓNICO DE COMPRA-VENTA

EL COMERCIO ELECTRÓNICO

Desde 1991 cuando se levanto la prohibición de los usuarios comerciales en la Internet, se ha proliferado esta de manera impresionante a lo largo del mundo con lo que han surgido muchas empresas dedicadas exclusivamente a esta actividad e incluso transformando otras para realizar sus operaciones normales a través de la Internet, el comercio electrónico puede ser realizado por diversas vías, la primera es entre empresas a empresas, la segunda entre empresas y particulares y por último entre particulares, aun que existe la posibilidad abierta de que ésta puede ser realizada por los gobiernos como parte en este comercio.

El comercio electrónico se entiende como la compraventa de productos realizada a través de la Internet, con la que debe de contar con diferentes fases, la primera consiste en la entrada de paginas especializadas en el comercio electrónico, la segunda fase consta en la manifestación de la voluntad de comprador en adquirir el producto en cuestión, la tercer fase es la aceptación por el vendedor al extender la orden de compra, por último el comprador realiza el pago, se realiza la entrega y se extiende recibo por la compra.

Durante los años de práctica han surgido diferentes organizaciones en la que puede ser llevado el comercio electrónico o medios de efectuarlo, el primero es realizado a través de las conocidas como Tiendas virtuales, es de las formas más sencillas de comercio, además de las más usadas para el comercio electrónico debido a que exclusivamente se ofrece el producto y las herramientas de pago por cualquier persona interesada. El segundo es el modelo de Centro Comercial donde en un solo sitio se ofrecen diferentes productos por zonas específicas dentro del mismo sitio, este modelo es utilizado por las cadenas comerciales y constan con las mismas garantías y seguridades que ofrecerían una tienda departamental de la misma cadena. El tercer modelo es el Portal Comercial donde un sitio presenta diversos servicios que no son necesariamente es compra-venta de productos, estos servicios pueden ser juegos, comunicación, descarga de programas de cómputos, noticias e información de interés.

Los grandes beneficios que ha traído el comercio electrónico son irrefutables debido a que las transacciones son de manera rápida, se puede tener información más detallada de los productos, no tiene que sujetarse a los horarios de las tiendas comerciales debido a que puede realizarse compras en Internet las 24 horas del día, ahorro de tiempo y trabajo, se evita el estrés de las compras directas y el sin número de personas que se pueden presentar en una sola tienda en días festivos, incentivos y descuentos al realizar las compras vía electrónica y en muchos casos se evita los intermediarios al hacer trato directo con los fabricantes.

En el mundo, este medio ha sido aceptado y cada vez está en más uso, pero en México aún no se ha convertido en una práctica común y el 80% de las personas que poseen acceso a Internet no desean hacerlo debido a que aún que se ha demostrado que es una práctica generalmente confiable no se posee la confianza para realizar transacciones vía Internet debido a que en nuestra cultura la compra-venta se prefiere realizar de manera inmediata y en muchos casos, la poca regulación jurídica que existe conforme al tema, claro está, cabe la posibilidad de que un tercero interfiera esas operaciones.

Los sitios más usados en México según su modalidad son:

- Las Tiendas Virtuales: www.deremate.com.mx, www.amazon.com.
- Centros Comerciales: www.liverpool.com-mx www.elpalaciodehierro.com.mx , www.sears.com.mx
- Portal Comercial: www.todito.com. www.esmas.com, www.prodigy.msn.com

EL CONTRATO DE COMPRA-VENTA EN INTERNET

En el contrato de compraventa a través de la Internet interviene la manifestación de voluntades que son la oferta y la aceptación, la oferta que consiste en la manifestación de la voluntad unilateral y obligatoria en el cual se propone a determinada o determinadas personas la conclusión de contrato sometido a ciertas condiciones, donde se presenta de manera definida la cosa, el precio, así como derechos y obligaciones los cuales deben de referirse a la entrega de la cosa, el pago de un precio cierto y en dinero, ésta manifestación de la voluntad puede realizarse en el momento en que el vendedor mediante medios electrónicos y aunque una computadora puede poner ofertas de manera automática se tiene que recordar que no

poseen voluntad propia sino poseen explícitamente la voluntad del creador del programa el cual tenía la intención de que la misma computadora realice la oferta.

La aceptación, que es la manifestación de la voluntad del comprador para adquirirse a la oferta del vendedor, ésta puede ser llevada de manera inmediata, dentro de un plazo establecido o dentro de 3 días cuando no se hace entre presentes; en los medios informáticos la aceptación se puede hacer de manera tácita con el simple hecho de hacer "Click" en el botón del Mouse; para la identificación del aceptante ésta puede ser realizada mediante firmas electrónicas, contraseñas, correos electrónicos o incluso creando cuentas en los sitios de compraventa. Se entiende cuando se ha recibido la aceptación en el momento en que el vendedor extiende una orden de compra y se perfecciona cuando ésta extiende un recibo. Se entenderá que el contrato se encuentra de manera escrita y firmada cuando están sus cláusulas por medio de archivos en soportes magnéticos o en la misma computadora.

LOS DOCUMENTOS ELECTRÓNICOS

Con la actividad diaria se ha introducido el uso de las computadoras para facilitar la vida y con ello han surgido los conocidos "Documentos Electrónicos" o "Informáticos" el cual contiene diferentes connotaciones para ser entendidos, en un sentido técnico y puro se entiende como Documento Electrónico al conjunto de impulsos electrónicos o lumínicos que se encuentran almacenados en soportes de la misma naturaleza, los cuales para ser leídos son necesarios la traducción hecha por una computadora para que esta pueda ser entendida por el hombre, otra connotación más fácil de entender sobre los documentos electrónicos son todos aquellos documentos creados por el hombre de manera directa o indirecta encontrados en soportes informáticos, estos soportes informáticos se clasifican en tres tipos, el primero son los soportes magnéticos como el disco duro encontrado en las computadoras (Hard Disk Drive); soportes móviles que comprenden disquetes (floppy Disck), tarjetas de memoria (multimedia Memory Cards, USB Memory Flash) y las cintas magnéticas como las encontradas en las tarjetas de crédito, el segundo medio son los sistemas ópticos que comprenden los discos compactos en sus diversos formatos (CD-ROM, DVD, HDDVD, BLUE-RAY) y por último se encuentran los códigos ópticos impresos o códigos de barras, el cual debe de tener como característica la inalterabilidad, autenticidad, durabilidad seguridad.

Se dice que los Documentos Electrónicos pueden ser realizados de manera directa por el hombre cuando su propia voluntad crea y recopila información por sí en una computadora con los elementos de entrada de una computadora ejemplo tecleándolo, dictándolo o escribiéndolos con plumas digitales, puede entrar la máquina en auxilio de esta actividad mediante escáner y lectores ópticos para cualquier texto directamente del papel; de manera indirecta pueden ser creados por la misma computadora en función de sus operaciones pero se tiene que recordar que la máquina no lo hace por sí misma sino que ésta lo hace porque así fue construida y se encuentra la voluntad de su programador, aunque no se descarta la posibilidad que en un futuro la computadora mediante inteligencia artificial pueda realizar documentos sin intervención humana.

Estos documentos no son perfectos al 100% por lo que aún no son confiables de usar y en muchas ocasiones temidos, debido a que presentan desventajas que pueden causar serios problemas en todos los campos, estos problemas principalmente son:

- Sólo pueden ser leídos mediante el auxilio de una computadora.
- No existe distinción entre originales y copias.
- Su alteración y sabotaje resulta extremadamente fácil.
- Incompatibilidad entre los soportes informáticos con los programas de cómputo o incluso los mismos sistemas de cómputo.
- No existe seguridad con relación al autor.

En México aún no se encuentran regulados adecuadamente todos los aspectos considerados como prueba, los primeros indicios que se dieron de esta regulación fueron en la Ley del Mercado de Valores en el Diario Oficial de la Federación del 2 de enero de 1975, donde ya se hacía mención de la existencia de estos documentos y requisitos base a seguir; después con las reformas del año 200 existen amplios ordenamientos que hacen mención. El primero es el Código Federal de Procedimientos Civiles en su Artículo 210-A donde se reconoce como prueba la información generada o comunicada que se halle en medios electrónicos, ópticos o en cualquier otra tecnología y para poderla valorar se deberá evaluar primordialmente la confiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la

información relativa y ser accesible para su ulterior consulta. Para el caso de que la Ley requiera que un documento sea conservado y presentado en su forma original, esto quedará satisfecho si se acredita que la información generada, comunicada, recibida y archivada se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta puede ser accesible para su consulta.

El segundo ordenamiento en aparecer fuel el Código de Comercio en su Artículo 1205 en el que se tiene admisible como prueba los "Mensajes de datos" y finalmente se encuentra el artículo 1298-A donde los mensajes de datos para que puedan ser valorados deberá estimarse la confiabilidad del método utilizado para generarla, archivarla, comunicarla y ser guardada.

Como se ha podido analizar la Informática ha aparecido en todas las labores del hombre en los últimos 50 años, y no obstante de su gran desarrollo han sido pocos los autores que lo han tratado de enfocar a las múltiples ciencias como es el Derecho.

El emocionante mundo de la informática ha sido en los últimos cinco años y será un gran instrumento para la Ciencia del Derecho por lo que es de gran importancia darle un Marco Jurídico apropiado para regular los diversos entornos en que puede presentarse, tales como el Civil, Administrativo, Laboral, Mercantil y el Penal entre otros, debiéndose perfeccionar aún más lo referente a los Delitos Informáticos sobre los cuales está una gran variación como se verá en el capítulo cuarto.

1.4 LOS DELITOS INFORMÁTICOS EN EL MARCO JURÍDICO FEDERAL EN MÉXICO

Un punto de los más relevantes en México fue la asignación de direcciones para el internet y son las siguientes:

.com	.gob	.edu	.net	.org

Los anteriores en virtud de los sitios comerciales, gubernamentales, educativos, y demás vinculados con la red y de organizaciones civiles respectivamente, los cuales serían los únicos en la esfera del Internet en ser susceptibles de ser regulados. No obstante a medida en que se fue ganando presencia dentro de los grupos sociales, cultural, educativos e incluso económicos, comenzaron los conflictos en torno a la red, y respecto de sus usuarios, especialmente en los gobiernos, lo anterior en virtud de la falta de reglas específicas para ordenar el disperso universo que es la red de redes, de igual forma el empleo de los recursos de la misma como lo es el correo electrónico (e-mail).

1.5 CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Dentro de nuestro sistema jurídico nacional en importante destacar que México se encuentra conformada en *"una República, Federal, integrada por Estados libres y soberanos en sus tres poderes Ejecutivo, Legislativo y Judicial, en donde cada uno de ellos se encargará de desarrollar sus funciones correspondientes"*, [47]según los dispositivos:

Artículo 40. Es voluntad del pueblo mexicano constituirse en una República representativa, democrática, laica, federal, compuesta de Estados libres y soberanos en todo lo concerniente a su régimen interior; pero unidos en una federación establecida según los principios de esta ley fundamental.

Artículo 41. El pueblo ejerce su soberanía por medio de los Poderes de la Unión, en los casos de la competencia de éstos, y por los de los Estados, en lo que toca a sus regímenes interiores, en los términos respectivamente establecidos por la presente Constitución Federal y las particulares de los Estados, las que en ningún caso podrán contravenir las estipulaciones del Pacto Federal.

DE LA DIVISIÓN DE PODERES

Artículo 49. El Supremo Poder de la Federación se divide para su ejercicio en Legislativo, Ejecutivo y Judicial. No podrán reunirse dos o más de estos Poderes en una sola persona o corporación, ni depositarse el Legislativo en un individuo, salvo el caso de facultades extraordinarias al Ejecutivo de la Unión, conforme a lo dispuesto en el artículo 29. En ningún

[47] Constitución Política de los Estados Unidos Mexicano, México 2013.

otro caso, salvo lo dispuesto en el segundo párrafo del artículo 131, se otorgarán facultades extraordinarias para legislar.

En virtud de lo antes señalado es de vital trascendencia determinar que el Poder que es materia de nuestro análisis es el Legislativo, tanto federal como local, atendiendo al **principio de exclusión** que señala: *"Es Local lo que no es Federal"*[48], es decir que la legislación local podrá crear leyes sobre las materias que no se encuentren reservadas para la Federación encontrando su fundamento en el numeral 73 fracción XXI que dice:

DE LAS FACULTADES DEL CONGRESO

El artículo 73 establece las facultades que tiene el Congreso de la Unión; interesándonos sobre todo las siguientes fracciones:

XXI. Para establecer los delitos y las faltas contra la Federación y fijar los castigos que por ellos deban imponerse; expedir leyes generales en materias de secuestro, y trata de personas, que establezcan, como mínimo, los tipos penales y sus sanciones, la distribución de competencias y las formas de coordinación entre la Federación, el Distrito Federal, los Estados y los Municipios; así como legislar en materia de delincuencia organizada. Las autoridades federales podrán conocer también de los delitos del fuero común, cuando éstos tengan conexidad con delitos federales o delitos contra periodistas, personas o instalaciones que afecten, limiten o menoscaben el derecho a la información o las libertades de expresión o imprenta. En las materias concurrentes previstas en esta Constitución, las leyes federales establecerán los supuestos en que las autoridades del fuero común podrán conocer y resolver sobre delitos federales;

XXIII. Para expedir leyes que establezcan las bases de coordinación entre la Federación, el Distrito Federal, los Estados y los Municipios, así como para establecer y organizar a las instituciones de seguridad pública en materia federal, de conformidad con lo establecido en el artículo 21 de esta Constitución.

XXIV. Para expedir la Ley que regule la organización de la entidad de fiscalización superior de la Federación y las demás que normen la gestión, control y evaluación de los Poderes de la Unión y de los entes públicos federales;

[48] Ídem.

XXIX-F. Para expedir leyes tendientes a la promoción de la inversión mexicana, la regulación de la inversión extranjera, la transferencia de tecnología y la generación, difusión y aplicación de los conocimientos científicos y tecnológicos que requiere el desarrollo nacional.

XXIX-M. Para expedir leyes en materia de seguridad nacional, estableciendo los requisitos y límites a las investigaciones correspondientes.

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

XXIX-P. Expedir leyes que establezcan la concurrencia de la Federación, los Estados, el Distrito Federal y los Municipios, en el ámbito de sus respectivas competencias, en materia de derechos de niñas, niños y adolescentes, velando en todo momento por el interés superior de los mismos y cumpliendo con los tratados internacionales de la materia, de los que México sea parte.

Nuestra Carta Magna a partir de las antes citadas reformas, del 18 de Junio del 2008, en que precisan que los **Derechos Fundamentales del Hombre**, como lo contempla el artículo:

Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia (principio pro-homine) (pro persona).

Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

Está prohibida la esclavitud en los Estados Unidos Mexicanos. Los esclavos del extranjero que entren al territorio nacional alcanzarán, por este solo hecho, su libertad y la protección de las leyes.

Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Y pese al error tan grande en cuestión de técnica legislativa, por parte de Nuestro Congreso de la Unión que le ha costado a México innumerables críticas respecto de que en una Constitución, jamás se deben contener tipificación de delitos, éstos los encontramos en los dispositivos 16, 18, 19, 20, 22 y 73 Constitucionales respecto de la Delincuencia Organizada. Que citan:

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

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.

Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a

disposición de la autoridad más cercana y ésta con la misma prontitud, a la del Ministerio Público. Existirá un registro inmediato de la detención.

Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder.

En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley.

La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días.

Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.

Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.

En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia.

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de

forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración.

La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.

La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.

La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley.

En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán

exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.

Es importante arribar al estudio del numeral **18 Constitucional** pues establece que delitos merecen pena privativa de libertad y cuando habrá lugar a la prisión preventiva, y la organización del sistema penitenciario, y la base del respeto a los derechos humanos, del trabajo, la capacitación para el mismo, la educación, la salud y el deporte como medios para lograr la reinserción del sentenciado a la sociedad y procurar que no vuelva a delinquir, observando los beneficios que para él prevé la ley.

La Federación, los Estados y el Distrito Federal establecerán, en el ámbito de sus respectivas competencias, un sistema integral de justicia que será aplicable a quienes se atribuya la realización de una conducta tipificada como delito por las leyes penales y tengan entre doce años cumplidos y menos de dieciocho años de edad, en el que se garanticen los derechos fundamentales que reconoce esta Constitución para todo individuo, así como aquellos derechos específicos que por su condición de personas en desarrollo les han sido reconocidos. Las personas menores de doce años que hayan realizado una conducta prevista como delito en la ley, solo serán sujetos a rehabilitación y asistencia social.

El internamiento se utilizará solo como medida extrema y por el tiempo más breve que proceda, y podrá aplicarse únicamente a los adolescentes mayores de catorce años de edad, por la comisión de conductas antisociales calificadas como graves.

Los sentenciados, en los casos y condiciones que establezca la ley, podrán compurgar sus penas en los centros penitenciarios más cercanos a su domicilio, a fin de propiciar su reintegración a la comunidad como forma de reinserción social. **Esta disposición no aplicará en caso de delincuencia organizada y respecto de otros internos que requieran medidas especiales de seguridad**.

Para la reclusión preventiva y la ejecución de sentencias en materia de delincuencia organizada se destinarán centros especiales. Las autoridades competentes podrán restringir las comunicaciones de los inculpados y sentenciados por delincuencia organizada con terceros, salvo el acceso a su defensor, e imponer medidas de vigilancia especial a quienes se encuentren internos en estos establecimientos. Lo anterior podrá aplicarse a otros internos que requieran medidas especiales de seguridad, en términos de la ley.

El **Artículo 19 Constitucional**, nos hace un análisis de en qué casos el Ministerio Público sólo podrá solicitar al juez la prisión preventiva cuando otras medidas cautelares no sean suficientes para garantizar la comparecencia del imputado en el juicio, el desarrollo de la investigación, la protección de la víctima, de los testigos o de la comunidad, así como cuando el imputado esté siendo procesado o haya sido sentenciado previamente por la comisión de un delito doloso. **El juez ordenará la prisión preventiva, oficiosamente, en los casos de delincuencia organizada, homicidio doloso, violación, secuestro, trata de personas, delitos cometidos con medios violentos como armas y explosivos, así como delitos graves que determine la ley en contra de la seguridad de la nación, el libre desarrollo de la personalidad y de la salud**.

Artículo 20 Constitucional, ya nos habla del nuevo proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación.

A. De los principios generales:

I. El proceso penal tendrá por objeto el esclarecimiento de los hechos, proteger al inocente, procurar que el culpable no quede impune y que los daños causados por el delito se reparen;

II. Toda audiencia se desarrollará en presencia del juez, sin que pueda delegar en ninguna persona el desahogo y la valoración de las pruebas, la cual deberá realizarse de manera libre y lógica;

III. Para los efectos de la sentencia sólo se considerarán como prueba aquellas que hayan sido desahogadas en la audiencia de juicio. La ley establecerá las excepciones y los requisitos para admitir en juicio la prueba anticipada, que por su naturaleza requiera desahogo previo;

IV. El juicio se celebrará ante un juez que no haya conocido del caso previamente. La presentación de los argumentos y los elementos probatorios se desarrollará de manera pública, contradictoria y oral;

V. La carga de la prueba para demostrar la culpabilidad corresponde a la parte acusadora, conforme lo establezca el tipo penal. Las partes tendrán igualdad procesal para sostener la acusación o la defensa, respectivamente;

VI. Ningún juzgador podrá tratar asuntos que estén sujetos a proceso con cualquiera de las partes sin que esté presente la otra, respetando en todo momento el principio de contradicción, salvo las excepciones que establece esta Constitución;

VII. Una vez iniciado el proceso penal, siempre y cuando no exista oposición del inculpado, se podrá decretar su terminación anticipada en los supuestos y bajo las modalidades que determine la ley. Si el imputado reconoce ante la autoridad judicial, voluntariamente y con conocimiento de las consecuencias, su participación en el delito y existen medios de convicción suficientes para corroborar la imputación, el juez citará a audiencia de sentencia. La ley establecerá los beneficios que se podrán otorgar al inculpado cuando acepte su responsabilidad;

VIII. El juez sólo condenará cuando exista convicción de la culpabilidad del procesado;

IX. Cualquier prueba obtenida con violación de derechos fundamentales será nula, y

X. Los principios previstos en este artículo, se observarán también en las audiencias preliminares al juicio.

B. De los derechos de toda persona imputada:

I. A que se presuma su inocencia mientras no se declare su responsabilidad mediante sentencia emitida por el juez de la causa;

II. A declarar o a guardar silencio. Desde el momento de su detención se le harán saber los motivos de la misma y su derecho a guardar silencio, el cual no podrá ser utilizado en su perjuicio. Queda prohibida y será sancionada por la ley penal, toda incomunicación, intimidación o tortura. La confesión rendida sin la asistencia del defensor carecerá de todo valor probatorio;

III. A que se le informe, tanto en el momento de su detención como en su comparecencia ante el Ministerio Público o el juez, los hechos que se le imputan y los derechos que le asisten. Tratándose de delincuencia organizada, la autoridad judicial podrá autorizar que se mantenga en reserva el nombre y datos del acusador.

La ley establecerá beneficios a favor del inculpado, procesado o sentenciado que preste ayuda eficaz para la investigación y persecución de delitos en materia de delincuencia organizada;

IV. Se le recibirán los testigos y demás pruebas pertinentes que ofrezca, concediéndosele el tiempo que la ley estime necesario al efecto y auxiliándosele para obtener la comparecencia de las personas cuyo testimonio solicite, en los términos que señale la ley;

V. Será juzgado en audiencia pública por un juez o tribunal. La publicidad sólo podrá restringirse en los casos de excepción que determine la ley, por razones de seguridad nacional,

seguridad pública, protección de las víctimas, testigos y menores, cuando se ponga en riesgo la revelación de datos legalmente protegidos, o cuando el tribunal estime que existen razones fundadas para justificarlo.

En delincuencia organizada, las actuaciones realizadas en la fase de investigación podrán tener valor probatorio, cuando no puedan ser reproducidas en juicio o exista riesgo para testigos o víctimas. Lo anterior sin perjuicio del derecho del inculpado de objetarlas o impugnarlas y aportar pruebas en contra;

VI. Le serán facilitados todos los datos que solicite para su defensa y que consten en el proceso.

El imputado y su defensor tendrán acceso a los registros de la investigación cuando el primero se encuentre detenido y cuando pretenda recibírsele declaración o entrevistarlo. Asimismo, antes de su primera comparecencia ante juez podrán consultar dichos registros, con la oportunidad debida para preparar la defensa. A partir de este momento no podrán mantenerse en reserva las actuaciones de la investigación, salvo los casos excepcionales expresamente señalados en la ley cuando ello sea imprescindible para salvaguardar el éxito de la investigación y siempre que sean oportunamente revelados para no afectar el derecho de defensa;

VII. Será juzgado antes de cuatro meses si se tratare de delitos cuya pena máxima no exceda de dos años de prisión, y antes de un año si la pena excediere de ese tiempo, salvo que solicite mayor plazo para su defensa;

VIII. Tendrá derecho a una defensa adecuada por abogado, al cual elegirá libremente incluso desde el momento de su detención. Si no quiere o no puede nombrar un abogado, después de haber sido requerido para hacerlo, el juez le designará un defensor público. También tendrá derecho a que su defensor comparezca en todos los actos del proceso y éste tendrá obligación de hacerlo cuantas veces se le requiera, y

IX. En ningún caso podrá prolongarse la prisión o detención, por falta de pago de honorarios de defensores o por cualquiera otra prestación de dinero, por causa de responsabilidad civil o algún otro motivo análogo.

La prisión preventiva no podrá exceder del tiempo que como máximo de pena fije la ley al delito que motivare el proceso y en ningún caso será superior a dos años, salvo que su prolongación se deba al ejercicio del derecho de defensa del imputado. Si cumplido este

término no se ha pronunciado sentencia, el imputado será puesto en libertad de inmediato mientras se sigue el proceso, sin que ello obste para imponer otras medidas cautelares.

En toda pena de prisión que imponga una sentencia, se computará el tiempo de la detención.

C. De los derechos de la víctima o del ofendido:

I. Recibir asesoría jurídica; ser informado de los derechos que en su favor establece la Constitución y, cuando lo solicite, ser informado del desarrollo del procedimiento penal;

II. Coadyuvar con el Ministerio Público; a que se le reciban todos los datos o elementos de prueba con los que cuente, tanto en la investigación como en el proceso, a que se desahoguen las diligencias correspondientes, y a intervenir en el juicio e interponer los recursos en los términos que prevea la ley.

Cuando el Ministerio Público considere que no es necesario el desahogo de la diligencia, deberá fundar y motivar su negativa;

III. Recibir, desde la comisión del delito, atención médica y psicológica de urgencia;

IV. Que se le repare el daño. En los casos en que sea procedente, el Ministerio Público estará obligado a solicitar la reparación del daño, sin menoscabo de que la víctima u ofendido lo pueda solicitar directamente, y el juzgador no podrá absolver al sentenciado de dicha reparación si ha emitido una sentencia condenatoria.

La ley fijará procedimientos ágiles para ejecutar las sentencias en materia de reparación del daño;

V. Al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa.

El Ministerio Público deberá garantizar la protección de víctimas, ofendidos, testigos y en general todas los sujetos que intervengan en el proceso. Los jueces deberán vigilar el buen cumplimiento de esta obligación;

VI. Solicitar las medidas cautelares y providencias necesarias para la protección y restitución de sus derechos, y

VII. Impugnar ante autoridad judicial las omisiones del Ministerio Público en la investigación de los delitos, así como las resoluciones de reserva, no ejercicio, desistimiento de la acción penal o suspensión del procedimiento cuando no esté satisfecha la reparación del daño.

El Artículo 22 Constitucional, nos habla de la prohibición de la tortura, la confiscación de bienes y cualesquiera otras penas inusitadas y trascendentales. Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado.

No se considerará confiscación la aplicación de bienes de una persona cuando sea decretada para el pago de multas o impuestos, ni cuando la decrete una autoridad judicial para el pago de responsabilidad civil derivada de la comisión de un delito. **Tampoco se considerará confiscación el decomiso que ordene la autoridad judicial de los bienes en caso de enriquecimiento ilícito en los términos del artículo 109, la aplicación a favor del Estado de bienes asegurados que causen abandono en los términos de las disposiciones aplicables, ni la de aquellos bienes cuyo dominio se declare extinto en sentencia. En el caso de extinción de dominio se establecerá un procedimiento que se regirá por las siguientes reglas:**

I. Será jurisdiccional y autónomo del de materia penal;

II. Procederá en los casos de delincuencia organizada, delitos contra la salud, secuestro, robo de vehículos y trata de personas, respecto de los bienes siguientes:

a) Aquellos que sean instrumento, objeto o producto del delito, aún cuando no se haya dictado la sentencia que determine la responsabilidad penal, pero existan elementos suficientes para determinar que el hecho ilícito sucedió.

b) Aquellos que no sean instrumento, objeto o producto del delito, pero que hayan sido utilizados o destinados a ocultar o mezclar bienes producto del delito, siempre y cuando se reúnan los extremos del inciso anterior.

c) Aquellos que estén siendo utilizados para la comisión de delitos por un tercero, si su dueño tuvo conocimiento de ello y no lo notificó a la autoridad o hizo algo para impedirlo.

d) Aquellos que estén intitulados a nombre de terceros, pero existan suficientes elementos para determinar que son producto de delitos patrimoniales o de delincuencia organizada, y el acusado por estos delitos se comporte como dueño.

III. Toda persona que se considere afectada podrá interponer los recursos respectivos para demostrar la procedencia lícita de los bienes y su actuación de buena fe, así como que estaba impedida para conocer la utilización ilícita de sus bienes.

Nuestra Carta Magna, contempla en sus artículos 13, 14, 17, 21, 24 el resto de las Garantías en Materia Penal que se nos otorgan en cuestión de Seguridad Jurídica y al tenor dicen:

Artículo 13. Nadie puede ser juzgado por leyes privativas ni por tribunales especiales. Ninguna persona o corporación puede tener fuero, ni gozar más emolumentos que los que sean compensación de servicios públicos y estén fijados por la ley. Subsiste el fuero de guerra para los delitos y faltas contra la disciplina militar; pero los tribunales militares en ningún caso y por ningún motivo podrán extender su jurisdicción sobre personas que no pertenezcan al Ejército. Cuando en un delito o falta del orden militar estuviese complicado un paisano, conocerá del caso la autoridad civil que corresponda.

Artículo 14. A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna.

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

En los juicios del 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 trata.

En los juicios del orden civil, la sentencia definitiva deberá ser conforme a la letra o a la interpretación jurídica de la ley, y a falta de ésta se fundará en los principios generales del derecho.

Artículo 17. Ninguna persona podrá hacerse justicia por sí misma, ni ejercer violencia para reclamar su derecho.

Toda persona tiene derecho a que se le administre justicia por tribunales que estarán expeditos para impartirla en los plazos y términos que fijen las leyes, emitiendo sus resoluciones de manera pronta, completa e imparcial. Su servicio será gratuito, quedando, en consecuencia, prohibidas las costas judiciales.

El Congreso de la Unión expedirá las leyes que regulen las acciones colectivas. Tales leyes determinarán las materias de aplicación, los procedimientos judiciales y los mecanismos de reparación del daño. Los jueces federales conocerán de forma exclusiva sobre estos procedimientos y mecanismos.

Las leyes preverán mecanismos alternativos de solución de controversias. En la materia penal regularán su aplicación, asegurarán la reparación del daño y establecerán los casos en los que se requerirá supervisión judicial.

Las sentencias que pongan fin a los procedimientos orales deberán ser explicadas en audiencia pública previa citación de las partes.

Las leyes federales y locales establecerán los medios necesarios para que se garantice la independencia de los tribunales y la plena ejecución de sus resoluciones.

La Federación, los Estados y el Distrito Federal garantizarán la existencia de un servicio de defensoría pública de calidad para la población y asegurarán las condiciones para un servicio profesional de carrera para los defensores. Las percepciones de los defensores no podrán ser inferiores a las que correspondan a los agentes del Ministerio Público.

Nadie puede ser aprisionado por deudas de carácter puramente civil.

Artículo 21. La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.

El ejercicio de la acción penal ante los tribunales corresponde al Ministerio Público. La ley determinará los casos en que los particulares podrán ejercer la acción penal ante la autoridad judicial.

La imposición de las penas, su modificación y duración son propias y exclusivas de la autoridad judicial.

Compete a la autoridad administrativa la aplicación de sanciones por las infracciones de los reglamentos gubernativos y de policía, las que únicamente consistirán en multa, arresto hasta por treinta y seis horas o en trabajo a favor de la comunidad; pero si el infractor no pagare la multa que se le hubiese impuesto, se permutará esta por el arresto correspondiente, que no excederá en ningún caso de treinta y seis horas.

Si el infractor de los reglamentos gubernativos y de policía fuese jornalero, obrero o trabajador, no podrá ser sancionado con multa mayor del importe de su jornal o salario de un día.

Tratándose de trabajadores no asalariados, la multa que se imponga por infracción de los reglamentos gubernativos y de policía, no excederá del equivalente a un día de su ingreso.

El Ministerio Público podrá considerar criterios de oportunidad para el ejercicio de la acción penal, en los supuestos y condiciones que fije la ley.

El Ejecutivo Federal podrá, con la aprobación del Senado en cada caso, reconocer la jurisdicción de la Corte Penal Internacional.

La seguridad pública es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución.

Las instituciones de seguridad pública serán de carácter civil, disciplinado y profesional. El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno deberán coordinarse entre sí para cumplir los objetivos de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública, que estará sujeto a las siguientes bases mínimas:

a) La regulación de la selección, ingreso, formación, permanencia, evaluación, reconocimiento y certificación de los integrantes de las instituciones de seguridad pública. La operación y desarrollo de estas acciones será competencia de la Federación, el Distrito Federal, los Estados y los municipios en el ámbito de sus respectivas atribuciones.

b) El establecimiento de las bases de datos criminalísticos y de personal para las instituciones de seguridad pública. Ninguna persona podrá ingresar a las instituciones de seguridad pública si no ha sido debidamente certificado y registrado en el sistema.

c) La formulación de políticas públicas tendientes a prevenir la comisión de delitos.

d) Se determinará la participación de la comunidad que coadyuvará, entre otros, en los procesos de evaluación de las políticas de prevención del delito así como de las instituciones de seguridad pública.

e) Los fondos de ayuda federal para la seguridad pública, a nivel nacional serán aportados a las entidades federativas y municipios para ser destinados exclusivamente a estos fines.

Artículo 23. Ningún juicio criminal deberá tener más de tres instancias. Nadie puede ser juzgado dos veces por el mismo delito, ya sea que en el juicio se le absuelva o se le condene. Queda prohibida la práctica de absolver de la instancia.

Artículo 24. Todo hombre es libre para profesar la creencia religiosa que más le agrade y para practicar las ceremonias, devociones o actos del culto respectivo, siempre que no constituyan un delito o falta penados por la ley.

El Congreso no puede dictar leyes que establezcan o prohíban religión alguna.

Los actos religiosos de culto público se celebrarán ordinariamente en los templos. Los que extraordinariamente se celebren fuera de éstos se sujetarán a la ley reglamentaria.

Existen Leyes Federales que contemplan y utilizan lo relativo a "Medio electrónico o Informático de formas muy distintas como lo vamos a verificar, pero vale la pena mencionar que nunca se utiliza la palabra Internet y son:

- La Ley de Propiedad Industrial. Artículos 28 y 29 Constitucional
- La Ley Federal de Derechos de Autor. Artículo 28 Constitucional
- Ley de Instituciones de Crédito
- La Ley Federal de Telecomunicaciones.
- La Ley Federal de Protección al Consumidor
- La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Articulo 6 y 7 Constitucional
- La Ley de Información y Estadística y Geografía
- Ley Orgánica del Poder Judicial de la Federación
- Ley Federal Contra la Delincuencia Organizada. Artículo 16 Constitucional
- Código Fiscal de la Federación
- Código de Comercio
- Código Penal Federal
- Código Civil Federal
- Código Federal de Procedimientos Civiles
- Ley General del Sistema Nacional de Seguridad Pública. Artículo 21 Constitucional.

1.6 LEY DE LA PROPIEDAD INDUSTRIAL

La Ley de Propiedad Industrial en sus dispositivos 82 y 83 que se refieren a Los Secretos Industriales, y nos dicen:

Artículo 82.- Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerará que entre al dominio público o que sea divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad. *Artículo reformado DOF 02-08-1994*

Artículo 83.- La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

Cabe destacar que esta Ley se tuvo que reformar a efecto de tipificar su relación con delitos informáticos y electrónicos, estas reformas se publicaron en el Diario Oficial de la Federación el 17 de Mayo del año 1999. Y fueron en relación con los numerales 223, 223 bis y 224 que dicen:

Artículo 223. SON DELITOS:

I. Reincidir en las conductas previstas en las fracciones II a XXII del Artículo 213 de esta Ley, una vez que la primera sanción administrativa impuesta por esta razón haya quedado firme;

II. Falsificar, en forma dolosa y con fin de especulación comercial, marcas protegidas por esta Ley; *Fracción reformada DOF 17-05-1999*

III. Producir, almacenar, transportar, introducir al país, distribuir o vender, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley, así como aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de objetos que ostenten falsificaciones de marcas protegidas por esta Ley; *Fracción adicionada DOF 17-05-1999*

IV. Revelar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto; *Fracción reformada DOF 17-05-1999 (se recorre)*

V. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y *Fracción reformada DOF 17-05-1999 (se recorre)*

VI. Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado. *Fracción reformada DOF 17-05-1999 (se recorre)*

Los delitos previstos en este artículo se perseguirán por querella de parte ofendida. *Artículo reformado DOF 02-08-1994*

Artículo 223 Bis.- Se impondrá de dos a seis años de prisión y multa de cien a diez mil días de salario mínimo general vigente en el Distrito Federal, al que venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley. Si la venta se

realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en los artículos 223 y 224 de esta Ley. Este delito se perseguirá de oficio. *Artículo adicionado DOF 17-05-1999. Reformado DOF 28-06-2010*

Artículo 224.- Se impondrán de dos a seis años de prisión y multa por el importe de cien a diez mil días de salario mínimo general vigente en el Distrito Federal, a quien cometa alguno de los delitos que se señalan en las fracciones I, IV, V o VI del artículo 223 de esta Ley. En el caso de los delitos previstos en las fracciones II o III del mismo artículo 223, se impondrán de tres a diez años de prisión y multa de dos mil a veinte mil días de salario mínimo general vigente en el Distrito Federal. *Artículo reformado DOF 02-08-1994, 17-05-1999*

1.7 LEY FEDERAL DEL DERECHO DE AUTOR

Esta Ley es Reglamentaria del artículo 28 de Nuestra Constitución Política de los Estados Unidos Mexicanos tal como lo precisa su artículo 1 que a la letra dice:

Artículo 1o.- La presente Ley, reglamentaria del artículo 28 constitucional, tiene por objeto la salvaguarda y promoción del acervo cultural de la Nación; protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual.

Esta Ley del Derecho de Autor fue publicada por decreto el día 18 de Diciembre de 1996, ley que tuvo su última reforma el día 23 de Julio del 2003, en la ley en comento en sus numerales 4 y 6 se precisa todo lo relativo a las obras que van a ser protegidas y se citan de la siguiente manera:

Artículo 4o.- Las obras objeto de protección pueden ser:

A. Según su autor:

I. Conocido: Contienen la mención del nombre, signo o firma con que se identifica a su autor;

II. Anónimas: Sin mención del nombre, signo o firma que identifica al autor, bien por voluntad del mismo, bien por no ser posible tal identificación, y

III. Seudónimas: Las divulgadas con un nombre, signo o firma que no revele la identidad del autor;

B. Según su comunicación:

I. Divulgadas: Las que han sido hechas del conocimiento público por primera vez en cualquier forma o medio, bien en su totalidad, bien en parte, bien en lo esencial de su contenido o, incluso, mediante una descripción de la misma;

II. Inéditas: Las no divulgadas, y

III. Publicadas:

a) Las que han sido editadas, cualquiera que sea el modo de reproducción de los ejemplares, siempre que la cantidad de éstos, puestos a disposición del público, satisfaga razonablemente las necesidades de su explotación, estimadas de acuerdo con la naturaleza de la obra, y

b) Las que han sido puestas a disposición del público mediante su almacenamiento por medios electrónicos que permitan al público obtener ejemplares tangibles de la misma, cualquiera que sea la índole de estos ejemplares;

C. Según su origen:

I. Primigenias: Las que han sido creadas de origen sin estar basadas en otra preexistente, o que estando basadas en otra, sus características permitan afirmar su originalidad, y

II. Derivadas: Aquellas que resulten de la adaptación, traducción u otra transformación de una obra primigenia;

D. Según los creadores que intervienen:

I. Individuales: Las que han sido creadas por una sola persona;

II. De colaboración: Las que han sido creadas por varios autores, y

III. Colectivas: Las creadas por la iniciativa de una persona física o moral que las publica y divulga bajo su dirección y su nombre y en las cuales la contribución personal de los diversos autores que han participado en su elaboración se funde en el conjunto con vistas al cual ha sido concebida, sin que sea posible atribuir a cada uno de ellos un derecho distinto e indiviso sobre el conjunto realizado.

Artículo 6o.- Fijación es la incorporación de letras, números, signos, sonidos, imágenes y demás elementos en que se haya expresado la obra, o de las representaciones digitales de aquellos, que en cualquier forma o soporte material, incluyendo los electrónicos, permita su percepción, reproducción u otra forma de comunicación.

El dispositivo 27 de la citada ley nos menciona como el titular del derecho jurídico protegido que en este caso es el "Patrimonio", puede autorizar o prohibir su publicación o reproducción total o parcial y lo señala:

Artículo 27.- Los titulares de los derechos patrimoniales podrán autorizar o prohibir:

I. La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico, fotográfico u otro similar. *Fracción reformada DOF 23-07-2003*

II. La comunicación pública de su obra a través de cualquiera de las siguientes maneras:

a) La representación, recitación y ejecución pública en el caso de las obras literarias y artísticas;

b) La exhibición pública por cualquier medio o procedimiento, en el caso de obras literarias y artísticas, y

c) El acceso público por medio de la telecomunicación;

III. La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, incluyendo la transmisión o retransmisión de las obras por:

a) Cable;

b) Fibra óptica;

c) Microondas;

d) Vía satélite, o

e) Cualquier otro medio conocido o por conocerse. *Inciso reformado DOF 23-07-2003*

IV. La distribución de la obra, incluyendo la venta u otras formas de transmisión de la propiedad de los soportes materiales que la contengan, así como cualquier forma de transmisión de uso o explotación. Cuando la distribución se lleve a cabo mediante venta, este derecho de oposición se entenderá agotado efectuada la primera venta, salvo en el caso expresamente contemplado en el artículo 104 de esta Ley;

V. La importación al territorio nacional de copias de la obra hechas sin su autorización;

VI. La divulgación de obras derivadas, en cualquiera de sus modalidades, tales como la traducción, adaptación, paráfrasis, arreglos y transformaciones, y

VII. Cualquier utilización pública de la obra salvo en los casos expresamente establecidos en esta Ley.

Sobre la protección de los programas de cómputo y de la base de datos la ley en comento menciona lo siguiente de los numerales 101 al 114:

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 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.

1.8 LEY DE INSTITUCIONES DE CRÉDITO

Estas Instituciones han sido en extremo protegidas por su importancia en nuestro país por los legisladores, sin embargo se han cometido varios errores al tratar de proteger a las Instituciones de crédito en lo referente a que si bien cierto el bien jurídico que afecta a estas instituciones, son los patrimoniales, llevados a cabo mediante los delitos informáticos, también lo es que ha habido confusiones para protegerlo, en virtud de que se ha tratado de tipificarlo en el delito de "fraude", cuando no se debe encontrar en ese tipo penal sino en el de "Robo", puesto que una de las características para que encuadre en el tipo de fraude es el engaño, las máquinas no son susceptibles de caer en este tipo de errores como sucede con las personas físicas o morales. Por lo que el acceso a un sistema de información para realizar operaciones, transferencias o movimiento de dinero o valores no puede ni debe considerarse "fraude", sino

"robo" o "en su caso más preciso "Robo Informático", en el cual se utiliza la computación como un medio o una herramienta para cometer un ilícito.

"El 17 de Junio de 2003 La Suprema Corte de Justicia de la Nación declaro inconstitucional el delito de fraude por acceso informático al sistema financiero incluido indebidamente por la Asamblea Legislativa del Distrito Federal en el Código Penal Capitalino. La Primera Sala de la Corte consideró que por ser una conducta que afecta al Sistema Financiero, únicamente el Congreso de la Unión, puede legislar sobre el tema. Los Ministros de la mayoría, declararon que el Artículo 387 fracción 22 del Anterior Código Penal es Inconstitucional".[49]

Esta ley hace referencia a los Medios electrónicos y al Internet en los artículos siguientes:

Artículo 48 Bis 4.- Las instituciones deberán mantener en su página electrónica en la red mundial "Internet", la información relativa al importe de las comisiones que cobran por los servicios que ofrecen al público relacionados con el uso de tarjetas de débito, tarjetas de crédito, cheques y órdenes de transferencias de fondos.

Asimismo, en sus sucursales deberán contar con la referida información en carteles, listas y folletos visibles de forma ostensible, así como permitir que ésta se obtenga a través de un medio electrónico ubicado en dichas sucursales, a fin de que cualquier persona que la solicite esté en posibilidad de consultarla gratuitamente.

Para garantizar la protección de los intereses del público, la determinación de comisiones y tarifas por los servicios que prestan las instituciones de crédito, se sujetará lo dispuesto por la Ley para la Transparencia y Ordenamiento de los Servicios Financieros. *Artículo adicionado DOF 15-06-2007.*

Artículo 109 Bis 8. En ejercicio de sus facultades sancionadoras, las Comisiones Nacionales Bancaria y de Valores y para la Protección y Defensa de los Usuarios de Servicios Financieros, ajustándose a los lineamientos que aprueben sus Juntas de Gobierno, deberán hacer del conocimiento del público en general, **a través de su portal de Internet**, las sanciones que al efecto impongan por infracciones a esta Ley, una vez que dichas resoluciones hayan quedado firmes o sean cosa juzgada, para lo cual deberán señalar exclusivamente la

[49] Fuentes, Víctor, "*Revocan reforma sobre Fraude Cibernético*", Diario Reforma, México, 17 de Junio del 2003.

denominación o razón social del infractor, el precepto infringido y la sanción. *Artículo adicionado DOF 06-02-2008. Reformado DOF 25-06-2009*

Artículo 110 Bis 10.- Las notificaciones por edictos se efectuarán en el supuesto de que el interesado haya desaparecido, hubiere fallecido, se desconozca su domicilio o exista imposibilidad de acceder a él, y no tenga representante conocido o domicilio en territorio nacional o se encuentre en el extranjero sin haber dejado representante.

Para tales efectos, se publicará por tres veces consecutivas un resumen del oficio respectivo, en un periódico de circulación nacional, **sin perjuicio de que la autoridad financiera que notifique difunda el edicto en la página electrónica de la red mundial denominada Internet que corresponda a la autoridad financiera que notifique**; indicando que el oficio original se encuentra a su disposición en el domicilio que también se señalará en dicho edicto. *Artículo adicionado DOF 06-02-2008*

Artículo 112 Bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:

I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en

alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada. *Artículo adicionado DOF 17-05-1999. Reformado DOF 26-06-2008*

Artículo 112 Ter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que posea, adquiera, utilice, comercialice o distribuya, cualquiera de los objetos a que se refiere el párrafo primero del artículo 112 Bis de esta Ley, a sabiendas de que estén alterados o falsificados. *Artículo adicionado DOF 26-06-2008*

Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o

II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada. *Artículo adicionado DOF 26-06-2008*

Artículo 112 Quintus.- La pena que corresponda podrá aumentarse hasta en una mitad más, si quien realice cualquiera de las conductas señaladas en los artículos 112 Bis, 112 Ter y 112 Quáter, tiene el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier institución de crédito, o las realice dentro de los dos años siguientes de haberse separado de alguno de dichos cargos, o sea propietario o empleado de cualquier entidad mercantil que a cambio de bienes o servicios reciba como contraprestación el pago a través de cualquiera de los instrumentos mencionados en el artículo 112 Bis. *Artículo adicionado DOF 26-06-2008*

1.9 LEY FEDERAL DE TELECOMUNICACIONES

Esta ley tiene competencia en el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite según lo observaremos del artículo 1 al 5 de la presente ley que al tenor señala:

Artículo 1. La presente Ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite.

Artículo 2. Corresponde al Estado la rectoría en materia de telecomunicaciones, a cuyo efecto protegerá la seguridad y la soberanía de la Nación.

En todo momento el Estado mantendrá el dominio sobre el espectro radioeléctrico y las posiciones orbitales asignadas al país.

Artículo 3. Para los efectos de esta Ley se entenderá por:

I. Banda de frecuencias: porción del espectro radioeléctrico que contiene un conjunto de frecuencias determinadas;

II. Espectro radioeléctrico: el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz;

III. Estación terrena: la antena y el equipo asociado a ésta que se utiliza para transmitir o recibir señales de comunicación vía satélite;

IV. Frecuencia: número de ciclos que por segundo efectúa una onda del espectro radioeléctrico;

V. Homologación: acto por el cual la Secretaría reconoce oficialmente que las especificaciones de un producto destinado a telecomunicaciones satisfacen las normas y requisitos establecidos, por lo que puede ser conectado a una red pública de telecomunicaciones, o hacer uso del espectro radioeléctrico;

VI. Orbita satelital: trayectoria que recorre un satélite al girar alrededor de la tierra;

VII. Posiciones orbitales geoestacionarias: ubicaciones en una órbita circular sobre el Ecuador que permiten que un satélite gire a la misma velocidad de rotación de la tierra, permitiendo que el satélite mantenga en forma permanente la misma latitud y longitud;

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

IX. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

X. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

XI. Secretaría: la Secretaría de Comunicaciones y Transportes;

XII. Servicios de valor agregado: los que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada;

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

XIV. Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

XV. Servicio de radiodifusión: servicio de telecomunicaciones definido por el artículo 2 de la Ley Federal de Radio y Televisión, y *Fracción adicionada DOF 11-04-2006*

XVI. Servicio de radio y televisión: el servicio de audio o de audio y video asociado que se presta a través de redes públicas de telecomunicaciones, así como el servicio de radiodifusión. *Fracción adicionada DOF 11-04-2006*

XVII. Localización geográfica en tiempo real: es la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada. *Fracción adicionada DOF 17-04-2012*

Artículo 4. Para los efectos de esta Ley, son vías generales de comunicación el espectro radioeléctrico, las redes de telecomunicaciones y los sistemas de comunicación vía satélite.

Artículo 5. Las vías generales de comunicación materia de esta Ley y los servicios que en ellas se presten son de jurisdicción federal.

Para los efectos de esta Ley se considera de interés público la instalación, operación, y mantenimiento de cableado subterráneo y aéreo y equipo destinado al servicio de las redes públicas de telecomunicaciones, debiéndose cumplir las disposiciones estatales y municipales en materia de desarrollo urbano y protección ecológica aplicables.

No obstante a que ésta Ley es la encargada de la regulación de todo tipo de vías de comunicación, no hace referencia específica al Internet y en ningún artículo hay especificaciones de este medio como tal.

Sin embargo si hay precisiones en el artículo 44 de la Ley Federal de Telecomunicaciones en cuanto a asignar a responsables operativos en la función de colaborar con las autoridades en la localización geográfica, en tiempo real, de los equipos de comunicación móvil que se encuentren relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas, en que se cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación.

Los concesionarios están obligados a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen.

Realizar estudios e investigaciones que tengan por objeto el desarrollo de medidas tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos. Los concesionarios podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones.
Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Congreso de la Unión y a la Comisión.

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

I. Permitir a concesionarios y permisionarios que comercialicen los servicios y capacidad que hayan adquirido de sus redes públicas de telecomunicaciones;

II. Abstenerse de interrumpir el tráfico de señales de telecomunicaciones entre concesionarios interconectados, sin la previa autorización de la Secretaría;

III. Abstenerse de realizar modificaciones a su red que afecten el funcionamiento de los equipos de los usuarios o de las redes con las que esté interconectada, sin contar con la anuencia de las partes afectadas y sin la aprobación previa de la Secretaría;

IV. Llevar contabilidad separada por servicios y atribuirse a sí mismo y a sus subsidiarias y filiales, tarifas desagregadas y no discriminatorias por los diferentes servicios de interconexión;

V. Permitir la portabilidad de números cuando, a juicio de la Secretaría, esto sea técnica y económicamente factible;

VI. Proporcionar de acuerdo a lo que establezcan los títulos de concesión respectivos, los servicios al público de manera no discriminatoria;

VII. Prestar los servicios sobre las bases tarifarias y de calidad contratadas con los usuarios;

VIII. Permitir la conexión de equipos terminales, cableados internos y redes privadas de los usuarios, que cumplan con las normas establecidas;

IX. Abstenerse de establecer barreras contractuales, técnicas o de cualquier naturaleza a la conexión de cableados ubicados dentro del domicilio de un usuario con otros concesionarios de redes públicas; *Fracción reformada DOF 09-02-2009*

X. Actuar sobre bases no discriminatorias al proporcionar información de carácter comercial, respecto de sus suscriptores, a filiales, subsidiarias o terceros; *Fracción reformada DOF 09-02-2009*

XI. Se deroga *Fracción adicionada DOF 09-02-2009. Derogada DOF 17-04-2012*

XII. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

b) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

c) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

d) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

e) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

f) La obligación de conservación de datos a que se refiere la presente fracción cesa a los doce meses, contados a partir de la fecha en que se haya producido la comunicación. Los concesionarios tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control; *Fracción adicionada DOF 09-02-2009*

XIII. Entregar los datos conservados, al Procurador General de la República o Procuradores Generales de Justicia de las Entidades Federativas, cuando realicen funciones de investigación de los delitos de extorsión, amenazas, secuestro, en cualquiera de sus modalidades o de algún delito grave o relacionado con la delincuencia organizada, en sus respectivas competencias. Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en el párrafo anterior, cualquier uso distinto será sancionado por las autoridades competentes en Términos administrativos y penales que resulten. Los concesionarios están obligados a entregar la información dentro del plazo máximo de setenta y dos horas siguientes contados a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad judicial.

El Reglamento establecerá los procedimientos, mecanismos y medidas de seguridad que los concesionarios deberán adoptar para identificar al personal facultado para acceder a la información, así como las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos a los legalmente autorizados, su destrucción accidental o ilícita o su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizado; *Fracción adicionada DOF 09-02-2009*

XIV. Realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier modalidad reportadas por los clientes, utilizando cualquier medio, como robadas o extraviadas; así como realizar la suspensión inmediata del servicio de telefonía para efectos de aseguramiento cuando así lo instruya la Comisión Federal de Telecomunicaciones, de conformidad con lo establecido en el Código Federal de Procedimientos Penales.

Los concesionarios están obligados a establecer procedimientos que permitan recibir reportes y acreditar la titularidad de líneas de forma expedita. *Fracción adicionada DOF 09-02-2009. Reformada DOF 30-11-2010, 17-04-2012*

XV. Desactivar permanentemente el servicio de telefonía o radiocomunicación de los equipos de comunicación móvil reportados por los clientes o usuarios como robados o extraviados. Dicho reporte deberá incluir el código de identidad de fabricación del equipo.

Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios. *Fracción adicionada DOF 09-02-2009. Reformada DOF 30-11-2010, 17-04-2012*

XVI. Contar con sistemas, equipos y tecnologías que permitan la ubicación o localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea. *Fracción adicionada DOF 17-04-2012*

XVII. Asignar un área con responsables operativos en la función de colaborar con las autoridades en la localización geográfica, en tiempo real, de los equipos de comunicación móvil que se encuentren relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas. *Fracción adicionada DOF 17-04-2012*

XVIII. Colaborar con las autoridades competentes para que en el ámbito técnico operativo se cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación.

El bloqueo de señales a que se refiere el párrafo anterior se hará sobre todas las bandas de frecuencia que se utilicen para la recepción en los equipos terminales de comunicación y en ningún caso excederá de veinte metros fuera de las instalaciones de los centros o establecimientos a fin de garantizar la continuidad y seguridad de los servicios a los usuarios externos. En la colaboración que realicen los concesionarios se deberán considerar los elementos técnicos de reemplazo, mantenimiento y servicio.

Los concesionarios están obligados a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen. ***Fracción adicionada DOF 30-11-2010. Reformada y recorrida DOF 17-04-2012***

XIX. Garantizar que los equipos de comunicación móvil cuenten con una combinación de teclas que al ser digitadas permitan a los clientes o usuarios enviar señales de auxilio.

La Comisión mediante disposiciones administrativas de carácter general determinará una marcación corta conformada por signos poco habituales para evitar que la señal de auxilio sea producto de error.

Las señales de auxilio serán enviadas de forma automática a un sistema nacional de atención de emergencias a fin de garantizar la intervención oportuna de las autoridades de la federación, de las entidades federativas o de los municipios, en el ámbito de su competencia. *Fracción adicionada DOF 17-04-2012*

XX. Realizar estudios e investigaciones que tengan por objeto el desarrollo de medidas tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos. Los concesionarios podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones.

Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Congreso de la Unión y a la Comisión. ***Fracción adicionada DOF 17-04-2012***

1.10 LEY FEDERAL DE PROTECCION AL CONSUMIDOR

Debido a todos los avances Tecnológicos que ha habido La Ley Federal del Consumidor tuvo que ser reformada y adicionada en sus artículos 1 fracción VIII, 16, 17, 18, 18 bis, 24 fracción IX, al igual que el dispositivo 76 bis, del 29 de Mayo del año 2000 que establecen:

ARTÍCULO 1.- La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas, convenios o estipulaciones en contrario. *Párrafo reformado DOF 04-02-2004.*

El objeto de esta ley es promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores. *Párrafo reformado DOF 04-02-2004*

Son principios básicos en las relaciones de consumo:

I. La protección de la vida, salud y seguridad del consumidor contra los riesgos provocados por productos, prácticas en el abastecimiento de productos y servicios considerados peligrosos o nocivos; *Fracción reformada DOF 04-02-2004*

II. La educación y divulgación sobre el consumo adecuado de los productos y servicios, que garanticen la libertad para escoger y la equidad en las contrataciones;

III. La información adecuada y clara sobre los diferentes productos y servicios, con especificación correcta de cantidad, características, composición, calidad y precio, así como sobre los riesgos que representen;

IV. La efectiva prevención y reparación de daños patrimoniales y morales, individuales o colectivos;

V. El acceso a los órganos administrativos con vistas a la prevención de daños patrimoniales y morales, individuales o colectivos, garantizando la protección jurídica, económica, administrativa y técnica a los consumidores; *Fracción reformada DOF 04-02-2004*

VI. El otorgamiento de información y de facilidades a los consumidores para la defensa de sus derechos; *Fracción reformada DOF 04-02-2004*

VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios.

VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados; ***Fracción adicionada DOF 29-05-2000. Reformada DOF 04-02-2004, 19-08-2010***

IX. El respeto a los derechos y obligaciones derivados de las relaciones de consumo y las medidas que garanticen su efectividad y cumplimiento; y *Fracción adicionada DOF 04-02-2004. Reformada DOF 19-08-2010*

X. La protección de los derechos de la infancia, adultos mayores, personas con discapacidad e indígenas. *Fracción adicionada DOF 19-08-2010*

Los derechos previstos en esta ley no excluyen otros derivados de tratados o convenciones internacionales de los que México sea signatario; de la legislación interna ordinaria; de reglamentos expedidos por las autoridades administrativas competentes; así como de los que deriven de los principios generales de derecho, la analogía, las costumbres y la equidad.

ARTÍCULO 16.- Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información. *Párrafo reformado DOF 04-02-2004*

Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores. *Párrafo adicionado DOF 04-02-2004*

ARTÍCULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría. *Párrafo reformado DOF 04-02-2004*

El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial. *Párrafo adicionado DOF 04-02-2004*

ARTÍCULO 18.- La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. **Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito**. Artículo reformado DOF 04-02-2004 **LEY**

ARTÍCULO 18 BIS.- Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros. *Artículo adicionado DOF 04-02-2004*

1.11 LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

Esta ley es uno de los grandes intentos del Legislador para Modernizar y poner a la vanguardia a México, por lo que esta Ley tiene sus fundamentos en los artículos 6 y 7 Constitucionales que dicen:

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley.

El derecho a la información será garantizado por el Estado.

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos.

Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

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

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delito de prensa, sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos.

Al tratar de dar claridad a los movimientos efectuados por los Poderes de Gobierno en sus diversas jerarquías por lo que analizaremos el acceso a la información, la información reservada y confidencial y la protección de datos personales mismos que se encuentran contemplados desde el numeral 1 al 26 que citan:

DISPOSICIONES GENERALES

Artículo 1. La presente Ley es de orden público. Tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

Artículo 2. Toda la información gubernamental a que se refiere esta Ley es pública y los particulares tendrán acceso a la misma en los términos que ésta señala.

Artículo 3. Para los efectos de esta Ley se entenderá por:

I. Comités: Los Comités de Información de cada una de las dependencias y entidades mencionados en el Artículo 29 de esta Ley o el titular de las referidas en el Artículo 31;

II. Datos personales: Cualquier información concerniente a una persona física identificada o identificable; *Fracción reformada DOF 05-07-2010*

III. Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de

las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;

IV. Dependencias y entidades: Las señaladas en la Ley Orgánica de la Administración Pública Federal, incluidas la Presidencia de la República, los órganos administrativos desconcentrados, así como la Procuraduría General de la República;

V. Información: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título;

VI. Información reservada: Aquella información que se encuentra temporalmente sujeta a alguna de las excepciones previstas en los Artículos 13 y 14 de esta Ley;

VII. Instituto: El Instituto Federal de Acceso a la Información y Protección de Datos, establecido en el Artículo 33 de esta Ley; *Fracción reformada DOF 05-07-2010*

VIII. Ley: La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

IX. Órganos constitucionales autónomos: El Instituto Federal Electoral, la Comisión Nacional de los Derechos Humanos, el Banco de México, las universidades y las demás instituciones de educación superior a las que la ley otorgue autonomía y cualquier otro establecido en la Constitución Política de los Estados Unidos Mexicanos;

X. Reglamento: El Reglamento respecto al Poder Ejecutivo Federal, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

XI. Servidores públicos: Los mencionados en el párrafo primero del Artículo 108 Constitucional y todas aquellas personas que manejen o apliquen recursos públicos federales;

XII. Seguridad nacional: Acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado Mexicano, la gobernabilidad democrática, la defensa exterior y la seguridad interior de la Federación, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado constitucional;

XIII. Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado;

XIV. Sujetos obligados:

a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;

b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;

c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

d) Los órganos constitucionales autónomos;

e) Los tribunales administrativos federales, y

f) Cualquier otro órgano federal.

XV. Unidades administrativas: Las que de acuerdo con la normatividad de cada uno de los sujetos obligados tengan la información de conformidad con las facultades que les correspondan.

Artículo 4. Son objetivos de esta Ley:

I. Proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos;

II. Transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados;

III. Garantizar la protección de los datos personales en posesión de los sujetos obligados;

IV. Favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados;

V. Mejorar la organización, clasificación y manejo de los documentos, y

VI. Contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

Artículo 5. La presente Ley es de observancia obligatoria para los servidores públicos federales.

Artículo 6. En la interpretación de esta Ley y de su Reglamento, así como de las normas de carácter general a las que se refiere el Artículo 61, se deberá favorecer el principio de máxima publicidad y disponibilidad de la información en posesión de los sujetos obligados.

El derecho de acceso a la información pública se interpretará conforme a la Constitución Política de los Estados Unidos Mexicanos; la Declaración Universal de los Derechos Humanos; el Pacto Internacional de

Derechos Civiles y Políticos; la Convención Americana sobre Derechos Humanos; la Convención Sobre la Eliminación de Todas las Formas de Discriminación Contra la Mujer, y

demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales especializados.
Artículo reformado DOF 06-06-2006

OBLIGACIONES DE TRANSPARENCIA

Artículo 7. Con excepción de la información reservada o confidencial prevista en esta Ley, los sujetos obligados deberán poner a disposición del público y actualizar, en los términos del Reglamento y los lineamientos que expida el Instituto o la instancia equivalente a que se refiere el Artículo 61, entre otra, la información siguiente:

I. Su estructura orgánica;

II. Las facultades de cada unidad administrativa;

III. El directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes;

IV. La remuneración mensual por puesto, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;

V. El domicilio de la unidad de enlace, además de la dirección electrónica donde podrán recibirse las solicitudes para obtener la información;

VI. Las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;

VII. Los servicios que ofrecen;

VIII. Los trámites, requisitos y formatos. En caso de que se encuentren inscritos en el Registro Federal de Trámites y Servicios o en el Registro que para la materia fiscal establezca la Secretaría de Hacienda y Crédito Público, deberán publicarse tal y como se registraron;

IX. La información sobre el presupuesto asignado, así como los informes sobre su ejecución, en los términos que establezca el Presupuesto de Egresos de la Federación. En el caso del Ejecutivo Federal, dicha información será proporcionada respecto de cada dependencia y entidad por la Secretaría de Hacienda y Crédito Público, la que además informará sobre la situación económica, las finanzas públicas y la deuda pública, en los términos que establezca el propio presupuesto;

X. Los resultados de las auditorias al ejercicio presupuestal de cada sujeto obligado que realicen, según corresponda, la Secretaría de la Función Pública, las contralorías internas o la

Auditoría Superior de la Federación y, en su caso, las aclaraciones que correspondan; *Fracción reformada DOF 09-04-2012*

XI. El diseño, ejecución, montos asignados y criterios de acceso a los programas de subsidio. Así como los padrones de beneficiarios de los programas sociales que establezca el Decreto del Presupuesto de Egresos de la Federación;

XII. Las concesiones, permisos o autorizaciones otorgados, especificando los titulares de aquéllos;

XIII. Las contrataciones que se hayan celebrado en términos de la legislación aplicable detallando por cada contrato:

a) Las obras públicas, los bienes adquiridos, arrendados y los servicios contratados; en el caso de estudios o investigaciones deberá señalarse el tema específico;

b) El monto;

c) El nombre del proveedor, contratista o de la persona física o moral con quienes se haya celebrado el contrato, y

d) Los plazos de cumplimiento de los contratos;

XIV. El marco normativo aplicable a cada sujeto obligado;

XV. Los informes que, por disposición legal, generen los sujetos obligados;

XVI. En su caso, los mecanismos de participación ciudadana, y

XVII. Cualquier otra información que sea de utilidad o se considere relevante, además de la que con base a la información estadística, responda a las preguntas hechas con más frecuencia por el público.

La información a que se refiere este Artículo deberá publicarse de tal forma que facilite su uso y comprensión por las personas, y que permita asegurar su calidad, veracidad, oportunidad y confiabilidad.

Las dependencias y entidades deberán atender las recomendaciones que al respecto expida el Instituto.

Artículo 8. El Poder Judicial de la Federación deberá hacer públicas las sentencias que hayan causado estado o ejecutoria, las partes podrán oponerse a la publicación de sus datos personales.

Artículo 9. La información a que se refiere el Artículo 7 deberá estar a disposición del público, a través de medios remotos o locales de comunicación electrónica. Los sujetos

obligados deberán tener a disposición de las personas interesadas equipo de cómputo, a fin de que éstas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, éstos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.

Las dependencias y entidades deberán preparar la automatización, presentación y contenido de su información, como también su integración en línea, en los términos que disponga el Reglamento y los lineamientos que al respecto expida el Instituto.

Artículo 10. Las dependencias y entidades deberán hacer públicas, directamente o a través de la Consejería Jurídica del Ejecutivo Federal o de la Comisión Federal de Mejora Regulatoria, en los términos que establezca el Reglamento, y por lo menos con 20 días hábiles de anticipación a la fecha en que se pretendan publicar o someter a firma del titular del Ejecutivo Federal, los anteproyectos de leyes y disposiciones administrativas de carácter general a que se refiere el Artículo 4 de la Ley Federal de Procedimiento Administrativo, salvo que se determine a juicio de la Consejería o la Comisión Federal de Mejora Regulatoria, según sea el caso, que su publicación puede comprometer los efectos que se pretendan lograr con la disposición o se trate de situaciones de emergencia, de conformidad con esa Ley.

Artículo 11. Los informes que presenten los partidos políticos y las agrupaciones políticas nacionales al Instituto Federal Electoral, así como las auditorías y verificaciones que ordene la Comisión de Fiscalización de los Recursos Públicos de los Partidos y Agrupaciones Políticas, deberán hacerse públicos al concluir el procedimiento de fiscalización respectivo.
Cualquier ciudadano podrá solicitar al Instituto Federal Electoral, la información relativa al uso de los recursos públicos que reciban los partidos políticos y las agrupaciones políticas nacionales.

Artículo 12. Los sujetos obligados deberán hacer pública toda aquella información relativa a los montos y las personas a quienes entreguen, por cualquier motivo, recursos públicos, así como los informes que dichas personas les entreguen sobre el uso y destino de dichos recursos.

INFORMACIÓN RESERVADA Y CONFIDENCIAL

Artículo 13. Como información reservada podrá clasificarse aquélla cuya difusión pueda:

I. Comprometer la seguridad nacional, la seguridad pública o la defensa nacional;

II. Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano;

III. Dañar la estabilidad financiera, económica o monetaria del país;

IV. Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o

V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.

Artículo 14. También se considerará como información reservada:

I. La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;

II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;

III. Las averiguaciones previas;

IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado;

V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva, o

VI. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.

Cuando concluya el periodo de reserva o las causas que hayan dado origen a la reserva de la información a que se refieren las fracciones III y IV de este Artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga.

No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad.

Artículo 15. La información clasificada como reservada según los artículos 13 y 14, podrá permanecer con tal carácter hasta por un periodo de doce años. Esta información podrá ser desclasificada cuando se extingan las causas que dieron origen a su clasificación o cuando haya transcurrido el periodo de reserva.

La disponibilidad de esa información será sin perjuicio de lo que, al respecto, establezcan otras leyes.

El Instituto, de conformidad con el Reglamento, o la instancia equivalente a que se refiere el Artículo 61, establecerán los criterios para la clasificación y desclasificación de la información reservada.

Excepcionalmente, los sujetos obligados podrán solicitar al Instituto o a la instancia establecida de conformidad con el Artículo 61, según corresponda, la ampliación del periodo de reserva, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación.

Artículo 16. Los titulares de las unidades administrativas serán responsables de clasificar la información de conformidad con los criterios establecidos en esta Ley, su Reglamento y los lineamientos expedidos por el Instituto o por la instancia equivalente a que se refiere el Artículo 61, según corresponda.

Artículo 17. Las unidades administrativas elaborarán semestralmente y por rubros temáticos, un índice de los expedientes clasificados como reservados. Dicho índice deberá indicar la unidad administrativa que generó la información, la fecha de la clasificación, su fundamento, el plazo de reserva y, en su caso, las partes de los documentos que se reservan. En ningún caso el índice será considerado como información reservada.

El titular de cada dependencia o entidad deberá adoptar las medidas necesarias para asegurar la custodia y conservación de los expedientes clasificados.

En todo momento, el Instituto tendrá acceso a la información reservada o confidencial para determinar su debida clasificación, desclasificación o la procedencia de otorgar su acceso.

Artículo 18. Como información confidencial se considerará:

I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y

II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.

No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

Artículo 19. Cuando los particulares entreguen a los sujetos obligados la información a que se refiere la fracción I del artículo anterior, deberán señalar los documentos que contengan información confidencial, reservada o comercial reservada, siempre que tengan el derecho de reservarse la información, de conformidad con las disposiciones aplicables. En el caso de que exista una solicitud de acceso que incluya información confidencial, los sujetos obligados la comunicarán siempre y cuando medie el consentimiento expreso del particular titular de la información confidencial.

PROTECCIÓN DE DATOS PERSONALES

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. (Se deroga). *Fracción derogada DOF 11-05-2004*

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en

un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

RESPONSABILIDADES Y SANCIONES

Artículo 63. Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en esta Ley las siguientes:

I. Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

II. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a esta Ley;

III. Denegar intencionalmente información no clasificada como reservada o no considerada confidencial conforme a esta Ley;

IV. Clasificar como reservada, con dolo, información que no cumple con las características señaladas en esta Ley. La sanción sólo procederá cuando exista una resolución previa respecto del criterio de clasificación de ese tipo de información del Comité, el Instituto, o las instancias equivalentes previstas en el Artículo 61;

V. Entregar información considerada como reservada o confidencial conforme a lo dispuesto por esta Ley;

VI. Entregar intencionalmente de manera incompleta información requerida en una solicitud de acceso, y

VII. No proporcionar la información cuya entrega haya sido ordenada por los órganos a que se refiere la fracción IV anterior o el Poder Judicial de la Federación.

La responsabilidad a que se refiere este Artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

La infracción prevista en la fracción VII o la reincidencia en las conductas previstas en las fracciones I a VI de este Artículo, serán consideradas como graves para efectos de su sanción administrativa.

Artículo 64. Las responsabilidades administrativas que se generen por el incumplimiento de las obligaciones a que se refiere el Artículo anterior, son independientes de las del orden civil o penal que procedan.

1.12 LEY DE INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA

En su numeral 2 en su fracción V si hace referencia al desarrollo y la utilización permanente de la informática en los servicios nacionales.

ARTICULO 2.- Esta Ley tiene por objeto:

I. Normar el funcionamiento de los Servicios Nacionales de Estadística y de Información Geográfica;

II. Establecer los principios las normas conforme a los cuales las dependencias y entidades de la administración pública federal, deberán ejercer las funciones que les correspondan como partes integrantes de los Servicios Nacionales de Estadística y de Información Geográfica;

III. Fijar las bases para coordinar la participación y colaboración que corresponda a los gobiernos de las entidades federativas y a las autoridades municipales, así como para promover, cuando se requiera, la colaboración de los particulares y de los grupos sociales interesados, a efecto de mejorar el funcionamiento de los servicios mencionados en la fracción anterior;

IV. Promover la integración y el desarrollo de los Sistemas Nacionales Estadístico y de Información Geográfica para que se suministre a quienes requieran, en los términos de esta Ley, el servicio público de información estadística y geográfica, y

V. Regular el desarrollo y la utilización permanente de la informática en los servicios nacionales a que se refiere este artículo.

1.13 LEY ORGÁNICA DEL PODER JUDICIAL DE LA FEDERACIÓN

Esta Ley se desprende del artículo 73 Fracción XXI que cita:

Artículo 73: Facultades del Congreso

XXI. Para establecer los delitos y las faltas contra la Federación y fijar los castigos que por ellos deban imponerse; expedir leyes generales en materias de secuestro, y trata de personas, que establezcan, como mínimo, los tipos penales y sus sanciones, la distribución de competencias y las formas de coordinación entre la Federación, el Distrito Federal, los Estados y los Municipios; así como legislar en materia de delincuencia organizada.

Las autoridades federales podrán conocer también de los delitos del fuero común, cuando éstos tengan conexidad con delitos federales o delitos contra periodistas, personas o instalaciones que afecten, limiten o menoscaben el derecho a la información o las libertades de expresión o imprenta.

En las materias concurrentes previstas en esta Constitución, las leyes federales establecerán los supuestos en que las autoridades del fuero común podrán conocer y resolver sobre delitos federales;

Otorgándole en la Ley Orgánica del Poder Judicial de la Federación, Facultades a los Jueces de Distrito para conocer de los siguientes delitos en los numerales 50, 50 bis, 50 ter, 50 Quater:

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. En el caso del Código Penal Federal, tendrán ese carácter los delitos a que se refieren los incisos b) a l) de esta fracción; *Inciso reformado DOF 18-05-1999*

b) Los señalados en los artículos 2 a 5 del Código Penal; *Inciso que fue reformado DOF 18-05-1999*

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 público o empleado federal, en ejercicio de sus funciones o con motivo de ellas;

g) Los cometidos en contra de un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas, así como los cometidos contra el Presidente de la República, los secretarios del despacho, el Procurador General de la República, los diputados y senadores al Congreso de la Unión, los ministros, magistrados y jueces del Poder Judicial Federal, los miembros de Consejo de la Judicatura Federal, los magistrados del Tribunal Electoral del Poder Judicial de la Federación, los miembros del Consejo General del Instituto Federal Electoral, el presidente de la Comisión Nacional de los Derechos Humanos, los directores o miembros de las Juntas de Gobierno o sus equivalentes de los organismos descentralizados; *Inciso reformado DOF 12-12-2011*

h) Los perpetrados con motivo del funcionamiento de un servicio público federal, aunque dicho servicio esté descentralizado o concesionado;

i) Los perpetrados en contra del funcionamiento de un servicio público federal o en menoscabo de los bienes afectados a la satisfacción de dicho servicio, aunque éste se encuentre descentralizado o concesionado;

j) Todos aquéllos 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; *Inciso reformado DOF 12-06-2000*

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, y *Inciso reformado DOF 12-06-2000*

m) Los previstos en los artículos 366, fracción III; 366 ter y 366 quáter del Código Penal Federal, cuando el delito sea con el propósito de trasladar o entregar al menor fuera del país. *Inciso adicionado DOF 12-06-2000*

II. De los procedimientos de extradición, salvo lo que se disponga en los tratados internacionales.

III.- De las autorizaciones para intervenir cualquier comunicación privada. ***Fracción adicionada DOF 07-11-1996***

Artículo 50 Bis. En materia federal, **la autorización para intervenir comunicaciones privadas será otorgada de conformidad con la Ley Federal contra la Delincuencia Organizada, la Ley de Seguridad Nacional, el Código Federal de Procedimientos Penales, la Ley de la Policía Federal, la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro o la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, según corresponda**. *Artículo adicionado DOF 07-11-1996. Reformado DOF 31-01-2005, 30-11-2010, 14-06-2012*

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 Público 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, secuestro o esclavitud, trata de personas o explotación, previstos en el Código Penal Federal, en la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro o la Ley General para Combatir y Erradicar los delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, respectivamente, o sus equivalentes en las legislaciones penales locales.

Párrafo reformado DOF 30-11-2010, 14-06-2012

La solicitud de autorización de intervención de comunicaciones de los delitos previstos en la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, se formulará de conformidad con ese ordenamiento. *Párrafo adicionado DOF 30-11-2010.*

La autorización se otorgará únicamente al titular del Ministerio Público 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 Público 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 llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses.

Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el titular del Ministerio Público de la entidad federativa acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinará las características de la intervención, sus modalidades y límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenará 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 autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las intervenciones, los originales y sus copias y ordenará su destrucción en presencia del titular del Ministerio Público de la entidad federativa. *Artículo adicionado DOF 07-11-1996*

Artículo 50 Quáter. A los jueces de Distrito Especializados para Adolescentes corresponde:

I. Conocer de las causas instauradas en contra de las personas a quienes se impute la realización de una conducta tipificada como delito, cuando tengan entre doce años cumplidos y menos de dieciocho años de edad;

II. Promover los procedimientos alternativos al juzgamiento, a fin de cumplir con los principios de mínima intervención y subsidiariedad;

III. Resolver los asuntos sometidos a su conocimiento, conforme a los plazos y términos previstos en la Ley Federal de Justicia para Adolescentes;

IV. Resolver sobre las medidas a imponer, atendiendo los principios de culpabilidad por el acto, proporcionalidad y racionalidad, así como a las circunstancias, gravedad de la conducta, características y necesidades de los adolescentes o adultos jóvenes;

V. Asegurarse de que el adolescente o adulto joven que se encuentra a su disposición, no sea incomunicado, coaccionado, intimidado, torturado o sometido a tratos crueles, inhumanos o degradantes, así como los demás que apliquen a su situación;

VI. Resolver sobre las cuestiones o incidentes que se susciten durante la ejecución de las medidas impuestas a adolescentes y adultos jóvenes en los términos que dispone la ley de la materia;

VII. Resolver los recursos que se presenten durante el procedimiento de la ejecución de la medida, en contra de las determinaciones de la Unidad Especializada;

VIII. Atender las solicitudes que realicen personalmente adolescentes y adultos jóvenes o sus representantes legales, y resolver a la brevedad lo que corresponda;

IX. Resolver conforme a las disposiciones legales sobre la adecuación de la medida si se considera que ésta ya produjo sus efectos, es innecesaria o afecta el desarrollo, la dignidad o la integración familiar y social de quienes estén sujetos a ella;

X. Dictar resolución mediante la cual se dé por cumplida la medida impuesta, así como la libertad total y definitiva de los adolescentes o adultos jóvenes; y

XI. Las demás que determine la ley. *Artículo adicionado DOF 27-12-2012*

1.14 LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA

Esta Ley a partir de las Reformas Constitucionales en Materia Penal, del 2008, sobre todo en el rubro de la delincuencia organizada, cobro gran trascendencia e importancia.

Puesto que en México la delincuencia "común", en realidad no es un problema de seguridad nacional como lo es la delincuencia organizada la cual ya rebaso los límites de control gubernamental; y ya tienen líneas especiales de operación basadas en un sistema complejo, tipo empresarial, bien estructurado en su comisión; cuando persigue a través de

determinadas acciones violentas la búsqueda del poder, ya sea político, económico o social, es cuando podemos decir, sin lugar a dudas, que estamos frente a un caso de delincuencia organizada.

Este tipo de delincuencia fue designada con la palabra "organizada", ya que se refiere a la "asociación", a la "sociedad", a la "corporación", al "grupo", en sí a la "unión", como forma de conjuntar esfuerzos en grupo; y con el empleo de la violencia, soborno, intimidación y fuerza, los delincuentes llevaban a cabo sus actividades ilegales, que ya se contemplaban en los Códigos Sustantivos pero antes con la denominación de "Asociación Delictuosa".

Este tipo de delincuencia la tenemos ya tan descontrolada que tienen vínculos en todos los niveles, incluyendo el político y el militar; con la ayuda de actos de corrupción logran su impunidad.

Así, las organizaciones dedicadas a la delincuencia organizada emprenden operaciones ilegales de tipo financiero, mercantil, bancario, bursátil o comercial; acciones de soborno, extorsión; ofrecimiento de servicios de protección, ocultación de servicios fraudulentos y ganancias ilegales; adquisiciones ilegítimas; control de centros de juego ilegales y centros de prostitución, pornografía, terrorismo, fraudes, robos, piratería, tráfico de armas, narcotráfico.

La delincuencia organizada tiene un eje central de dirección y mando y está estructura en forma celular y flexible, con rangos permanentes de autoridad, de acuerdo a la célula que la integran; alberga una permanencia en el tiempo, más allá de la vida de sus miembros; tienen un grupo de sicarios a su servicio; tienden a corromper a las autoridades; estos son dos de los recursos conocidos para el cumplimiento de sus objetivos; opera bajo un principio desarrollado de división del trabajo mediante células que sólo se relacionan entre sí a través de los mandos superiores.

Como tendremos de descontrolada las cuestiones de delincuencia, corrupción e impunidad que incluso la constitución tuvo que regular indebidamente en ella un "Tipo penal de Delincuencia Organizada", la cual la observamos en los dispositivos 16, 18, 19, 20, 22 y 73 y de ahí se desprende esta Ley Federal contra la Delincuencia Organizada en sus artículos del 1 al 28 que al tenor dicen:

DISPOSICIONES GENERALES

Artículo 1o.- La presente Ley tiene por objeto establecer reglas para la investigación, persecución, procesamiento, sanción y ejecución de las penas, por los delitos cometidos por algún miembro de la delincuencia organizada. Sus disposiciones son de orden público y de aplicación en todo el territorio nacional.

Artículo 2o.- Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada: *Párrafo reformado DOF 23-01-2009*

I. Terrorismo, previsto en los artículos 139 a 139 Ter y terrorismo internacional previsto en los artículos 148 Bis al 148 Quáter; contra la salud, previsto en los artículos 194 y 195, párrafo primero; falsificación o alteración de moneda, previstos en los artículos 234, 236 y 237; el previsto en la fracción IV del artículo 368 Quáter en materia de hidrocarburos; operaciones con recursos de procedencia ilícita, previsto en el artículo 400 Bis; y el previsto en el artículo 424 Bis, todos del Código Penal Federal; *Fracción reformada DOF 11-05-2004, 28-06-2007, 24-10-2011*

II. Acopio y tráfico de armas, previstos en los artículos 83 bis y 84 de la Ley Federal de Armas de Fuego y Explosivos;

III. Tráfico de indocumentados, previsto en el artículo 159 de la Ley de Migración; *Fracción reformada DOF 25-05-2011*

IV. Tráfico de órganos previsto en los artículos 461, 462 y 462 bis de la Ley General de Salud; *Fracción reformada DOF 27-11-2007*

V. Corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo previsto en el artículo 201; Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en el artículo 202; Turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tiene capacidad para resistirlo, previsto en los artículos 203 y 203 Bis; Lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de

personas que no tienen capacidad para resistirlo, previsto en el artículo 204; Asalto, previsto en los artículos 286 y 287; Tráfico de menores o personas que no tienen capacidad para comprender el significado del hecho, previsto en el artículo 366 Ter, y Robo de vehículos, previsto en los artículos 376 Bis y 377 del Código Penal Federal, o en las disposiciones correspondientes de las legislaciones penales estatales o del Distrito Federal; *Fracción reformada DOF 27-03-2007, 27-11-2007, 23-01-2009, 30-11-2010*

VI. Delitos en materia de trata de personas, previstos y sancionados en el Título Segundo de la Ley General para Combatir y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, excepto en el caso de los artículos 32, 33 y 34 y sus respectivas tentativas punibles. *Fracción adicionada DOF 27-11-2007. Fracción reformada DOF 30-11-2010, 14-06-2012*

VII. Las conductas previstas en los artículos 9, 10, 11, 17 y 18 de la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. *Fracción adicionada DOF 30-11-2010*

Artículo 3o.- Los delitos a que se refieren las fracciones I, II, III y IV del artículo anterior, que sean cometidos por algún miembro de la delincuencia organizada, serán investigados, perseguidos, procesados y sancionados conforme a las disposiciones de esta Ley.

Los delitos señalados en las fracciones V y VII de dicho artículo lo serán únicamente si, además de cometerse por un miembro de la delincuencia organizada, el Ministerio Público de la Federación ejerce la facultad de atracción. En este caso, el Ministerio Público de la Federación y las autoridades judiciales federales serán las competentes para conocer de tales delitos. Bajo ninguna circunstancia se agravarán las penas previstas en las legislaciones de las entidades federativas.

Párrafo reformado DOF 30-11-2010

Artículo 4o.- Sin perjuicio de las penas que correspondan por el delito o delitos que se cometan, al miembro de la delincuencia organizada se le aplicarán las penas siguientes:

I. En los casos de los delitos contra la salud a que se refiere la fracción I del artículo 2o. de esta Ley:

a) A quien tenga funciones de administración, dirección o supervisión, respecto de la delincuencia organizada, de veinte a cuarenta años de prisión y de quinientos a veinticinco mil días multa, o

b) A quien no tenga las funciones anteriores, de diez a veinte años de prisión y de doscientos cincuenta a doce mil quinientos días multa.

II. En los demás delitos a que se refiere el artículo 2o. de esta Ley:

a) A quien tenga funciones de administración, dirección o supervisión, de ocho a dieciséis años de prisión y de quinientos a veinticinco mil días multa, o

b) A quien no tenga las funciones anteriores, de cuatro a ocho años de prisión y de doscientos cincuenta a doce mil quinientos días multa.

En todos los casos a que este artículo se refiere, además, se decomisarán los objetos, instrumentos o productos del delito, así como los bienes propiedad del sentenciado y aquéllos respecto de los cuales éste se conduzca como dueño, si no acredita la legítima procedencia de dichos bienes.

Artículo 5o.- Las penas a que se refiere el artículo anterior se aumentarán hasta en una mitad, cuando:

I. Se trate de cualquier servidor público que participe en la realización de los delitos previstos para la delincuencia organizada. Además, se impondrán a dicho servidor público, destitución e inhabilitación para desempeñar cualquier cargo o comisión públicos, o

II. Se utilice a menores de edad o incapaces para cometer cualesquiera de los delitos a que se refiere esta Ley.

Artículo 6o.- Los plazos para la prescripción de la pretensión punitiva y de la potestad de ejecutar las penas y medidas de seguridad correspondientes, se duplicarán respecto de los delitos a que se refiere el artículo 2o. de esta Ley cometidos por miembros de la delincuencia organizada.

Artículo 7o.- Son aplicables supletoriamente a esta Ley, las disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal, las del Código Federal de Procedimientos Penales y las de la legislación que establezca las normas sobre ejecución de penas y medidas de seguridad, así como las comprendidas en leyes especiales.

DE LA INVESTIGACIÓN DE LA DELINCUENCIA ORGANIZADA

Artículo 8o.- La Procuraduría General de la República deberá contar con una unidad especializada en la investigación y persecución de delitos cometidos por miembros de la delincuencia organizada, integrada por agentes del Ministerio Público de la Federación, auxiliados por agentes de la Policía Judicial Federal y peritos.

La unidad especializada contará con un cuerpo técnico de control, que en las intervenciones de comunicaciones privadas verificará la autenticidad de sus resultados; establecerá lineamientos sobre las características de los aparatos, equipos y sistemas a autorizar; así como sobre la guarda, conservación, mantenimiento y uso de los mismos.

El Reglamento de la Ley Orgánica de la Procuraduría General de la República, establecerá los perfiles y requisitos que deberán satisfacer los servidores públicos que conformen a la unidad especializada, para asegurar un alto nivel profesional de acuerdo a las atribuciones que les confiere esta Ley.

Siempre que en esta Ley se mencione al Ministerio Público de la Federación, se entenderá que se refiere a aquéllos que pertenecen a la unidad especializada que este artículo establece.

En caso necesario, el titular de esta unidad podrá solicitar la colaboración de otras dependencias de la Administración Pública Federal o entidades federativas.

Artículo 9o.- Cuando el Ministerio Público de la Federación investigue actividades de miembros de la delincuencia organizada relacionadas con el delito de operaciones con recursos de procedencia ilícita, deberá realizar su investigación en coordinación con la Secretaría de Hacienda y Crédito Público.

Los requerimientos del Ministerio Público de la Federación, o de la autoridad judicial federal, de información o documentos relativos al sistema bancario y financiero, se harán por conducto de la Comisión Nacional Bancaria y de Valores, la Comisión Nacional del Sistema de Ahorro para el Retiro y de la Comisión Nacional de Seguros y Fianzas, según corresponda. Los de naturaleza fiscal, a través de la Secretaría de Hacienda y Crédito Público.

La información que se obtenga conforme al párrafo anterior, podrá ser utilizada exclusivamente en la investigación o en el proceso penal correspondiente, debiéndose guardar la más estricta confidencialidad.

Al servidor público que indebidamente quebrante la reserva de las actuaciones o proporcione copia de ellas o de los documentos, se le sujetará al procedimiento de responsabilidad administrativa o penal, según corresponda.

Artículo 10.- A solicitud del Ministerio Público de la Federación, la Secretaría de Hacienda y Crédito Público podrá realizar auditorías a personas físicas o morales, cuando existan indicios suficientes que hagan presumir fundadamente que son miembros de la delincuencia organizada.

Artículo 11.- En las averiguaciones previas relativas a los delitos a que se refiere esta Ley, la investigación también deberá abarcar el conocimiento de las estructuras de organización, formas de operación y ámbitos de actuación. Para tal efecto, el Procurador General de la República podrá autorizar la infiltración de agentes.

En estos casos se investigará no sólo a las personas físicas que pertenezcan a esta organización, sino las personas morales de las que se valgan para la realización de sus fines delictivos.

Artículo 11 Bis.- El Titular del órgano previsto en el artículo 8 podrá autorizar la reserva de la identidad de los agentes de la policía infiltrados, así como de los que participen en la ejecución de órdenes de aprehensión, detenciones en flagrancia y cateos relacionados con los delitos a que se refiere esta Ley, mediante resolución fundada y teniendo en cuenta el tipo de investigación, imposibilitando que conste en la averiguación previa respectiva su nombre, domicilio, así como cualquier otro dato o circunstancia que pudiera servir para la identificación de los mismos.

En tales casos, se asignará una clave numérica, que sólo será del conocimiento del Procurador General de la República, del Titular del órgano antes citado, del Secretario de Seguridad Pública y del servidor público a quien se asigne la clave.

En las actuaciones de averiguación previa, en el ejercicio de la acción penal y durante el proceso penal, el Ministerio Público y la autoridad judicial citarán la clave numérica en lugar de los datos de identidad del agente. En todo caso, el Ministerio Público acreditará ante la autoridad judicial el acuerdo por el que se haya autorizado el otorgamiento de la clave numérica y que ésta corresponde al servidor público respectivo, preservando la confidencialidad de los datos de identidad del agente. En caso de que el agente de la policía cuya identidad se encuentre reservada tenga que intervenir personalmente en diligencias de desahogo de pruebas,

se podrá emplear cualquier procedimiento que garantice la reserva de su identidad. *Artículo adicionado DOF 23-01-2009*

DE LA DETENCIÓN Y RETENCIÓN DE INDICIADOS

Artículo 12.- El Juez podrá dictar el arraigo, a solicitud del Ministerio Público de la Federación, en los casos previstos en el artículo 2o. de esta Ley y con las modalidades de lugar, tiempo, forma y medios de realización señalados en la solicitud, siempre que sea necesario para el éxito de la investigación, para la protección de personas, de bienes jurídicos o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia, sin que esta medida pueda exceder de cuarenta días y se realice con la vigilancia de la autoridad, la que ejercerá el Ministerio Público de la Federación y la Policía que se encuentre bajo su conducción y mando inmediato en la investigación.

La duración del arraigo podrá prolongarse siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen, sin que la duración total de esta medida precautoria exceda de ochenta días. *Artículo reformado DOF 23-01-2009*

LA RESERVA DE LAS ACTUACIONES EN LA AVERIGUACIÓN PREVIA

Artículo 13. A las actuaciones de averiguación previa por los delitos a que se refiere esta Ley, exclusivamente deberán tener acceso el indiciado y su defensor, una vez que haya aceptado el cargo, únicamente con relación a los hechos imputados en su contra, por lo que el Ministerio Público de la Federación y sus auxiliares guardarán la mayor reserva respecto de ellas, sin perjuicio de que el indiciado o su defensor, en base en la información recibida, puedan presentar las pruebas de descargo que juzguen oportunas. *Párrafo reformado DOF 30-11-2010*

No se concederá valor probatorio a las actuaciones que contengan hechos imputados al indiciado, cuando habiendo solicitado el acceso a las mismas al Ministerio Público de la Federación, se le haya negado.

Artículo 14.- Cuando se presuma fundadamente que está en riesgo la integridad de las personas que rindan testimonio en contra de algún miembro de la delincuencia organizada deberá, a juicio del Ministerio Público de la Federación, mantenerse bajo reserva su identidad hasta el ejercicio de la acción penal.

DE LAS ÓRDENES DE CATEO Y DE INTERVENCIÓN DE COMUNICACIONES PRIVADAS

Artículo 15.- Cuando el Ministerio Público de la Federación solicite por cualquier medio al juez de distrito una orden de cateo con motivo de la investigación de alguno de los delitos a los que se refiere el presente ordenamiento, dicha petición deberá ser resuelta en los términos de Ley dentro de las doce horas siguientes después de recibida por la autoridad judicial. *Párrafo reformado DOF 23-01-2009*

Si dentro del plazo antes indicado, el juez no resuelve sobre el pedimento de cateo, el Ministerio Público de la Federación deberá recurrir al tribunal unitario de circuito correspondiente para que éste substancie y resuelva en un plazo igual. *Párrafo reformado DOF 15-11-2011*

El auto que niegue la autorización, es apelable por el Ministerio Público de la Federación. En estos casos la apelación deberá ser resuelta en un plazo no mayor de cuarenta y ocho horas.

Cuando el Juez de Distrito competente, acuerde obsequiar una orden de aprehensión, deberá también acompañarla de una autorización de orden de cateo, si procediere, en el caso de que ésta haya sido solicitada por el agente del Ministerio Público de la Federación, debiendo especificar el domicilio del probable responsable o aquél que se señale como el de su posible ubicación, o bien el del lugar que deba catearse por tener relación con el delito, así como los demás requisitos que señala el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. *Párrafo reformado DOF 23-01-2009*

Artículo 16.- Cuando en la averiguación previa de alguno de los delitos a que se refiere esta Ley o durante el proceso respectivo, el Procurador General de la República o el titular de la unidad especializada a que se refiere el artículo 8o. anterior, consideren necesaria la intervención de comunicaciones privadas, lo solicitarán por escrito al juez de distrito, expresando el objeto y necesidad de la intervención, los indicios que hagan presumir fundadamente que en los delitos investigados participa algún miembro de la delincuencia organizada; así como los hechos, circunstancias, datos y demás elementos que se pretenda probar.

Las solicitudes de intervención deberán señalar, además, la persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizará; el tipo

de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención.

Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

Artículo 17.- El juez de distrito requerido deberá resolver la petición en los términos de ley dentro de las doce horas siguientes a que fuera recibida la solicitud, pero en ningún caso podrá autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Artículo 18.- Para conceder o negar la solicitud, **el juez de distrito constatará la existencia de indicios suficientes que hagan presumir fundadamente que la persona investigada es miembro de la delincuencia organizada y que la intervención es el medio idóneo para allegarse de elementos probatorios**.

En la autorización el juez determinará las características de la intervención, sus modalidades y límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

La autorización judicial para intervenir comunicaciones privadas, que únicamente llevará a cabo el Ministerio Público de la Federación bajo su responsabilidad, con la participación de perito calificado, señalará las comunicaciones que serán escuchadas o interceptadas, los lugares que serán vigilados, así como el periodo durante el cual se llevarán a cabo las intervenciones, el que podrá ser prorrogado por el juez de distrito a petición del Ministerio Público de la Federación, sin que el periodo de intervención, incluyendo sus prórrogas pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse intervenciones cuando el Ministerio Público de la Federación acredite nuevos elementos que así lo justifiquen.

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

El Ministerio Público de la Federación solicitará la prórroga con dos días de anticipación a la fecha en que fenezca el periodo anterior. El juez de distrito resolverá dentro de las doce horas siguientes, con base en el informe que se le hubiere presentado. De negarse la prórroga, concluirá la intervención autorizada, debiendo levantarse acta y rendirse informe complementario, para ser remitido al juzgador.

Al concluir toda intervención, el Ministerio Público de la Federación informará al juez de distrito sobre su desarrollo, así como de sus resultados y levantará el acta respectiva. Las intervenciones realizadas sin las autorizaciones antes citadas o fuera de los términos en ellas ordenados, carecerán de valor probatorio.

Artículo 19.- Si en los plazos indicados en los dos artículos anteriores, el juez de distrito no resuelve sobre la solicitud de autorización o de sus prórrogas, el Ministerio Público de la Federación deberá recurrir al tribunal unitario de circuito correspondiente, para que éste substancie y resuelva en un plazo igual. *Párrafo reformado DOF 15-11-2011*

El auto que niegue la autorización o la prórroga, es apelable por el Ministerio Público de la Federación. En estos casos la apelación deberá ser resuelta en un plazo no mayor de cuarenta y ocho horas.

Artículo 20.- Durante las intervenciones de las comunicaciones privadas, el Ministerio Público de la Federación ordenará la transcripción de aquellas grabaciones que resulten de interés para la averiguación previa y las cotejará en presencia del personal del cuerpo técnico de control de la unidad especializada prevista en el artículo 8o. anterior, en cuyo caso serán ratificadas por quien las realizó. La transcripción contendrá los datos necesarios para identificar la cinta de donde fue tomada. Los datos o Informes impresos que resulten de la intervención serán igualmente integrados a la averiguación.

Las imágenes de video que se estimen convenientes podrán, en su caso, ser convertidas a imágenes fijas y ser impresas para su integración a la indagatoria. En este caso, se indicará la cinta de donde proviene la imagen y el nombre y cargo de la persona que realizó la conversión.

Artículo 21.- Si en la práctica de una intervención de comunicaciones privadas se tuviera conocimiento de la comisión de delitos diversos de aquéllos que motivan la

medida, se hará constar esta circunstancia en el acta correspondiente, con excepción de los relacionados con las materias expresamente excluidas en el artículo 16 constitucional. Toda actuación del Ministerio Público de la Federación o de la Policía Judicial Federal, hechas en contravención a esta disposición carecerán de valor probatorio.

Cuando de la misma práctica se advierta la necesidad de ampliar a otros sujetos o lugares la intervención, el Ministerio Público de la Federación presentará al juez de distrito la solicitud respectiva.

Cuando la intervención tenga como resultado el conocimiento de hechos y datos distintos de los que pretendan probarse conforme a la autorización correspondiente podrá ser utilizado como medio de prueba, siempre que se refieran al propio sujeto de la intervención y se trate de alguno de los delitos referidos en esta ley. Si se refieren a una persona distinta sólo podrán utilizarse, en su caso, en el procedimiento en que se autorizó dicha intervención. De lo contrario, el Ministerio Público de la Federación iniciará la averiguación previa o lo pondrá en conocimiento de las autoridades competentes, según corresponda.

Artículo 22.- De toda intervención se levantará acta circunstanciada por el Ministerio Público de la Federación, que contendrá las fechas de inicio y término de la intervención; un inventario pormenorizado de los documentos, objetos y las cintas de audio o video que contengan los sonidos o imágenes captadas durante la misma; la identificación de quienes hayan participado en las diligencias, así como los demás datos que considere relevantes para la investigación. Las cintas originales y el duplicado de cada una de ellas, se numerarán progresivamente y contendrán los datos necesarios para su identificación. Se guardarán en sobre sellado y el Ministerio Público de la Federación será responsable de su seguridad, cuidado e integridad.

Artículo 23.- Al iniciarse el proceso, las cintas, así como todas las copias existentes y cualquier otro resultado de la intervención serán entregados al juez de distrito.

Durante el proceso, el juez de distrito, pondrá las cintas a disposición del inculpado, quien podrá escucharlas o verlas durante un periodo de diez días, bajo la supervisión de la autoridad judicial federal, quien velará por la integridad de estos elementos probatorios. Al término de este periodo de diez días, el inculpado o su defensor, formularán sus observaciones,

si las tuvieran, y podrán solicitar al juez la destrucción de aquellas cintas o documentos no relevantes para el proceso. Asimismo, podrá solicitar la transcripción de aquellas grabaciones o la fijación en impreso de imágenes, que considere relevantes para su defensa.

La destrucción también será procedente cuando las cintas o registros provengan de una intervención no autorizada o no se hubieran cumplido los términos de la autorización judicial respectiva.

El auto que resuelva la destrucción de cintas, la transcripción de grabaciones o la fijación de imágenes, es apelable con efecto suspensivo.

Artículo 24.- En caso de no ejercicio de la acción penal, y una vez transcurrido el plazo legal para impugnarlo sin que ello suceda, las cintas se pondrán a disposición del juez de distrito que autorizó la intervención, quien ordenará su destrucción en presencia del Ministerio Público de la Federación. Igual procedimiento se aplicará cuando, por reserva de la averiguación previa u otra circunstancia, dicha averiguación no hubiera sido consignada y haya transcurrido el plazo para la prescripción de la acción penal.

Artículo 25.- En los casos en que el Ministerio Público de la Federación haya ordenado la detención de alguna persona conforme a lo previsto en el artículo 16 constitucional, podrá solicitar al juez de distrito la autorización para realizar la intervención de comunicaciones privadas, solicitud que deberá resolverse en los términos de ley dentro de las doce horas siguientes a que fuera recibida, si cumpliera con todos los requisitos establecidos por la ley.

Artículo 26.- Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención en los términos del presente capítulo, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichas diligencias, de conformidad con la normatividad aplicable y la orden judicial correspondiente.

Artículo 27.- Los servidores públicos de la unidad especializada a que se refiere el artículo 8o. de esta Ley, así como cualquier otro servidor público, que intervengan comunicaciones privadas sin la autorización judicial correspondiente, o que la realicen en términos distintos de los autorizados, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con destitución e inhabilitación para desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo de la pena de prisión impuesta.

Artículo 28.- Quienes participen en alguna intervención de comunicaciones privadas deberán guardar reserva sobre el contenido de las mismas.

Los servidores públicos de la unidad especializada prevista en el artículo 8o. de esta Ley, así como cualquier otro servidor público o los servidores públicos del Poder Judicial Federal, que participen en algún proceso de los delitos a que se refiere esta Ley, que revelen, divulguen o utilicen en forma indebida o en perjuicio de otro la información o imágenes obtenidas en el curso de una intervención de comunicaciones privadas, autorizada o no, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con la destitución e inhabilitación para desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo que la pena de prisión impuesta.

La misma pena se impondrá a quienes con motivo de su empleo, cargo o comisión público tengan conocimiento de la existencia de una solicitud o autorización de intervención de comunicaciones privadas y revelen su existencia o contenido.

1.15 CÓDIGO FISCAL DE LA FEDERACIÓN

En el Código Fiscal de la Federación el Artículo 15-B, del Capítulo I del Título primero nos dice que se consideran regalías, entre otros, los pagos de cualquier clase por el uso o goce temporal de patentes, certificados de invención o mejora, marcas de fábrica, nombres comerciales, derechos de autor sobre obras literarias, artísticas o científicas, incluidas las películas cinematográficas y grabaciones para radio o televisión, así como de dibujos o modelos, planos, fórmulas, o procedimientos y equipos industriales, comerciales o científicos, así como las cantidades pagadas por transferencia de tecnología o informaciones relativas a experiencias industriales, comerciales o científicas, u otro derecho o propiedad similar.

Para los efectos del párrafo anterior, el uso o goce temporal de derechos de autor sobre obras científicas incluye la de los programas o conjuntos de instrucciones para computadoras requeridos para los procesos operacionales de las mismas o para llevar a cabo tareas de aplicación, con independencia del medio por el que se transmitan.

De igual forma se consideran regalías los pagos efectuados por el derecho a recibir para retransmitir imágenes visuales, sonidos o ambos, o bien los pagos efectuados por el derecho a

permitir el acceso al público a dichas imágenes o sonidos, cuando en ambos casos se transmitan por vía satélite, cable, fibra óptica u otros medios similares.

En el Capítulo II, de los Medios Electrónicos, el Artículo 17-D nos comenta que se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.

Igualmente, nos habla de Firmas Electrónicas y del proceso de creación y la interacción con los organismos fiscales.

1.16 CÓDIGO DE COMERCIO

El Código de Comercio nos habla de la Correspondencia en el Artículo 48 del Capítulo IV, que afirma que tratándose de las copias de las cartas, telegramas y otros documentos que los comerciantes expidan, así como de los que reciban que no estén incluidos en el artículo siguiente, el archivo podrá integrarse con copias obtenidas por cualquier medio: mecánico, fotográfico o electrónico, que permita su reproducción posterior íntegra y su consulta o compulsa en caso necesario.

Nuevamente, el Capítulo II nos habla de los contratos mercantiles en general, el Artículo 80 nos dice que los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

La que consideramos la parte más importante de este código y de todo el cuerpo legal que podría regular el Internet es la parte que contiene el Título Segundo, del Comercio Electrónico cuyo Capítulo I nos habla de los Mensajes de Datos; este nos dice que en los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología.

Y nos ofrece conceptos utilizados en este rubro:

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

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

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

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

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

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

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

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

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

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

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

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

Secretaría: Se entenderá la Secretaría de Economía.

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

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

Complementa el hecho de que las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los

TRATADOS INTERNACIONALES DE LOS QUE MÉXICO SEA PARTE.

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

1.17 CÓDIGO PENAL FEDERAL

El Código Penal Federal, en su Capítulo II, de la Corrupción de menores e incapaces; pornografía infantil y prostitución sexual de menores, nos dice, su Artículo 201 que se comete el delito de corrupción de menores, induciendo, procurando, facilitando u obligando a un menor de dieciocho años de edad o a quien no tenga capacidad para comprender el significado del hecho, a realizar actos de exhibicionismo corporal, lascivos o sexuales, prostitución, ebriedad, consumo de narcóticos, prácticas sexuales o a cometer hechos delictuosos. Al autor de este delito se le aplicarán de cinco a diez años de prisión y de quinientos a dos mil días multa.

Al que obligue o induzca a la práctica de la mendicidad, se le impondrá de tres a ocho años de prisión y de cincuenta a doscientos días multa.

No se entenderá por corrupción de menores los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre función reproductiva, la prevención de enfermedades de transmisión sexual y el embarazo de adolescentes, siempre que estén aprobados por la autoridad competente.

Cuando de la práctica reiterada de los actos de corrupción el menor o incapaz adquiera los hábitos del alcoholismo, farmacodependencia, se dedique a la prostitución o a formar parte

de una asociación delictuosa, la pena será de siete a doce años de prisión y de trescientos a seiscientos días multa.

Si además de los delitos previstos en este Capítulo resultase cometido otro, se aplicarán las reglas de la acumulación.

Además, el Artículo 202, nos dice que aquel que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.

Al que fije, grabe, imprima actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de dieciocho años, se le impondrá la pena de diez a catorce años de prisión y de quinientos a tres mil días multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieren las acciones anteriores.

Para los efectos de este artículo se entiende por pornografía infantil, la representación sexualmente explícita de imágenes de menores de dieciocho años.

El Código Penal Federal también nos habla de la Revelación de Secretos en sus numerales del 210 al 211 bis que indican:

REVELACIÓN DE SECRETOS

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

Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Esta misma Ley contempla los Delitos Informáticos en sus artículos 211 bis 1 al 211 bis 7 y dicen:

ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

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

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

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

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

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de

información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

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

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

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

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

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

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

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

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

El mismo Código en referencia a los delitos en Materia de Derechos de Autor (Piratería), nos dice en los Artículos 424 al 429 que se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación."

1.18 CÓDIGO CIVIL FEDERAL

En el Código Civil Federal en el Título Primero (Fuentes de las Obligaciones) en la Primera parte (De las Obligaciones en General) del Libro Cuarto (De las Obligaciones), el Capítulo I en el apartado de los Contratos.

El Artículo 1792 nos da la definición de un Convenio, que es un acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones.

El Artículo 1793 nos dice que los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos y que se requiere del consentimiento para que este contrato exista.

Este consentimiento debe ser expreso o tácito (Art. 1803) y en el caso de ser expreso, la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Internet ingresa en estos términos: medio electrónico o cualquier otra tecnología, sin embargo, situación que se repetirá varias veces, el término tal cual, Internet, no está regulado.

De este mismo cuerpo jurídico, el Artículo 1805 nos dice que una oferta que se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente.

La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

1.19 CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES

El Código Federal de Procedimientos Civiles en su Capítulo I nos dice que para conocer la verdad, puede el juzgador valerse de cualquier persona, sea parte o tercero, y de cualquier cosa o documento, ya sea que pertenezca a las partes o a un tercero, sin más limitaciones que las de que las pruebas estén reconocidas por la ley y tengan relación inmediata con los hechos controvertidos (Artículo 79), el Artículo 93 afirma que la ley reconoce como medios de prueba:

I.- La confesión;

II.- Los documentos públicos;

III.- Los documentos privados;

IV.- Los dictámenes periciales;

V.- El reconocimiento o inspección judicial;

VI.- Los testigos;

VII.- Las fotografías, escritos y notas taquigráficas, y, en general, todos aquellos elementos aportados por los descubrimientos de la ciencia; y

VIII.- Las presunciones."

Esto vuelve a ser afirmado en el Artículo 188 que nos comenta que para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar

fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia.

El Capítulo IX nos señala sobre la valuación de la prueba, cuyo Artículo 210-A comenta que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

1.20 ÓRGANOS NACIONALES

NIC MÉXICO

El Network Information Center - México, (NIC-México) es la organización encargada de la administración del nombre de dominio territorial (ccTLD, country code Top Level Domain) .MX, el código de dos letras asignado a cada país según el ISO 3166.

Entre sus funciones están el proveer los servicios de información y registro para .MX así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso.

Este nace el 1º de Febrero de 1989, cuando el ITESM, Campus Monterrey establece conexión directa a Internet.

1.21 POLICÍA CIBERNÉTICA

"La Policía Cibernética trabaja en temas de delitos informáticos, llevando a cabo campañas de prevención del delito informático a través de la radio y de cursos en instituciones públicas y privadas. También está el equipo UNAM-CERT, que sin tener la misión de perseguir los delitos cibernéticos, igual realiza acciones de análisis forenses". [50]

Ejerciendo sus atribuciones legales y para garantizar la presencia de la autoridad en la supercarretera de la información**,** "*La Policía Federal preventiva desarrolló en México la primera unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados".* [51]

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

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

La Secretaría de Seguridad Pública mediante la Policía Federal Preventiva, contribuye con su granito de arena para proteger el entorno de la red Internet y en ese esfuerzo, requiere apoyo de la ciudadanía por lo que invitamos a los que quieran proteger a los niños en particular, y sobre todo a los interesados en la seguridad de la red, hagan contacto con nosotros para que nos ayuden.

---

[50] Véase "Página de la Secretaría de Seguridad Pública", 20 de Febrero del 2013, *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1276161*

[51] Véase "Guía Taller contra la Prevención del Delito Cibernético", 20 de Febrero del 2013, *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1214152//archivo*.

FUNCIONES:

• Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.

• Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

• Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos utilizando computadoras.

• Realización de operaciones de patrullaje anti-hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red. Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve una cultura de legalidad, respeto y seguridad en la red.[52]

ACTIVIDADES:

• Integrar un equipo especializado en delitos cibernéticos a fin de hacer este medio electrónico un lugar seguro para el intercambio de información. Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.

• Utilizar Internet como un instrumento para identificar a los delincuentes que cometen este tipo de delitos.

• Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.

• Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.

• Ofrecer seguridad en la navegación en la Internet para los menores, ya que existen peligros en ella.

• Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.

---

[52] Véase a Policía Cibernética, *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/388074//archivo*

• Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.
• Identificar y combatir el crimen organizado dedicado al tráfico de menores.
• Establecer técnicas adecuadas para la búsqueda y localización oportuna de niños extraviados, perdidos y/o robados.
• Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.
• Desintegrar y proponer a disposición del Agente del Ministerio Público a las bandas de pedófilos dedicadas a la explotación sexual de menores y a la pornografía infantil.
• Acciones de operación con autoridades locales, federales e internacionales.

FINALIDADES:

• Atención a fraudes computacionales
• Combatir la explotación sexual infantil
• Detección de intrusiones y robo de identidad
• Analizar daños a sistemas
• Identificar virus, gusanos, etc.
• Detección de intrusos como Hackers y Crackers
• Proteger la infraestructura interinstitucional
• Detección de sitios de riesgo criminal
• Detección de espionaje industrial
• Venta de drogas y armas
• Combatir el Terrorismo y crímenes violentos contra menores
• Combatir el robo, sustracción y tráfico de menores.

El Grupo Interinstitucional de Combate a Delitos Cibernéticos, DC México, advirtió de la necesidad de impulsar ante el Poder Legislativo la creación de leyes que combatan la delincuencia cibernética, que siempre renueva su capacidad tecnológica.

CAPÍTULO SEGUNDO. EL DELINCUENTE, LOS DELITOS INFORMÁTICOS Y LOS BIENES JURÍDICOS QUE TUTELAN.

2.1 SUJETOS DEL DELITO INFORMÁTICO

Para la comisión del delito como aquella conducta antisocial, encontraremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias:

SUJETO ACTIVO

Es aquella persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pues son personas listas, decididas y motivadas, dispuestas a aceptar un reto tecnológico, mediante el cual vulneran bienes jurídicos tutelados en materia penal.

SUJETO PASIVO

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

2.2 EL DELINCUENTE INFORMÁTICO

Son los sujetos que intervienen y realizan los Delitos Informáticos e ilícitos cometidos por medios informáticos.

EL HACKER

Es el más peligroso de todos es un "Intruso o Pirata informático, que pueden ser vistos como los mismos programadores o personas inadaptadas que sólo se dedican a cometer ilícitos con las computadoras, o bien éste término es utilizado para denominar a toda aquella persona, experta en una rama de la informática y las telecomunicaciones como: programación, software, hardware.

EL LAMER

Son personas que no poseen el gran conocimiento de un Hacker aunque tienen un nivel básico para actuar, es un término usado de forma despectiva para este tipo de usuarios, no siguen la sed de conocimiento que un Hacker debe tener, por lo regular sus ataques son por diversión y presumir sus pocas habilidades.

EL WRACKER

Shareware o Freeware navegando por Internet, en muchos casos no poseen conocimientos amplios sobre informática y llegan a causar daño sin querer y en otros casos lo hacen sin saber. Se considera una práctica peligrosa debido a que al investigar y descargar programas dañinos para su beneficio muchas veces se encuentra en riesgo de ser atacado por virus o personas.

EL CRACKER

Son los más peligrosos en el mundo de la informática, en muchos casos son Hackers al mismo tiempo, poseen gran capacidad de programación, amplios conocimientos en criptografías y criptoanálisis. Se dedican a acceder en lugares prohibidos tanto de empresas privadas como gubernamentales para robar, destruir y distribuir programas comerciales pirateados, crean todo tipo de virus para su beneficio e incluso para venderlos a terceros, más para violar derechos de autor que por curiosidad y búsqueda de conocimiento como el Hacker.

EL PHREAKER

Son los usuarios que realizan actividades ilegales para enriquecerse, destruir o actos terroristas contra equipos informáticos, en unos inicios sólo atacan sistemas de telefonía fija o móvil celular, televisión de paga para obtener servicio gratuito mediante tecnología de avanzada comprada o creada por ellos mismos, después se enfocaron en ingresar a sitios bancarios para robar cuentas bancarias y números de tarjetas de crédito, o incluso de crear números de cuentas usando programas originales de las empresas de tarjetas de crédito y siempre son auxiliados con grandes sistemas de cómputo armados por ellos mismos.

EL SCRIPT-KIDDIE	Son personas que se consideran Crackers, pero poseen menores conocimientos que los mismos, presumen de sus conocimientos utilizando programas de terceros para hacer daño que en la mayoría del caso son el reflejo de actos de vandalismo.
EL SPEAKER	Considerado como el máximo espía de la informática; son usuarios con grandes conocimientos y capacidades, son relativamente indetectables debido a que no provocan daño, sólo cuando es realmente necesario, generalmente trabajan para organismos gubernamentales.
EL RIDER	Son todos los usuarios anteriores que han decidido dejar estas prácticas y trabajar para empresas de seguridad informática, gobiernos y empresas para emplear sus conocimientos y capacidades como especialistas en la seguridad, en el área de delitos informáticos con la policía, además del diseño de programas y protocolos de seguridad.

2.3 CARACTERISTICAS DE LOS DELITOS INFORMÁTICOS

En forma general, analizaremos las principales características que revisten a los Delitos informáticos serán las siguientes:

a) Conductas criminógenas de cuello blanco.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.
k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por lo anteriormente expuesto, se puede determinar que los que cometen este tipo de ilícitos, son personas con muy amplios y sofisticados conocimientos sobre la informática y cibernética, en los cuales, se localizan en lugares estratégicos y con facilidad para poder acceder a información de carácter delicado, como lo son preferentemente la instituciones financieras y crediticias o el propio gobierno, y las grandes empresas o personas en lo particular, dañando en la generalidad de los casos directamente el patrimonio de la víctima, quedando impune el ilícito por la falta de leyes que no son aplicables a los casos concretos o determinados, y no son denunciados estos tipos de conductas antisociales; siendo esto alarmante, pues como ya precisamos en líneas precedentes este tipo de acciones tienden a proliferar y extenderse y cada vez van a ser mucho más comunes, por lo que se pretende en la presente investigación, es crear una conciencia sobre la imperiosa necesidad urgente de regular todas estas conductas, ya que debe ser legislado de una manera seria, técnica y honesta, recurriendo a las diferentes personalidades que tienen un amplio conocimiento, tanto técnico en materia de computación, como en lo legal, ya que si no se conoce de la materia, difícilmente se podrían aplicar sanciones justas a las personas que realizan este tipo de actividades ilícitas de manera regular.

2.4 CLASIFICACION DEL DELITO INFORMÁTICO

Los expertos en la materia han clasifican a este tipo de acciones de dos formas, como instrumento o medio y como fin u objeto.

Aún así autores que son muy reconocidos como Sarzana aluden que: *"Estos ilícitos pueden catalogarse en atención a que éstos producen un provecho para el sujeto activo o autor y provocan un daño directo en contra de la computadora como una entidad física y que procuran un daño a un individuo o grupos sociales, tanto en su integridad física, honor o patrimonio"*.[53]

"Para el tratadista Julio Téllez Valdés, cataloga a los ilícitos informáticos", [54]

1. Como Método o Medio, señalando que estas conductas criminógenas que se valen de las computadoras como método, medio en la para cometer el ilícito; por ejemplo:

1. La falsificación de documentos vía computarizada (como ocurre en las denominadas tarjetas de crédito, en los cheques, etcétera);

2. La tergiversación tanto de los activos como de los y pasivos en la situación contable de las empresas;

3. La planeación o falsedad de delitos convencionales (como lo serían el robo, el homicidio, el fraude, etcétera), el "robo" de tiempo de computadora;

4. La lectura, el hurto o el copiado de información considerada como confidencial;

5. El aprovechamiento ilegítimo o violación de los código para penetrar y perpetrar a un sistema introduciendo instrucciones inapropiadas (como lo sería el famoso Caballo de Troya);

[53] Tellez Valdés, Julio, *"Derecho Informático"*, Segunda Edición, Editorial McGrawHill, México 1996, p. 104.
[54] Ídem.

6. Variación en cuanto al destino de pequeñas cantidades de dinero, los famosos centavos que se trasladan de varias cuentas a otra cuenta bancaria (que es lo que se conoce como la técnica salami);

7. El uso no autorizado de programas de cómputo; (software)

8. La alteración o modificación en la labor de los sistemas (los llamados virus informáticos) y el acceso remoto a áreas informatizadas en forma no autorizadas entre muchas más;

9. *"Acceso a áreas informatizadas en forma no autorizada"*. [55]

2. Como fin y objeto. En esta clase se van a encuadrar las conductas criminógenas que van a estar orientadas en contra directamente de la computadora, de sus accesorios o de sus programas (software) como entidad física, en los cuales consiguen por medio de la programación o de instrucciones que produzcan un bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria de la computadora, o el atentado físico contra la máquina o sus accesorios (discos, usb, sd, cintas, terminales, etcétera); (son los llamados Virus).

"Para la autora del Libro "Delitos Electrónicos" María de la Luz Lima, establece un catalogo en tres categorías": [56]

1.- Los que utilizan la tecnología electrónica como método;

2.- Los que utilizan la tecnología electrónica como medio y;

3.- Los que utilizan la tecnología electrónica como fin.

[55] Ibídem, pp 105 y 106.
[56] Lima De La Luz, María, "*Delitos Electrónicos*", en Criminalia, México, Academia Mexicana de Ciencias Penales, Editorial Porrúa, No. 1-6. Año L. Enero - Junio 1984.

Como Método	Son los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
Como Medio	Son aquellas conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.
Como Fin	Se dirigen en contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.5 LOS DELITOS INFORMÁTICOS CONOCIDOS POR LAS NACIONES UNIDAS

Existen una gran diversidad de ilícitos informáticos, la multiplicidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, el único límite existente viene dado por la conexión de tres factores: **la gran imaginación del autor del delito, su gran capacidad técnica y las deficiencias existentes en el control en las instalaciones informáticas**, por tal razón y siguiendo la clasificación dada por las Naciones Unidas, he intentado establecer una clasificación, por lo expuesto precedentemente y sin pretender agotar la multiplicidad de conductas que componen a esta clase de delincuencia en forma efímera señalaremos en qué consiste cada una de estas conductas delictivas:

2.5.1 LOS FRAUDES

2.5.1.1 LOS DATOS FALSOS O ENGAÑOSOS

También denominados como (Data diddling), conocidos también como introducción de datos falsos, esta es una manipulación de datos de entrada al computador con el fin de provocar o alcanzar movimientos falsos en las transacciones que tiene una empresa. Este tipo de fraude informático es denominado como ***manipulación de datos de entrada***, simboliza el delito informático más común en virtud de que es más fácil de cometer o de realizar y es difícil de descubrir. Este delito no demanda de conocimientos muy especializados de informática y

puede realizarlo casi cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

2.5.1.2 MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA"

Son muy conocidos como los Caballos de Troya (Troya Horses), Es extremadamente difíciles de descubrir y por lo general van a pasar inadvertidos debido a que el delincuente debe tener conocimientos técnicos especializados que son precisos de la informática. Este ilícito reside en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un procedimiento común utilizado por los individuos que tienen conocimientos especializados en programación informática en el llamado Caballo de Troya que consiste en insertar un sin número de instrucciones de computadora de forma encubierta u oculta en los programas informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

2.5.1.3 LA TÉCNICA DEL SALAMI

La Técnica de salami o (Salami Technique/Rounching Down), Produce las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

2.5.1.4 FALSIFICACIONES INFORMÁTICAS

Son de dos tipos como objetos y como Instrumentos:

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

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer

reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

2.5.1.5 MANIPULACIÓN DE LOS DATOS DE SALIDA

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

2.5.1.6 PISHING

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar. En estos momentos también existe una nueva modalidad de Pishing que es el llamado Spear Pishing o Pishing segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

2.5.2 EL SABOTAJE INFORMÁTICO.

Es el acto por medio del cual se borran, suprimen o modifican sin autorización funciones o datos de computadora con la intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos y son:

2.5.2.1 BOMBAS LÓGICAS (LOGIC BOMBS)

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

2.5.2.2 GUSANOS

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita

2.5.2.3 VIRUS INFORMÁTICOS Y MALWARE

Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como: *"Pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar"*. [57]

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

2.5.2.4 CIBERTERRORISMO

Terrorismo informático es el acto por medio del cual se pretende desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además de lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común necesitaría.

2.5.2.5 ATAQUES DE DENEGACIÓN DE SERVICIO

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

[57] Guibourg, Ricardo y otro, "*Manual de Informática Jurídica*", Editorial Astrea, Buenos Aires, Argentina.

2.5.3 EL ESPIONAJE INFORMÁTICO Y EL ROBO O HURTO DE SOFTWARE

2.5.3.1 FUGA DE DATOS (DATA LEAKAGE)

También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, *"La facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"*.[58]

La forma más sencilla de proteger la información confidencial es la criptografía.

2.5.3.2 REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

[58] Camacho Losa, Luis, "*El Delito Informático*", Madrid España 1987.

2.5.4 EL ROBO DE SERVICIOS

2.5.4.1 HURTO DEL TIEMPO DEL COMPUTADOR

Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

2.5.4.2 APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING)

Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Toscavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

2.5.4.3 PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION)

Figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, Entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

2.5.5 EL ACCESO NO AUTORIZADO A SERVICIOS INFORMÁTICOS

2.5.5.1 LAS PUERTAS FALSAS (TRAP DOORS)

Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

2.5.5.2 LA LLAVE MAESTRA (SUPERZAPPING)

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

2.5.5.3 PINCHADO DE LÍNEAS (WIRETAPPING)

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Como se señalo anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

2.5.5.4 PIRATAS INFORMÁTICOS O HACKERS

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

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

2.6 DELITOS INFORMÁTICOS COMETIDOS COMO MEDIO O INSTRUMENTO PARA PERPETRAR OTROS ILÍCITOS

PORNOGRAFÍA.

El Internet es uno de los espacios que son más utilizados por quienes intentan colocar material de contenido sexual explícito o similar. Se estima que alrededor de un 15% de todo el material que circula en el Internet tienen un contenido pornográfico y/o intolerante.

Se coloca el material en páginas de alojamiento gratuito o pagado, puede tratarse de fotos, videos, relatos u otro tipo de imágenes digitalizadas.

En algunas de las páginas que contienen este tipo de material se toman el trabajo de crear un código de verificación de edad a través del cual se verifica que la persona que esta navegando sea mayor de 18 años. Los sistemas de verificación de edad requieren el uso de tarjetas de crédito y como no hay demasiadas personas dispuestas a otorgar su número de tarjeta por la red Internet.

El servicio de correo electrónico (e-mail, en el idioma inglés) se ha visto afectado en forma indirecta, muchas personas que se dedican a enviar material explícito (en cualquier formato digital).

Al tratar este tema nos realizamos las siguientes preguntas: ¿Cuál es la ley aplicable para determinar si el material exhibido es o no pornográfico, presenta o no contenido discriminativo?

Tal vez la ley del lugar de asiento físico del servidor, ¿La ley del lugar en donde las páginas electrónicas se pueden accesar, la ley del lugar físico desde donde se intercambia el material?

Determinada la ley aplicable, debemos buscar a la persona que debe ser sujeta a sanción penal a quien debe sancionarse, a los que arman la página con contenido sexual, a los que la accedan, a quien provee el alojamiento o prestan su servidor de conversaciones en tiempo real y/o Chat, para intercambiar material.

"Existen en la jurisprudencia estadounidense fallos judiciales sobre el tema referido, como el caso de Félix Somm, conocido como caso Compuserve. La empresa Compuserve de capitales alemanes y norteamericanos brindaba desde sus servidores en Alemania acceso mundial a varios sitios de contenidos pedófilos. Procedida la denuncia en Estados Unidos de América se allanaron las sedes de la empresa en Alemania y Félix Somm fue encontrado penalmente responsable de contribuir al delito de divulgación de pornografía infantil".[59]

Con la finalidad de tratar de solucionar este problema el gobierno australiano ha creado un organismo oficial el Australian Broadcasting Authority (ABA), que deberá regular el contenido de Internet según una ley sancionada por la legislatura australiana.

La pornografía se ha convertido en un negocio lucrativo alrededor del mundo durante muchos años dejando millonarias ganancias tanto a productores, actores y distribuidores, que en muchos casos son negocios lícitos y aceptados en diferentes partes del mundo, son negocios lícitos que con la llegada de la Internet y la libre apertura para publicar cualquier contenido, la circulación y redes pornográficas han venido creciendo de manera desproporcionada, pero dentro de este mundo se presenta un problema mayor aún más serio de resolver que es la pornografía infantil.

La pornografía infantil gracias a la libertad de publicar cualquier contenido, la extraterritorialidad y el relativo anonimato que otorga la Internet se ha convertido en un serio problema en todo el mundo. Las redes de prostitución infantil constituye una industria muy bien organizada y estructurada en diferentes lugares del mundo, aprovechando en muchos

[59] Sobre el tema puede revisarse las siguientes direcciones electrónicas, 20 de febrero del 2013, *http://www.stop-childpornog.at/, y también http://www.info2000.csic.es/midas-net/pornoinfantil.htm*

casos de la violencia, pobreza, hambre y las permisivas conductas de gobiernos corruptos, pero con la llegada de la Internet este problema que tiene dificultades en ser resuelto se convirtió en un serio problema a nivel internacional y aún más difícil de combatir, ya que no sólo se convirtió en industria privada aislada sino de bandas delictivas bien organizadas entre algunas naciones que conocían la magnitud del problema sin la Internet, sino que cualquier persona con acceso a una computadora, cámara digital, escáner y con acceso a Internet lo ha convertido en un negocio casero al alcance de cualquier persona, apilándose a un ámbito a nivel familiar y pequeña comunidad.

La pornografía infantil se puede encontrar tipificada en el Código Penal Federal en su artículo 202 el cual señala:

Articulo 202. Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, **exhibirlos o describirlos** a través de anuncios impresos, **transmisión de archivos de datos en red pública o privada de telecomunicaciones**, **sistemas de computo, electrónicos o sucedáneos**. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, **video grabe, fotografié, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad.**

O una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien **reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.**

Se tiene que hacer referencia que este artículo en su primer párrafo hace referencia a que este delito puede ser cometido mediante el uso de medios informáticos y la Internet. Un

serio problema que presenta esta actividad a combatir en todo el mundo es que en la Pornografía infantil existe un amplio y variante rango de edad para determinar a un menor de edad, el articulo 202 hace referencia a: comete el delito de ***pornografía de personas menores de dieciocho años de edad***… otro problema es la pornografía infantil simulada o ficticia en la cual se aprovecha de los adelantos en la tecnología sobre modificación de imágenes, efectos de maquillaje y complexión de los actores, en la que demuestran a presuntos menores de edad en actos sexuales y son anunciados como pornografía infantil en los sitios de Internet.

"La UNICEF (United Nations Children's Fund) estima que más de un millón de niños alrededor del mundo son forzados o usados para la prostitución y producir pornografía infantil cada año, en la mayoría de los casos son entregados por sus padres, forzados por las condiciones de pobreza extrema en la que se encuentran".[60]

La pornografía infantil por Internet encierra muchas actividades delictivas alrededor de todo el mundo amparados por el anonimato que ofrece este sistema, iniciando con el secuestro de menores, o atraídos aprovechando su precaria situación, falsas adopciones protegidos por funcionarios corruptos, tráfico de personas hasta el turismo sexual ofrecidos en sitios de Internet invitan a extranjeros a nuestro país mediante la excusa de turismo convencional ofrecen paquetes de avión y hotel a precios económicos, donde incluyendo este servicio de prostitución infantil, finalizando con homicidio y tráfico de órganos.

En México el Turismo Sexual se puede encontrar tipificado en los Artículos 202, 202 bis, 203, y 203 bis del Código Penal Federal, los cuales mencionan:

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo,

[60] Trejo García, Elma del Carmen, "*Regulación Jurídica de Internet*", Servicio de Investigación y Análisis, subdirección de Política Exterior, Cámara de Diputados. *http://www.diputados.gob.mx/cedia/sia/spe/SPE-ISS-12-06.pdf*

electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores. Sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

EL TURISMO SEXUAL EN CONTRA DE PERSONAS MENORES DE DIECIOCHO AÑOS DE EDAD O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA COMPRENDER EL SIGNIFICADO DEL HECHO O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA RESISTIRLO.

Articulo 203. Comete el delito de turismo sexual quien **promueva, publicite, invite, facilite o gestione** por cualquier medio a que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad, o con una o varias personas que no tienen capacidad para comprender el significado del hecho o con una o varias personas que no tienen capacidad para resistirlo.

Al autor de este delito se le impondrá una pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

Artículo 203 bis. A quien realice **cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad, o con una o**

varias personas que no tienen capacidad para comprender el significado del hecho o con una o varias personas que no tienen capacidad para resistirlo, en virtud del turismo sexual, se le impondrá una pena de doce a dieciséis años de prisión y de dos mil a tres mil días multa, asimismo, estará sujeto al tratamiento psiquiátrico especializado.

PROSTITUCIÓN.

La prostitución en México y sobre todo en el Internet, ha proliferado y se ha convertido en una verdadera Industria extremadamente lucrativa, tanto en adultos y mucho más la prostitución Infantil, la agresión viene de la industria sexual organizada que bajo el pretexto de turismo, lo que ofrece son vulneraciones tanto a Adultos y en más grado los menores que son víctima de la miseria y del hambre que existe en nuestro País, y nos enfrentamos a la Pasividad complaciente de los Estados, del País y del Mundo entero.

Hay muchos sitios en la red dedicados a promover a México como un destino para vacacionistas eróticos y el Turismo sexual, en el que Tijuana es uno de los sitios preferidos de los turistas sexuales.

La explotación sexual comercial puede tener consecuencias graves, duraderas de por vida, e incluso mortales, donde podemos encontrar desde embarazos, violaciones, lesiones, enfermedades de transmisión sexual, entre ellas el VIH-SIDA.

Finalmente debemos hacer notar que además de la existencia de leyes, políticas y programas para hacer frente a la explotación sexual comercial de las personas, se necesita una mayor voluntad política, medidas de implementación más efectivas y una asignación adecuada de los recursos para lograr la plena eficacia del espíritu y la letra de las leyes, políticas y programas, basta ya de ser indiferentes todos nosotros ante un problema de desintegración social.

El Código Penal Federal regula estas conductas ilícitas en sus numerales siguientes:

Artículo 204.- Comete el delito de lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo:

I.- Toda persona que explote el cuerpo de las personas antes mencionadas, por medio del comercio carnal u obtenga de él un lucro cualquiera;

II.- Al que induzca o solicite a cualquiera de las personas antes mencionadas, para que comercie sexualmente con su cuerpo o le facilite los medios para que se entregue a la prostitución, y

III.- Al que regentee, administre o sostenga directa o indirectamente, prostíbulos, casas de cita o lugares de concurrencia dedicados a explotar la prostitución de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, u obtenga cualquier beneficio con sus productos.

Al responsable de este delito se le impondrá prisión de ocho a quince años y de mil a dos mil quinientos días de multa, así como clausura definitiva de los establecimientos descritos en la fracción III.

LENOCINIO Y TRATA DE PERSONAS. (CODIGO PENAL FEDERAL)

Artículo. 206.- El lenocinio se sancionará con prisión de dos a nueve años y de cincuenta a quinientos días multa.

Artículo 206 BIS.- Comete el delito de lenocinio:

I.- Toda persona que explote el cuerpo de otra por medio del comercio carnal, se mantenga de este comercio u obtenga de él un lucro cualquiera;

II.- Al que induzca o solicite a una persona para que con otra, comercie sexualmente con su cuerpo o le facilite los medios para que se entregue a la prostitución, y

III.- Al que regentee, administre o sostenga directa o indirectamente, prostíbulos, casas de cita o lugares de concurrencia expresamente dedicados a explotar la prostitución, u obtenga cualquier beneficio con sus productos.

NARCOTRÁFICO.

La red se utiliza también para la transmisión de fórmulas Químicas para la fabricación de estupefacientes.

Para la coordinación de compra y venta de drogas y los lugares en los que se distribuye, rutas seguras para circular la droga e inclusive métodos para esconder droga y métodos para que ésta no sea detectada por las autoridades.

También se utiliza los medios y sistemas informáticos para blanquear el dinero proveniente de esta actividad ilícita.

"Las modalidades de blanqueo de dinero en la banca convencional y en la banca electrónica de acuerdo con los informes del Grupo de Acción Financiera (GAFI)".[61]

1. Ingresar grandes sumas de dinero en efectivo en una cuenta, con el fin de efectuar inmediatamente una transferencia electrónica a otra cuenta.
2. Numerosos depósitos de pequeñas cantidades, situadas por debajo de la obligación de declarar y en varias cuentas, desde las que se efectúan transferencias a otra cuenta, generalmente en el extranjero.
3. Uso de entidades off shore.
4. Introducción de personas de confianza en pequeñas entidades financieras o en delegaciones.
5. Cuentas de colecta o recaudación: Un número importante de inmigrantes hacen pequeños ingresos sucesivos que envían al exterior en forma agrupada.
6. Depósitos en cuentas extranjeras de una cantidad que actúa como garantía de un préstamo que es enviada al país de origen como una operación legítima que justifica la recepción de ese capital.
7. Las transferencias electrónicas son el principal instrumento utilizado en el blanqueo de dinero, debido a la rapidez con que se transfiere de un país a otro.
8. A pesar de la mejora en los sistemas de identificación de los clientes en las entidades financieras, sigue el problema de identificar de manera plena a la persona que ordena la transferencia.

[61] Los informes de GAFI (Grupo de Acción Financiera) consultado el 21 de febrero del 2013 sobre el blanqueo de dinero se encuentran visibles en *http://oecd.org/fatf/index.html.*

TERRORISMO.

El terrorismo informático se define como el uso de la tecnología informática y telemática con el objetivo de atacar infraestructuras nacionales críticas (tales como energía, transporte, u operaciones del gobierno) con el fin de intimidar a naciones enteras.

Muchos grupos terroristas del mundo están utilizando cada vez más las nuevas tecnologías informáticas y del Internet para formular planes, recaudar fondos, hacer propaganda, y comunicarse con seguridad. Grupos como la banda terrorista ETA (EUSKADI TA ASKATASUNA) e IRA (EJÉRCITO REPUBLICANO IRLANDES) incluyendo Hizbollah, HAMAS, la organización de Abu Nidal, y del terrorista Osama Bin Laden están utilizando ficheros automatizados, correo electrónico, y el cifrado de mensajes para utilizar sus operaciones.

En ocasión del levantamiento palestino de octubre y noviembre del 2000 se ha hecho evidentes ataques perpetrados directamente por organizaciones terroristas a sitios del gobierno estadounidense e israelitas, así como empresas multinacionales de capitales de ciudadanos de las naciones referidas anteriormente.

Todo ataque terrorista tiene por objeto generar terror en una determinada población o hacer que gobiernos, órganos u organismos internacionales cambien sus políticas, por ejemplo tenemos al ataque de las torres gemelas en la ciudad de Nueva York, el pentágono en Washington el 11 de septiembre de 2001 y las bombas en los trenes de Madrid el 11 de Marzo de 2004, que dejaron una gran secuela en la población y gobierno no sólo de esas dos naciones sino de todo el mundo, pero también se presenta la posibilidad de ataques llevados entre Estados ya sea de manera pública o clandestina con el fin de causar terror en la población de otro Estado o el cambio de opinión política, pero ahora con la Internet y la informática este tipo de ataques puede ser llevado a nuevas escalas nunca antes vistas en la humanidad.

En Abril del 2007, el gobierno de Estonia tomó la decisión de cambiar de lugar el Monumento al Combatiente Libertador Soviético, conocido como el Soldado de Bronce, en memoria de la victoria sobre el Fascismo en la Segunda Guerra Mundial, del centro de su Capital Tallin al cementerio militar de esa misma ciudad sobre una fosa en la que descansan los restos de 12 soldados del ejército rojo, para homenajear a los muchos soldados soviéticos que murieron en suelo estonio durante los combates contra las tropas nazis, causando indignación

y descontento en la Federación Rusa y en una minoría eslava, dañando aún más las ya deterioradas relaciones entre estas dos naciones.

Dando inicio a protestas en Tallin por activistas de organizaciones juveniles apoyadas desde Moscú, las que derivaron en violentos enfrentamientos con grupos nacionalistas causando la pérdida de un joven ruso de 20 años de edad, respondiendo el gobierno estonio con el empleo de la fuerza, tiempo después Estonia cerró temporalmente la sección consular de su Embajada, evacuando a sus diplomáticos junto con sus familiares, a su vez Rusia suspendió el suministro de petróleo vía ferrocarril alegando cuestiones técnicas, asimismo varias empresas rusas dejaron de importar productos estonios.

Pero no terminó en lo anterior, este conflicto se extendió al mundo de la Internet, días después del cambio de lugar de la estatua, Estonia fue víctima de un ciberataque en masa contra las redes informáticas del gobierno estonio de computadoras que se encontraban dentro de la Federación Rusa, y el sitio Web del partido al que pertenece el Primer Ministro estonio, después se extendió a las redes públicas dentro de servidores de su mismo país, así como, redes bancarias, financieras y comerciales, finalizando con redes privadas y cualquier red de servidores en otros países que sirvieran al pueblo y al gobierno estonio, causando un gran daño a su economía y de seguridad operacional, por lo que se solicitó ayuda a la OTAN debido a la naturaleza de este peculiar ataque, el cual envió expertos a Tallin para poder determinar la causa y el origen del ataque, el gobierno estonio alega tener pruebas que los ataques fueron originados dentro de Rusia e incluso ser coordinados por su gobierno, pero las autoridades rusas niegan y condenan dicho ataque.

En la impotencia contra estos ataques y en búsqueda de un responsable el Primer Ministro de Defensa estonio Aaviksoo reconoció: "actualmente, la OTAN no define a los Ciberataques de forma expresa como una acción militar, por lo que las provisiones del Articulo V del Tratado relativas a la defensa mutua…". Por lo que no se llegó a una solución de este nuevo tipo de ataques, siendo el primer ataque a escala masiva contra un Estado.

La finalidad de los ataques es tratar de inutilizar los sistemas automáticos de información, y de los sitios en el Internet, mediante el envío de virus informáticos, gusanos, bombas lógicas, de otros mecanismos considerados como conductas delictivas enmarcadas en el sabotaje informático.

En México tenemos contemplado el Terrorismo en el Código Penal Federal en los dispositivos siguientes:

TERRORISMO

Artículo 139.- Se impondrá pena de prisión de seis a cuarenta años y hasta mil doscientos días multa, sin perjuicio de las penas que correspondan por los delitos que resulten, al que utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo o instrumentos que emitan radiaciones, explosivos o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, realice actos en contra de las personas, las cosas o servicios públicos, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad para que tome una determinación.

La misma sanción se impondrá al que directa o indirectamente financie, aporte o recaude fondos económicos o recursos de cualquier naturaleza, con conocimiento de que serán utilizados, en todo o en parte, en apoyo de personas u organizaciones que operen o cometan actos terroristas en el territorio nacional.

Artículo 139 Bis.- Se aplicará pena de uno a nueve años de prisión y de cien a trescientos días multa, a quien encubra a un terrorista, teniendo conocimiento de sus actividades o de su identidad.

Artículo 139 Ter.- Se aplicará pena de cinco a quince años de prisión y de doscientos a seiscientos días multa al que amenace con cometer el delito de terrorismo a que se refiere el párrafo primero del artículo 139.

Artículo 145.- Se aplicará pena de cinco a cuarenta años de prisión y de ciento veinte a mil ciento cincuenta días multa, al funcionario o empleado de los Gobiernos Federal o Estatales, o de los Municipios, de organismos públicos descentralizados, de empresas de participación estatal o de servicios públicos, federales o locales, que incurran en alguno de los delitos previstos por este Título, con excepción del delito de terrorismo, cuya pena será de nueve a cuarenta y cinco años de prisión y de quinientos a mil ciento cincuenta días multa.

ESPIONAJE.

Revisemos la siguiente definición de espionaje informático: "Es toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información".

En el derecho se ha entendido por espionaje informático, aquel delito que consiste en obtener una información de forma no autorizada, sea por motivo de lucro o de simple curiosidad, hecho que implica espiar y procurarse una comunicación o bien una utilización de un sistema de tratamiento de la información en forma desleal, no autorizada.

Se clasifica al delito de espionaje informático en:

a) Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.

b) Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

Se pensaba de forma general que la comisión de un delito informático era facultad de personas, que tenían conocimientos relacionados con la Informática y las Nuevas Tecnologías de Información.

En la actualidad, existe un consenso en el derecho comparado de estimar que cualquier persona puede ejecutarlos, no es necesario que se inviertan miles de dólares para la compra de equipos sofisticados para el cometimiento del delito de espionaje informático.

En la actualidad este delito preocupa especialmente a las empresas, es aquí justamente donde ha sido evidente ya que puede ser muy lucrativo para su autor, lo que lo hace especialmente peligroso y con enormes repercusiones técnicas y económicas.

Hay un caso célebre descubierto por el Servicio de Contraespionaje de la República Federal Alemana en 1989, en el cual un grupo de jóvenes alemanes expertos en Informática, pagados por la KGB soviética accedieron a los datos de los sistemas de el Pentágono, la NASA, del Consorcio Franco-Italiano Thompson, del Centro de Investigaciones Nucleares de Ginebra, de la Agencia Espacial Europea y del Instituto Max Planck de física nuclear en Heildelberg entre otros.

En el campo del espionaje informático donde queda más al descubierto la precariedad de los sistemas de seguridad, incluso estatales y la vulnerabilidad de los sistemas de tratamiento

de la información, de los datos en él contenidos y de la gravedad e importancia a nivel internacional del problema de la creciente criminalidad informática.

ESPIONAJE INDUSTRIAL.

En este numeral tomaremos muy en cuenta las opiniones del Dr. Manfred Mohrenschaleger quien afirma que los secretos empresariales y el valioso know how son almacenados en ordenadores o computadores.

Junto a las formas tradicionales de espionaje económico, han surgido un nuevo tipo de delito, el espionaje informático. De esta forma el objeto del delito puede ser tanto el hardware como el software, además de los datos almacenados, desempeñando un papel de gran importancia la copia y uso no autorizado de programas de computadora.

El delito puede ser cometido por la copia ilícita de datos almacenados y la intervención de las líneas de transmisión de datos, es decir a intervención de la transmisión o de las radiaciones electrónicas de las pantallas de los terminales.

PIRATERÍA

El fenómeno de la "piratería" cometida en perjuicio del derecho de autor, los derechos conexos y la propiedad industrial constituye hoy día en México una práctica ilícita que afecta gravemente a nuestra planta productiva.

La actividad creativa se ha visto afectada por la piratería, entendiéndose como tal, de manera enunciativa y no limitativa, toda aquella producción, reproducción, importación, comercialización, almacenamiento, transportación, venta, arrendamiento, distribución y puesta a disposición de bienes o productos en contravención a lo previsto por la Ley Federal del Derecho de Autor y la Ley de la Propiedad Industrial.

Dicho fenómeno ha afectado la creación de empleos y el crecimiento económico; puesto en entredicho la perspectiva de desarrollo de sectores estratégicos para el país; limitado el crecimiento y la participación de empresas formales y productivas en el mercado y ocasionado escenarios de competencia desleal al aumentar la economía informal y al disminuir la calidad de productos y servicios.

Asimismo, ha impedido al erario federal la posibilidad de aumentar su recaudación y desalentado la actividad creativa al impedir la aparición continua de nuevos y mejores productos y servicios en el mercado, que es uno de los signos clave para evaluar la competitividad de un país.

La piratería ha provocado, también, la promoción de una "cultura de ilegalidad" que niega respeto y seguridad jurídica a los titulares de derechos y que debilita la vigencia de un Estado de Derecho.

El impacto de la piratería demanda definir una Política de Estado para contenerla de inmediato y para erradicarla. Como Política de Estado, su ejercicio deberá ser permanente.

Una Política de Estado garantiza permanencia en la agenda nacional a los ejes de acción que le animan. Dos ejes de acción deben apuntalar esa Política de Estado:

PRIMERO. El combate a la ilegalidad en materia del derecho de autor, los derechos conexos y la propiedad industrial y

SEGUNDO. La recuperación del mercado interno. Ambas acciones deben desarrollarse concomitantemente para transitar con éxito hacia el propósito señalado.

El despliegue de esfuerzos por separado y sin coordinación dificultaría alcanzar dichas metas.

La ejecución de los ejes señalados debe atender a algunas variables socio-económicas que subyacen en el fenómeno de la piratería y que no pueden soslayarse. Destacan particularmente el desempleo, el subempleo, el bajo poder adquisitivo y la pérdida del mercado interno de los sectores productivos.

Como Política de Estado, los tres órdenes de Gobierno, Federal, Estatal y Municipal, deberán participar en su ejecución, pero también los tres poderes que sustentan al Estado, el Ejecutivo, el Legislativo y el Judicial.

Esta participación debe darse con absoluto respeto a su autonomía y esfera de competencias. El compromiso expreso y eficaz del Estado Mexicano para contener y erradicar la piratería es indispensable para lograr la meta planteada.

Asimismo, la participación de los sectores productivos y de la sociedad civil resulta fundamental para consolidarla; sin ellos sería imposible lograr su consecución. En el escenario planteado los industriales asumen una participación determinante. De acuerdo con sus perspectivas de desarrollo, deberán desarrollar proyectos que les permitan recuperar su

mercado. En esa tesitura resulta indispensable que atiendan a la sociedad civil, su gran consumidor.

Es imprescindible tener en cuenta el escenario internacional en que se plantea la Política de Estado señalada. Los compromisos del Estado Mexicano frente a la comunidad internacional en materia del derecho de autor, los derechos conexos y la propiedad industrial, así como de regulación de comercio deben reflejarse necesariamente en su contenido.

La consecución de la tarea señalada obliga a establecer una Agenda Nacional que defina la participación coordinada de los sectores público y privado en función de las consideraciones expuestas.

La definición de dicha Agenda debe partir de las siguientes consideraciones:

A. El impacto de diversas variables socio-económicas en un alto porcentaje de nuestra población, tales como: el bajo nivel del poder adquisitivo de los salarios, el desempleo y el subempleo;

B. El desarrollo de tecnologías que facilitan la reproducción de obras y productos tutelados por la legislación autoral y de propiedad industrial;

C. La oferta indiscriminada de bienes y servicios de origen ilegal;

D. Un marco jurídico regulador de los derechos y de los ilícitos en materia del derecho de autor, los derechos conexos y la propiedad industrial, así como del comercio interior y exterior que puede perfeccionarse;

E. La falta de una cultura de aprecio al valor de las ideas y de la creatividad;

Hay que ofrecer una mejor calidad de vida a nuestras generaciones futuras, por lo que a través de su cumplimiento se pretende lo siguiente:

I. Reactivar la planta industrial;

II. Fortalecer el desempeño, la participación y el crecimiento de empresas formales en el mercado;

III. Crear empleos y procurar un mayor crecimiento económico nacional;

IV. Incrementar el universo de contribuyentes que generen recursos al erario federal y que permitan fortalecer el gasto social.

V. Fortalecer la cultura de legalidad que debe imperar en nuestras relaciones sociales.

VI. Asegurar una eficiente procuración y administración de justicia que disminuya los índices de impunidad.

ACUERDO NACIONAL CONTRA LA PIRATERÍA

El Código Penal Federal Contempla los Delitos en Materia De Derechos De Autor en sus numerales siguientes:

Artículo 424.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;

II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada. Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 424 ter.- Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código.

Artículo 425.- Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa, a quien publique a sabiendas una obra substituyendo el nombre del autor por otro nombre.

Artículo 428.- Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor.

Artículo 429.- Los delitos previstos en este Título se perseguirán de oficio, excepto lo previsto en los artículos 424, fracción II y 427.

DELINCUENCIA ORGANIZADA

Cuando con el transcurso del tiempo la delincuencia "común", llega a tal extremo de "evolución" o "perfeccionamiento"; cuando rebasa los límites de control gubernamental; o cuando establece líneas especiales de operación basadas en un sistema complejo, tipo empresarial, muy bien estructurado en su comisión; cuando persigue a través de determinadas acciones violentas la búsqueda del poder, ya sea político, económico o social, es cuando podemos decir, sin lugar a dudas, que estamos frente a un caso de delincuencia organizada.

El concepto "delincuencia organizada" fue empleado por primera vez por el criminólogo norteamericano John Ladesco en 1929, para designar a las operaciones delictivas provenientes de la mafia.

Este tipo de delincuencia fue designada con la palabra "organizada", ya que se refiere a la "asociación", a la "sociedad", a la "corporación", al "grupo", al "sindicato", a la "liga", al "gremio", a la "coalición", en sí a la "unión", como forma de conjuntar esfuerzos en grupo; y con el empleo de la violencia, soborno, intimidación y fuerza, los delincuentes llevaban a cabo sus actividades ilegales.

La fuerza de la delincuencia organizada radica en el establecimiento de "alianzas y vínculos" que logra en todos los niveles, incluyendo el político y el militar; con la ayuda de actos de corrupción logran su impunidad.

Así, las organizaciones dedicadas a la delincuencia organizada emprenden operaciones ilegales de tipo financiero, mercantil, bancario, bursátil o comercial; acciones de soborno, extorsión; ofrecimiento de servicios de protección, ocultación de servicios fraudulentos y ganancias ilegales; adquisiciones ilegítimas; control de centros de juego ilegales y centros de prostitución, tráfico de armas, narcotráfico.

Por ello, la delincuencia en su manifestación organizada constituye uno de los más graves y vitales problemas que dañan y perjudican a la humanidad.

Cuando la delincuencia organizada construye conexiones con organizaciones similares formando redes en todo el mundo, la Organización de las Naciones Unidas la identifica como delincuencia organizada transnacional.

La delincuencia organizada tiene un eje central de dirección y mando y está estructura en forma celular y flexible, con rangos permanentes de autoridad, de acuerdo a la célula que la integran; alberga una permanencia en el tiempo, más allá de la vida de sus miembros; tienen un grupo de sicarios a su servicio; tienden a corromper a las autoridades; estos son dos de los recursos conocidos para el cumplimiento de sus objetivos; opera bajo un principio desarrollado de división del trabajo mediante células que sólo se relacionan entre sí a través de los mandos superiores.

Este tipo de delito ha tenido tanto impacto en nuestro país que se legislo al nivel más alto en Nuestro país; que es en nuestra Constitución Política de los Estados Unidos Mexicanos; y que es materia fundamental de las nuevas reformas penales; y lo tenemos previsto en sus numerales 16, 18, 19, 20, 22 y 73.

FRAUDE

Estaríamos ante la figura del fraude electrónico, cuando en las compras en línea entre particulares te ofrecen un producto (un bien) así como las especificaciones, se realiza el pago, y o no llega el producto o el producto recibido no cumple con lo ofertado.

También las Instituciones de Crédito que constituyen uno de los pilares más importantes en nuestro país son susceptibles de fraudes electrónicos e implican una lesión no sólo a los particulares sino también a la propia Institución a que hacemos referencia y pone en peligro, tanto su funcionamiento como la confianza de los sujetos económicos, por eso la importancia de "una protección a esta figura" como "fraude electrónico". Esta figura no está contemplada en el Código Sustantivo Federal.

Un ejemplo de ellos sería cuando se da la "clonación de tarjetas de crédito y debito", esto es la transferencia de información de la tarjeta de la víctima para utilizarla en compras fraudulentas. La transferencia de la información de una tarjeta a otra falsa es una práctica llamada "skimming".

Otro ejemplo de fraude electrónico dentro de las Instituciones de Crédito, es cuando un individuo ocurre al cajero automático y este se encuentra viciado de forma electromagnética y obtienen el número de (NIP) (Número Inter Personal) y dejan sin dinero la cuenta bancaria.

ROBO

Esta figura se va a aplicar cuando se utilicen medios eléctricos o magnéticos o electromagnéticos, aquí entraría el robo de la señal de Internet, e inclusive los delitos contra las Instituciones de Crédito cuando por alguna manipulación en equipos de cómputo se obtiene un beneficio hay que aclarar que entraría en el supuesto de "Robo" y no de "Fraude" puesto que no se puede engañar a una máquina esto es sólo susceptible de los individuos aquí estaríamos dentro del supuesto de robo, puesto que por esa modificación o manipulación de máquinas (obtienen un beneficio económico); es decir dinero. (Técnica Salami) y este ilícito se encuentra regulado en el Código Penal Federal en los numerales que a la letra dicen:

Artículo 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.

Artículo 368.- Se equiparan al robo y se castigarán como tal:

I.- El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y

II.- El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Artículo 371.- Para estimar la cuantía del robo se atenderá únicamente el valor intrínseco del objeto del apoderamiento, pero si por alguna circunstancia no fuere estimable en dinero o si por su naturaleza no fuere posible fijar su valor, se aplicará prisión de tres días hasta cinco años.

En los casos de tentativa de robo, cuando no fuere posible determinar su monto, se aplicarán de tres días a dos años de prisión.

Cuando el robo sea cometido por dos o más sujetos, sin importar el monto de lo robado, a través de la violencia, la acechanza o cualquier otra circunstancia que disminuya las

posibilidades de defensa de la víctima o la ponga en condiciones de desventaja, la pena aplicable será de cinco a quince años de prisión y hasta mil días multa. También podrá aplicarse la prohibición de ir a lugar determinado o vigilancia de la autoridad, hasta por un término igual al de la sanción privativa de la libertad impuesta.

2.7 BIENES JURÍDICOS

En primer término tenemos que precisar y determinar que son los bienes jurídicos que se lesionan por las conductas ilegales denominados como delitos informáticos, debemos primero esgrimir a los grandes tratadistas del Derecho Penal para entender y comprender el Concepto de bienes jurídicos.

Para el erudito Von Liszt: *"Los bienes jurídicos son aquellos intereses que son trascendentes, y de interés para el individuo o la comunidad. No es el ordenamiento jurídico lo que crea el interés, sino la vida; pero el resguardo jurídico va a elevar el interés vital a bien jurídico tutelado. Los intereses vitales deben ser necesarios para la convivencia comunitaria luego de lo cual y como consecuencia de ello serán protegidos normativamente bajo juicios de valor positivo"*.[62]

Para el Doctor Francisco Muñoz Conde: *"Nos describe a los bienes jurídicos como aquellos presupuestos que la persona requiere para su auto realización y el mejoramiento de su personalidad en la vida social"*.[63]

Los bienes jurídicos en el Derecho Penal son muy trascendentales puesto que establecen cuales son los intereses que la sociedad considera imprescindibles para proteger.

El legislador a través de la norma sustantiva penal va a otorgar la protección jurídica a los bienes referidos, normas que trasladarán la amenaza y la imposición de una pena.

El bien jurídico puede exteriorizarse como: *"El objeto de protección de la ley o como objeto de ataque contra el que se rige el delito y no debe confundirse con el objeto de la acción que pertenece al mundo de lo*

[62] Citando a Von Liszt Frank, Cit. Por Bustos, Ramírez Juan y otro, "*Derecho Penal Latinoamericano comparado Parte General*". Buenos Aires, Argentina 1981, pp 130 y 131.
[63] Muñoz Conde, Francisco y otro, "*Manual de Derecho Penal*", p 54.

sensible. Siguiendo el ejemplo más común; el robo, el objeto de la acción es la cosa que es sustraída; el objeto de la protección es la propiedad".[64]

2.8 LOS BIENES JURÍDICOS PROTEGIDOS EN EL DELITO INFORMÁTICO

Dentro de los ilícitos informáticos, podemos expresar que la predisposición es la protección a los bienes jurídicos, y se realizara desde el punto de vista de los delitos tradicionales, con una reinterpretación teleológica de los tipos penales ya existentes, para enmendar las lagunas de ley originadas por las novedosas conductas delictivas. Esto sin duda dará como regla general que los bienes jurídicos tutelados, serán los mismos que los delitos reinterpretados o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte de los órganos jurisdiccionales competentes, Federales o Locales.

Por otro lado otra corriente doctrinaria presume la emergente sociedad de la información, que hace totalmente necesaria la incorporación de valores inmateriales y de la Información, como bien jurídico tutelado, esto tomando en consideración las diferencias existentes por ejemplo: entre la propiedad tangible y la propiedad intangible. Esto en cuanto a la información no puede ser tratada de la misma forma en que se emplea a los bienes corporales.

Si bien es cierto que los bienes tienen valor compartido, que es una tasación económica, es por tanto que la información y otros intangibles son objetos de propiedad. Y lo encontramos protegida Constitucionalmente.

La información en cuanto a un bien jurídico tutelado debe tener perennemente en cuenta el principio de la necesaria protección de los bienes jurídicos que señala la penalización de conductas, bajo el principio de dañosidad y lesividad. Así una conducta sólo puede deducirse con una pena cuando resulta del todo incompatible con los presupuestos de vida en común, pacífica, libre y materialmente asegurada.

[64] Enciclopedia Jurídica Omeba, T II, p 189.

Su origen lo encontramos cimentados en la Teoría del Contrato Social de Juan Jacobo Rosseau, y su máxima expresión la podemos confirmar en la maravillosa obra del Marqués de Beccaria "De los Delitos y las Penas", en donde se precisa como un bien vital, "bona vitae", estado social valioso, perteneciente a la comunidad o al individuo, que por su significación es garantizada, a través del poder punitivo del Estado, a todos de forma igual.

Es por ello que podemos inferir que el bien jurídico tutelado en general es la información, pero está meditada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y de tráfico jurídico, y finalmente por los sistemas que procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales como lo son:

1. Derecho a La Intimidad y Confidencialidad
2. Derecho a La Información
3. Derechos Patrimoniales
4. Seguridad Nacional

En tal virtud el bien jurídico protegido, acoge varios puntos como lo son, la confidencialidad, la integridad, la disponibilidad de la información y de los sistemas informáticos en donde ésta se acumula, almacena o se transfiere.

Por eso podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan una diversidad de ellos que ponen de relieve intereses colectivos, en tal sentido María Luz Gutiérrez Francés nos dice: *"La representación del fraude informático presenta indudablemente un carácter pluriofensivo, en cada una de sus modalidades se causa una doble afección; la de un interés económico (ya sea micro o macro social), como la del sistema financiero, el sistema crediticio, el patrimonio, y la de un interés macro social vinculado al funcionamiento de los sistemas informáticos"*.[65]

[65] Gutiérrez Francés, María Luz, "*Fraude Informático y Estafa*", Centro de Publicaciones del Ministerio de Justicia, Madrid España, 1991.

Por tanto el origen de esta nueva tecnología, está proveída a nuevos elementos para atentar contra bienes ya existentes como lo son (la intimidad, la seguridad nacional, el patrimonio, etc).

2.9 DERECHO A LA INTIMIDAD Y CONFIDENCIALIDAD

En virtud de un ensayo denominado como: "The right privacy", el cual fue publicado en Estados Unidos de América a fines del siglo XIX en el que dos abogados norteamericanos exponen que todo individuo debe de ser dejado en paz, tiene derecho a proteger su soledad, su vida íntima, y de la misma forma a proteger en todo momento su vida privada, este conocimiento ha ido evolucionando y ahora no solamente se refiere a las relaciones de los individuos particulares, sino también a las relaciones entre los ciudadanos y la administración pública.

Las empresas públicas y privadas que resguardan los datos concernientes a los individuos como lo son el nombre, su domicilio, el lugar de su nacimiento, los números telefónicos que tiene; los datos como el estado de salud que tiene, constituyen datos que se consideran como íntimos, y que la doctrina los ha calificado dentro de la categoría de **datos sensibles**, incluyendo los hábitos o preferencias sexuales, creencias religiosas, preferencias en productos o preferencias políticas de una persona.

Cuando los datos como nombre, domicilio, números de teléfono, que son datos personales que son puestos a disposición de un gran número de personas, como lo puede ser el Directorio Telefónico, si no se quieren hacer públicos, es necesario indicar a la compañía telefónica que se quiere tener un número privado, en tal circunstancia esos datos no aparecerán al público, en caso del padrón electoral solo las autoridades judiciales o administrativas tendrán acceso a ellas, hay datos que se consideran públicos como el Registro Público de la Propiedad, Catastro e inclusive el Sistema de Tesorería de los Estados, a estos se les denominan datos públicos.

El Derecho a la Intimidad y a la Confidencialidad se rige como un medio de control y de protección a los datos sensibles de las personas, ya sea que estos se encuentren informatizados o no, en otras palabras es brindar la protección a la vida privada e intima de todos los individuos que se encuentran almacenados en archivos automáticos o informáticos, el legislador tanto en nivel federal como local deberá de ser muy cuidadoso y tomar muy en cuenta para elaborar y analizar la normatividad jurídica para proteger la intimidad del individuo al momento de utilizar los medios Informáticos y las Nuevas Tecnologías.

Sobre el Derecho a la Intimidad la Doctrina Española es muy basta y se ha desarrollado muy acertadamente y nos indica que es: "La facultad de aislamiento (ius solitundis) al poder del control sobre las informaciones relevantes para cada sujeto, observándose un adelanto positivo para los Españoles y presenta un doble aspecto; por un lado un derecho de protección de la persona y por el otro, el control de las informaciones que afectan, entendido éste como un derecho de intervención, hay aspectos específicos de la intimidad como lo es el propio cuerpo, la ampliación del concepto al entorno familiar y el derecho al olvido. Con referencia al olvido, éste consiste en la facultad que tiene un individuo o su familia de que no se traigan al presente hechos verídicos realizados en el pasado, deshonrosos o no y que por el simple transcurso del tiempo no son conocidos socialmente, pero que de divulgarse puedan aparejarle el descrédito público. *"El derecho al olvido, en el caso del tratamiento de los datos personales, implica que éstos tengan un periodo de vida útil, y después del cual su permanencia en los archivos manuales o automatizados podría resultar lesiva, o dañosa y estigmatizadora del individuo, obstaculizando su inserción en la sociedad y el desarrollo pleno de su personalidad"*.[66]

"Para los tratadistas Españoles como el Doctor Navarra y el Doctor Pérez Luño, se trata de proteger lo que la doctrina anglosajona denomino "PRIVACY", término castellanizado como "PRIVACIDAD", que le va garantiza al ciudadano en todo momento el derecho a exigir que permanezca en su esfera interna el resultado del tratamiento de su información personal. En España este Derecho se encuentra regulado por la Ley Orgánica de Protección de Datos de Carácter Personal 15/99 Vigente en España".[67]

---

[66] Carrillo, Marc, "*Los Límites a la Libertad de Prensa en la Constitución Española De 1978*", Promociones y Publicaciones Universitarias (PPU), p 73.

[67] Se puede revisar el texto íntegro de La Ley Orgánica de Protección de Datos de Carácter Personal de España (LOPD), 22 de febrero del 2013, *http://club.telepolis.com/vicenti/ce78/Vicenti/lotc/Vicenti/lloo/lo15_99.htm*

El perfeccionamiento del contenido del derecho a la privacidad a que dentro de éste confluye en un conjunto más amplio de espacios de lo individual, que ameritan protección jurídica. Es el caso de los **Derechos a la imagen, al nombre y a la voz y al olvido, cuestiones que en México no tenemos ni contemplados ni regulados**.

El derecho de acceso a datos, contratos y documentos en poder del Estado, es un tema muy delicado y relevante que es esencial para las Sociedades modernas del siglo XXI, pero no debe de ser confundido con la garantía del "HABEAS DATA", **que es el derecho al conocimiento por parte de la persona, de sus propios datos y con el principio de "Auto Determinación Informativa, que es el derecho del interesado a ejercer el control sobre informaciones que se refieren a sí mismo, que se amparan y que es el derecho de cada persona para controlar y decidir exclusivamente sobre el procesamiento de sus datos personales y nominativos, sea por entes Estatales o por Empresas particulares**.

En México esta protección a la Intimidad la encontramos en los artículos 1, 14 y 16 Constitucionales:

Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

Las normas que son referentes a los derechos humanos se dilucidarán de conformidad con esta constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia, que es lo que se denomina (principio pro persona).

Todas las autoridades, en el entorno de sus competencias, van a tener la obligación de promover, respetar, proteger y garantizar los derechos humanos (fundamentales) de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

Está expresamente prohibida la esclavitud en los Estados Unidos Mexicanos. Los esclavos del extranjero que entren al territorio nacional alcanzarán, por este solo hecho, su libertad y la protección de las leyes.

Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Artículo 14. A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna. Nadie podrá ser privado de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las Leyes expedidas con anterioridad al hecho.

En los juicios del 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 trata.

En los juicios del orden civil, la sentencia definitiva deberá ser conforme a la letra o a la interpretación jurídica de la ley, y a falta de ésta se fundará en los principios generales del derecho.

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

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.

Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a disposición de la autoridad más cercana y ésta con la misma prontitud, a la del Ministerio Público. Existirá un registro inmediato de la detención.

Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder.

En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley.

La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días.

Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.

Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.

En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la

diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia.

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración.

La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.

La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.

La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley. En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.

2.10 DERECHO A LA INFORMACIÓN

Las ciencias informáticas nos han obsequiado nuevas tecnologías y estas han sido cuantiosas, entre las cuales podemos destacar las telecomunicaciones y la telemática, pero cabe hacer la anotación de su mala utilización y su aprovechamiento traen como consecuencia que se ejecuten nuevos tipos de atentados a bienes jurídicos de protección penal.

El procedimiento automatizado de los datos que se han dado en las últimas décadas de información se ha logrado la difusión de contenidos con mucha más velocidad, que épocas anteriores de la humanidad, un ejemplo de ello es que en el año de 1865 se necesitaron 12 días para conocer en Europa el asesinato del Presidente de Estados Unidos Abraham Lincoln. Cien años después de ese acontecimiento el 22 de Noviembre de 1963 bastaron 12 minutos para que se difundiera el asesinato del también Presidente de Estados Unidos John F. Kennedy. En 1990 el mundo entero miró atónito, por televisión abierta, los bombarderos de Bagdad-Irak en la llamada guerra del Golfo, imágenes que llegaron a nuestros hogares de forma inmediata, sin mediar tan sólo un segundo entre la realidad y las imágenes que se observaban, al igual que los ataques sufridos el 11 de Septiembre de 2001 a Estados Unidos en las Torres Gemelas de Nueva York, mismas que al instante que fueron atacadas lo veíamos inmediatamente en nuestros televisores como si fuera una película de Acción, cuando en realidad la tragedia estaba en vivo y en directo en el mundo entero.

Advirtamos que actualmente el alcance que tienen el concepto de derecho a la información para entender porque se protege este bien jurídico en la opinión del autor Frosini: *"Que es el derecho que todos tenemos de ser informados de lo que sucede y puede interesarnos; y es también el derecho atribuido en particular a los periodistas, a los reporteros gráficos, a los operadores de televisión, de informar a los lectores a los espectadores de televisión a cerca de los acontecimientos. Este derecho consiste en la*

libertad de recoger e intercambiar informaciones, se encuentra reconocido como uno de los derechos humanos en los acuerdos de Helsinki de 1975, suscrito entre Estados Unidos, la Unión Soviética y los países Europeos".[68]

Nuestra legislación la resguarda en el mismo sentido del autor antes precisados y ese derecho lo tenemos legislado y contemplado en: **Nuestra Constitución Política de los Estados Unidos Mexicanos** en sus artículos 6 y 7 que a la letra dicen:

Artículo 6. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos.

Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

[68] Frosini, Vittorio, *"Informática y Derecho"*, Editorial Temis, Bogotá Colombia, 1988, p 66.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

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

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delito de prensa, sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos.

En México tuvo un importante resultado la transparencia de la Información de la Administración Pública, por lo que surgió la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y en su artículo 4 de la mencionada ley dice a la letra:

Artículo 4. Son objetivos de esta Ley:

I. Proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos;

II. Transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados;

III. Garantizar la protección de los datos personales en posesión de los sujetos obligados;

IV. Favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados;

V. Mejorar la organización, clasificación y manejo de los documentos, y

VI. Contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

Este último artículo es el que sustenta el Derecho de Acceso a la Información Pública, de lo que se trata este contexto es una dimensión de la transparencia, y consiste en la facultad que tiene toda persona de acceder a la información gubernamental, en poder de las instituciones públicas; es decir, es el derecho de solicitar información y recibir la misma sin necesidad de acreditar que se tiene un interés legitimo ni de justificar la finalidad de para que se solicita la información.

2.11 DERECHOS PATRIMONIALES

Para poder fijar la protección de los derechos patrimoniales primero es conveniente dar y desarrollar ampliamente el concepto de patrimonio y es: "El conjunto de los bienes y derechos pertenecientes a una persona, física o jurídica. Históricamente la idea de patrimonio estaba ligada a la de herencia. La palabra es también utilizada para referirse a la propiedad de un individuo, independientemente como sea que la haya adquirido. Desde este punto de vista, el individuo puede ser ya sea una persona física o Moral".

Así cuando se habla de las personas morales también ellas cuentan con el Patrimonio Empresarial que es: "El conjunto de bienes, derechos y obligaciones, pertenecientes a una empresa como persona moral y que constituyen los medios económicos y financieros a través de los cuales ésta puede cumplir sus objetivos".

En el ámbito legal el concepto significa: "El conjunto de relaciones jurídicas pertenecientes a una persona física o moral, que tienen una utilidad económica y por ello son susceptibles de estimación pecuniaria, y cuya relaciones jurídicas están constituidas por derechos y obligaciones (activos y pasivos)".

ACTIVO

El activo comprende todos los bienes y derechos de un mismo propietario. Es la pertenencia al mismo sujeto de una serie de derechos. Bajo esta designación se engloban los bienes y los derechos (tanto reales como de crédito).

PASIVO

Sobre el pasivo patrimonial caen todas las obligaciones, deudas y cargas en general. Este pasivo es resguardado por los activos que forman parte del patrimonio. Así, por ejemplo, en una sucesión, los herederos reciben un patrimonio, que si incluye deudas no satisfechas y exigibles, deben satisfacerlas con el activo de la sucesión.

La mayoría de los escritores trazan el origen de la teoría del patrimonio como: "el conjunto de relaciones jurídicas valorables en dinero, que son los activos o pasivos de la misma persona y que se considera como constituyendo una universalidad jurídica".

Lo anterior involucra varias cosas: Cada persona tiene un patrimonio (por decirlo así, una característica o atributo universal de las personas físicas o morales) y ese patrimonio es individual, único, indivisible. Sigue que el patrimonio como tal es diferente a lo que lo constituye (el patrimonio es como una bolsa, cuyo contenido son derechos de propiedad, etc.). Sigue también que no todos los derechos o bienes de una persona son patrimoniales (solo aquellos capaces de ser evaluados monetariamente).

El patrimonio es independiente de los bienes que una persona posea. Inclusive, una persona puede no tener ningún bien, y aún así, tiene un patrimonio. Es en otras palabras, una *aptitud para poseer*, de tal forma que el patrimonio de una persona también incluye derechos de propiedad futuros. En el sentido, por ejemplo, que una obligación actual recae sobre cualquier bien (o derecho sobre tal), incluso los adquiridos en el futuro). Por eso el nonato es susceptible de heredar.

Los bienes de la persona forman un todo unitario que responde por las obligaciones que esta haya contraído, es decir, cuando una persona se obliga, obliga a la masa de bienes.

LA VINCULACIÓN A LA PERSONALIDAD

El patrimonio es un resultado de la personalidad. Los elementos tanto del activo como del pasivo, se hallan sometidos a las disposiciones de una única voluntad: las de la persona titular. De esta premisa se desprenden dos principios:

1. Solo las personas pueden tener patrimonio: esto acapara tanto las personas físicas como morales.
2. Toda persona tiene un patrimonio: con la separación de los bienes del patrimonio, se llega a la conclusión que toda persona tiene un patrimonio, cuyos contenidos varían. El patrimonio no es más que una potencialidad adquisitiva que toda persona tiene.

Los que sufren más ataques por el delito informático en cuanto al patrimonio son principalmente dos:

1. **Las Instituciones Bancarias y de Crédito**
2. **Los Derechos de Autor**
3. **Estafas electrónicas (comercio en línea), subastas en línea y robo de servicios**

Los primeros precisados son quienes más recienten la afectación directa de los delitos patrimoniales, esto en virtud de la comisión de delitos informáticos en México según un análisis realizado por BANAMEX, CITYBANK, **son las Instituciones Bancarias Mexicanas** por medio del fraude electrónico; y de las transferencias de fondos, de igual forma por la llamada manipulación de los datos de salida, los cuales causan una gran afectación a los usuarios de la banca, y a la banca misma, siendo Estados Unidos el principal país que es blanco de dichos ataques informáticos, con un cincuenta y dos por ciento, los ataques informáticos se conciben primordialmente en contra de los clientes y no precisamente en contra de la Institución Crediticia, lo que obedece a los altos sistemas de protección de que gozan las Instituciones Bancarias, tales ataques se llevan a cabo a través de dos programas principalmente los cuales se han denominado: **PHISING Y PHARMING**, el propósito de esos programas es hacerse de los recursos del usuario de la banca, aprovechándose de dos

factores básicos que toman en consideración los defraudadores, los cuales son el nivel técnico y cultural del usuario y la nata curiosidad del ser humano.

Ante los múltiples ataques de los defraudadores cibernéticos se han instrumentado continuamente sistemas novedosos de protección que deben tener cualquier usuario de internet entre los cuales se destacan:

1. Tener una herramienta antivirus vigente y actualizada
2. Poseer herramientas anti intrusos
3. Tener un firewall personal
4. Tener autorizados parches de seguridad y
5. Controlar las entradas y salidas de las unidades USB y otras Memorias para evitar las descargas de impresiones fotográficas u otras cosas.

Además también se recomiendan las consecutivas medidas:

1. No compartir el e-mail
2. No enviar información confidencial
3. No dar CLIC a las ligas adjuntas a e-mails y
4. Proteger siempre al equipo con antivirus

A los esfuerzos de las citadas Instituciones Bancarias se amplía la creación de la unidad **ICRAI** cuya finalidad y objetivo esencial es el análisis exhaustivo de los sistemas informáticos a través de los sistemas de cómputo forense, por medio de los cuales pueden estudiar los múltiples registros anteriores de las computadoras, y así también llevan a cabo la investigación y reconocimiento de las computadoras que en el momento en que se están utilizando.

Estas medidas de seguridad proporcionaran un gran alivio para detectar los FRAUDES CIBERNÉTICOS, en el momento oportuno lo cual se tiene vislumbrado en nuestra legislación en el artículo 52 de la Ley de Instituciones de Crédito que dice:

Artículo 52.- Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios

electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente:

I. Las operaciones y servicios cuya prestación se pacte;

II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso;

III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

Cuando las instituciones bancarias y de crédito así lo convengan con su clientela, las instituciones podrán suspender o cancelar el trámite de operaciones que se pretendan realizar mediante el uso de equipos o medios electrónicos a que se refiere el primer párrafo de este artículo, siempre y cuando cuenten con los elementos bastantes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma inadecuada o indebida. Lo anterior también resultará aplicable cuando las instituciones detecten algún error en la instrucción respectiva.

De igual manera, las instituciones podrán pactar con su clientela que, cuando ésta haya recibido recursos mediante alguno de los equipos o medios señalados en el párrafo anterior y aquéllas cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida, podrán restringir hasta por quince días hábiles la disposición de tales recursos, a fin de llevar a cabo las investigaciones y las consultas que sean necesarias con otras instituciones de crédito relacionadas con la operación de que se trate. La institución de crédito podrá prorrogar el plazo antes referido hasta por diez días hábiles más, siempre que se haya dado vista a la autoridad competente sobre probables hechos ilícitos cometidos en virtud de la operación respectiva.

No obstante lo previsto en el párrafo anterior, cuando las instituciones así lo hayan acordado con su clientela, en los casos en que, por motivo de las investigaciones antes referidas, tengan evidencia de que la cuenta respectiva fue abierta con información o documentación falsa, o bien, que los medios de identificación pactados para la realización de la operación de que se trate fueron utilizados en forma indebida, podrán, bajo su responsabilidad, cargar el importe respectivo con el propósito de que se abone en la cuenta de la que procedieron los recursos correspondientes.

Las instituciones que por error hayan abonado recursos en alguna de las cuentas que lleven a su clientela, podrán cargar el importe respectivo a la cuenta de que se trate con el propósito de corregir el error, siempre que así lo hubiera pactado.

En los casos marcados en los cuatro párrafos anteriores, las instituciones tienen que notificar al cliente respectivo la realización de cualquiera de las acciones que hayan llevado a cabo de conformidad con lo previsto en los mismos.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, causará los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, asumirán el mismo valor probatorio.

La disposición y el uso de los equipos y medios señalados en el primer párrafo de este artículo se van a sujetar a las reglas de carácter general que emita la Comisión Nacional Bancaria y de Valores, sin perjuicio de las facultades con que cuenta el Banco de México para regular las operaciones que efectúen las instituciones de crédito relacionadas con los sistemas de pagos y las de transferencias de fondos en términos de su ley.

Las instituciones de crédito podrán intercambiar información en términos de las disposiciones de carácter general a que se refiere el artículo 115 de esta Ley, con la finalidad de robustecer las medidas para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos en contra de su clientela o de la propia institución.

El intercambio de información a que se refiere el párrafo anterior no implicará trasgresión alguna a lo establecido en el artículo 117 de esta Ley. *Artículo reformado DOF 04-06-2001, 01-02-2008*

DENTRO DE LOS DERECHOS PATRIMONIALES OTRO QUE SUFRE INNUMERABLES VULNERACIONES SON LOS LLAMADOS DERECHOS DE AUTOR, un autor tiene todo el derecho de explotar su obra(s), o bien autorizar o prohibir su explotación, o divulgación sin que por esto deje de ser titular de sus derechos, así este puede trasladarlos, transmitirlos o adjudicar las licencias de exclusividad y no exclusividad de uso durante un tiempo determinado y de manera onerosa, o gratuita quedando determinados los

montos, y el procedimiento, así como en qué términos se establecen para el pago de las remuneraciones correspondientes.

Los acuerdos, los convenios y los contratos que se tengan para transmitir los derechos patrimoniales deben constar por escrito y además se beben inscribir en el Registro Público de Derechos de Autor. Y si hubiera alguna ausencia expresa tiene que considerarse la transmisión de los derechos patrimoniales por 5 años. Se podrán celebrar acuerdos por más de 15 años cuando el tipo de obra y la inversión determinada lo justifiquen. Los derechos patrimoniales en sí no pueden ser embargables, aunque si lo puede ser el producto de estos. En cuanto a la vigencia de éste derecho patrimonial lo localizamos estipulado en el dispositivo número 29 de la Ley Federal de Derechos de Autor que a la letra dice:

Artículo 29.- Los derechos patrimoniales estarán vigentes durante:

I. La vida del autor y, a partir de su muerte, cien años más. Cuando la obra le pertenezca a varios coautores los cien años se contarán a partir de la muerte del último, y *Fracción reformada DOF 23-07-2003*

II. Cien años después de divulgadas. *Fracción reformada DOF 23-07-2003*
Si el titular del derecho patrimonial distinto del autor muere sin herederos la facultad de explotar o autorizar la explotación de la obra corresponderá al autor y, a falta de éste, corresponderá al Estado por conducto del Instituto, quien respetará los derechos adquiridos por terceros con anterioridad.

Pasados los términos previstos en las fracciones de este artículo, la obra pasará al dominio público.

La Ley Federal de Derechos de Autor establece una limitación a los derechos patrimoniales, en su artículo 148 y cita:

Artículo 148.- Las obras literarias y artísticas ya divulgadas podrán utilizarse, siempre que no se afecte la explotación normal de la obra, sin autorización del titular del derecho

patrimonial y sin remuneración, citando invariablemente la fuente y sin alterar la obra, sólo en los siguientes casos:

I. Cita de textos, siempre que la cantidad tomada no pueda considerarse como una reproducción simulada y sustancial del contenido de la obra;

II. Reproducción de artículos, fotografías, ilustraciones y comentarios referentes a acontecimientos de actualidad, publicados por la prensa o difundidos por la radio o la televisión, o cualquier otro medio de difusión, si esto no hubiere sido expresamente prohibido por el titular del derecho;

III. Reproducción de partes de la obra, para la crítica e investigación científica, literaria o artística;

IV. Reproducción por una sola vez, y en un sólo ejemplar, de una obra literaria o artística, para uso personal y privado de quien la hace y sin fines de lucro. Las personas morales no podrán valerse de lo dispuesto en esta fracción salvo que se trate de una institución educativa, de investigación, o que no esté dedicada a actividades mercantiles;

V. Reproducción de una sola copia, por parte de un archivo o biblioteca, por razones de seguridad y preservación, y que se encuentre agotada, descatalogada y en peligro de desaparecer;

VI. Reproducción para constancia en un procedimiento judicial o administrativo, y

VII. Reproducción, comunicación y distribución por medio de dibujos, pinturas, fotografías y procedimientos audiovisuales de las obras que sean visibles desde lugares públicos.

Como ya lo observamos se podrán utilizar sin solicitar autorización del titular del derecho patrimonial y sin cubrirle remuneración alguna; pero forzosamente debe citar la fuente y la obra no debe de ser alterada.

Así pueden:

1. Citarse textos no simulados y tampoco sustanciales de una obra;
2. Reproducirse artículos, fotografías, ilustraciones o comentarios, publicados en la prensa, la radio o la televisión, si no lo prohíbe el titular.
3. Reproducirse fragmentos para la crítica y la investigación;
4. Reproducirse un solo ejemplar para uso personal y sin lucro, a excepción de personas morales que no sean instituciones educativas, de investigación o no mercantiles;
5. Reproducirse una sola vez un archivo o biblioteca una obra agotada, descatalogada y en peligro de extinción para preservarla;
6. Reproducirse una obra como constancia en un procedimiento judicial o administrativo y;
7. Reproducirse, comunicarse y distribuirse en lugares públicos una obra mediante dibujos, pinturas, fotografías o audiovisuales.

La persona creadora de una obra digital la cual se encuentra alojada o albergada en Internet tiene todas las prerrogativas y privilegios de carácter patrimonial, por el simple hecho de que la Ley Federal del Derecho de Autor ampara y protege su realización. De esta manera el autor de un contenido digital, como imagen, audio o video texto, tiene todo el derecho para explotar de manera exclusiva su obra, o bien, autorizar a otros individuos su explotación, en cualquier forma, según lo determina el artículo 24, así como: "El derecho de recibir y percibir una regalía por la comunicación o la transmisión pública de su obra por cualquier medio" de acuerdo con el artículo 26 bis y el 27 de la ley en comento que dicen:

Artículo 24.- En virtud del derecho patrimonial, corresponde al autor el derecho de explotar de manera exclusiva sus obras, o de autorizar a otros su explotación, en cualquier forma, dentro de los límites que establece la presente Ley y sin menoscabo de la titularidad de los derechos morales a que se refiere el artículo 21 de la misma.

Artículo 26 bis.- El autor y su causahabiente gozarán del derecho a percibir una regalía por la comunicación o transmisión pública de su obra por cualquier medio. El derecho del autor es irrenunciable.

Esta regalía será pagada directamente por quien realice la comunicación o transmisión pública de las obras directamente al autor, o a la sociedad de gestión colectiva que los represente, con sujeción a lo previsto por los Artículos 200 y 202 Fracciones V y VI de la Ley.

El importe de las regalías deberán pactarse directamente entre el autor, o en su caso, la Sociedad de Gestión Colectiva que corresponda y las personas que realicen la comunicación o transmisión pública de las obras en términos del Artículo 27 Fracciones II y III de esta Ley. A falta de convenio el Instituto deberá establecer una tarifa conforme al procedimiento previsto en el Artículo 212 de esta Ley. *Artículo adicionado DOF 23-07-2003*

Artículo 27.- Los titulares de los derechos patrimoniales podrán autorizar o prohibir:

I. La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico, fotográfico u otro similar. *Fracción reformada DOF 23-07-2003*

II. La comunicación pública de su obra a través de cualquiera de las siguientes maneras:

a) La representación, recitación y ejecución pública en el caso de las obras literarias y artísticas;

b) La exhibición pública por cualquier medio o procedimiento, en el caso de obras literarias y artísticas, y

c) El acceso público por medio de la telecomunicación;

III. La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, incluyendo la transmisión o retransmisión de las obras por:

a) Cable;

b) Fibra óptica;

c) Microondas;

d) Vía satélite, o

e) Cualquier otro medio conocido o por conocerse. *Inciso reformado DOF 23-07-2003*

IV. La distribución de la obra, incluyendo la venta u otras formas de transmisión de la propiedad de los soportes materiales que la contengan, así como cualquier forma de transmisión de uso o explotación. Cuando la distribución se lleve a cabo mediante venta, este derecho de oposición se entenderá agotado efectuada la primera venta, salvo en el caso expresamente contemplado en el artículo 104 de esta Ley;

V. La importación al territorio nacional de copias de la obra hechas sin su autorización;

VI. La divulgación de obras derivadas, en cualquiera de sus modalidades, tales como la traducción, adaptación, paráfrasis, arreglos y transformaciones, y

VII. Cualquier utilización pública de la obra salvo en los casos expresamente establecidos en esta Ley.

En el último presupuesto de la protección del bien jurídico del patrimonio, en estos se encuentran la proliferación de las compras telemáticas que permiten en gran medida el aumento también de los casos de **FRAUDES**, se trataría en este caso de la dinámica comisiva que cumpliría todas las exigencias para el delito de Fraude, que tenemos contemplados dentro de nuestros Códigos Sustantivos Penales Federales y locales; ya que es el engaño y "ánimos defraudandi" donde existe un engaño a la persona que compra.

Cuando se trata de las subastas en línea denominadas también on line, también es un fraude cuando utilizan en Internet como herramienta, para obtener un lucro o beneficio económico y la forma más común es utilizando el correo electrónico (E-MAIL), o los sitios WEB, y también las salas de CHAT. Estas subastas tienen como características que son realizadas por hábiles timadores que ofrecen infinidad de productos a postores que envían confiadamente su dinero pero nunca reciben el producto que les es prometido, o bien reciben objetos que no son lo que aparentaban ser. (No las tenemos reguladas en nuestro país).

2.12 SEGURIDAD NACIONAL

Por lo que concierne al concepto mexicano de seguridad nacional, a continuación se expone una serie de términos que nos permitirán expresar ampliamente cuales son las bases de esta materia en nuestro país:

La seguridad nacional surge por primera vez en un documento oficial, que marco las políticas de gobierno, en el plan global de desarrollo 1980-1982, en el cual se exterioriza que la seguridad nacional va a ser una función esencial y vital de las fuerzas armadas, las cuales van a *"Reafirmar y a consolidan la viabilidad de México como un país absolutamente independiente. Intrínsecamente se da una visión conceptual propia a las condiciones de México, como lo es la defensa de la integridad, la*

independencia y la soberanía de nuestra nación se va referir en el mantenimiento toda de la normatividad constitucional y el fortalecimiento de todas las instituciones políticas de México".[69]

En el plan global de desarrollo 1983-1988, el cual fue librado por el Presidente Miguel de la Madrid, la seguridad nacional se interpreto como: *"La herramienta para mantener la condición de libertad, paz y justicia social dentro del marco constitucional México, por principio funda su propia seguridad en la reiteración del derecho y en la práctica de la cooperación internacional y no en la idea de que la seguridad de una nación dependa de la afirmación de su propio poder, a expensas de las otras. En consecuencia convergen en este concepto las acciones en favor de la paz, el respeto a la autodeterminación y el rechazo a la política de bloques y hegemonías".*[70]

La seguridad nacional es considerado como un bien invaluable de nuestra sociedad y se va a concebir como: *"La condición permanente de paz, libertad y justicia social que, dentro del marco del derecho, procuran pueblo y gobierno. Su subsistencia implica el equilibrio dinámico de los intereses de los diversos sectores de la población para el logro de los determinados objetivos nacionales, garantizando en todo momento la integridad territorial y el ejercicio pleno de la soberanía e independencia".*[71]

De igual forma, tendremos que proporcionar una serie de definiciones expresadas en los ámbitos militar y académico, entre las más destacadas podemos mencionar las siguientes:

Para el Colegio de Defensa Nacional el concepto de seguridad nacional comprende lo siguiente:

"Condición permanente de soberanía, libertad, paz y justicia social que dentro de un marco institucional y de derecho procuran en nuestro país los poderes de la federación mediante la acción armónica, coordinada y dinámica de los campos del poder (político, económico, social y militar) con el fin de alcanzar y mantener los objetivos nacionales y preservarlos tanto de las amenazas en el ámbito interno como las procedentes del exterior".[72]

El General Gerardo C. R. Vega va a precisar la seguridad nacional como: *"La condición de pensamiento y acción del estado, por la cual una sociedad organizada, en el entorno del derecho, obtiene y preserva sus objetivos nacionales".*[73]

---

[69] Plan Global de Desarrollo 1980-1982, "*México Talleres Gráficos de la Nación",* México 1980, p 132.
[70] Plan Nacional de Desarrollo 1983-1988, "*México Poder Ejecutivo Federal, Secretaría de Programación y Presupuesto"*, México 1983, pp 58 al 61.
[71] Plan Nacional de Desarrollo 1989-1994, "*El Mercado de Valores",* México, Junio 1 de 1989, p 54.
[72] Plan Nacional de Desarrollo 1995-2000, "*Poder Ejecutivo Federal"*, México 1995, p 8.
[73] General García, Vega Gerardo, "*Seguridad Nacional, Concepto Organización Método"*, México 1988, Inédito, p78.

El Vicealmirante Mario Santos Caamal puntualiza la seguridad nacional como: *"La creación de las condiciones adecuadas para que el estado nacional, a partir de sus valores y apoyándose en sus instituciones se realice de acuerdo con el proyecto de nación"*.[74]

El jurista Manuel M. Moreno indica que: *"La seguridad nacional abarca todos los campos del acontecer social y su encausamiento va encaminado a la afirmación de todo lo que contribuye a consolidar nuestras formas institucionales de existencia, dentro de los márgenes establecidos por la constitución"*. [75]

El concepto completo de la seguridad nacional comprende dos aspectos, uno interno y el otro externo.

En el orden externo, México, se considera como un país con vocación civilista y de inalterable tradición pacifista, quién siempre ha normado su conducta en el campo internacional, por principios fuertes fundados en los ideales de paz y de justicia, apoyados con justificación con la fuerza de la razón.

En cuanto al ámbito interno la seguridad esta cimentada, de manera especial, en la firmeza y estabilidad de todas nuestras instituciones sociales, se encuentran debidamente tuteladas por el orden jurídico emanado directamente de nuestra constitución. *"La acción del estado en este aspecto está enfocada, fundamentalmente, a lograr el desarrollo integral del país dentro de los cauces de justicia social que la propia constitución preconiza"*.[76]

Luis Herrera-Lasso M. Y Guadalupe González G. Nos otorgan una enunciación de lo que es la seguridad nacional como: *"Todo el conjunto de condiciones de aspecto político, económico, militar, social y cultural que son ineludibles para garantizar la soberanía, y la independencia y la promoción de los intereses de la nación, robusteciendo los componentes del proyecto nacional y reduciendo al mínimo las debilidades o inconsistencias que pueden trastocarse en ventanas de vulnerabilidad frente al exterior"*.[77]

Sergio Aguayo reconoce que: *"La seguridad nacional debe ser un concepto amplio que, aun cuando ha recibido muchas formulaciones, tiene como puntos rectores -aunque con diferentes énfasis- la defensa frente a amenazas externas o internas del territorio, de la soberanía y de los valores nacionales (este último aspecto es generalmente traducido por los gobiernos como la preservación del orden establecido). La seguridad nacional se*

---

[74] Vicealmirante Santos, Caamal, "*La Esencia de la Seguridad Nacional*", CESNAV, México 1995, p 34.
[75] Moreno M. Manuel, "*La Seguridad Nacional desde la Perspectiva de la Constitución"*, UNAM-ENEP, Cuadernos de Investigación número 7, México 1987, p 80.
[76] Ídem.
[77] Herrera-lasso, Luis y otro, "*Balance y Perspectiva del uso del concepto de la Seguridad Nacional en el caso de México"*, Editores Siglo XXI, México 1990, p 391.

liga con el concepto de poder nacional y no se reduce a lo militar sino que tiene dimensiones económicas, políticas, sociales, culturales, etc.".[78]

La finalidad fundamental de la Seguridad Nacional es responder por la sobrevivencia de la nación en la comunidad internacional, como un estado libre, soberano e independiente, por lo que se requiere el aseguramiento y el logro de las condiciones primordiales que le permitan al estado ejercer su autodeterminación, así como mantener su integridad nacional y obtener su desarrollo adecuado. En el caso de México, la seguridad nacional va a ser en esencia la tarea que tiene de vigilar, preservar y proteger interna y externamente el orden constitucional, los objetivos nacionales permanentes y coyunturales y la defensa del territorio nacional.

En mi particular punto de vista, la seguridad nacional en México podría entenderse como: "Aquella política que tiene el Estado Nacional, la cual va a ser desplegada por todos y cada uno de sus integrantes bajo las marcadas directrices del gobierno, dedicada a la máxima tarea que es la preservación y conquista de los objetivos nacionales permanentes y coyunturales, con la única finalidad de lograr el máximo bienestar de la colectividad".

No obstante, en México aun no se ha establecido como tal un sistema de seguridad nacional, entendido este como el conjunto organizado y bien estructurado de los diversos recursos, instituciones y componentes de un estado que en forma coordinada, coadyuvada disponen de capacidad para manifestar el poderío nacional que de manera evidente y funcional para facilitar el desarrollo nacional, resguardado de soberanía e independencia. En nuestro país aun no se ha establecido una cultura de la seguridad nacional, que es tan fundamental por lo que en la esfera gubernamental este fenómeno sigue siendo aún incipiente.

No existe un ordenamiento legal específico en materia de seguridad nacional, el cual en la actualidad resultaría muy necesario. El organismo que ostenta la mayor jerarquía, sería el gabinete de seguridad nacional, que depende del poder ejecutivo, instancia de coordinación que es creada por el presidente de la republica, y se encuentra integrado por todos los titulares de las secretarías de gobierno, el de relaciones exteriores, defensa nacional, marina y el de la procuraduría general de la republica, así como cualquier otro funcionario que es designado el titular del poder ejecutivo. Y este organismo examina temas que son de alta prioridad para la

[78] Aguayo, Sergio, "*Chiapas: las Amenazas a la Seguridad Nacional*", Centro Latinoamericano de Estudios Estratégicos A.C, México Junio de 1987, p 6.

nación, y que toman acuerdos y resoluciones sobre cuestiones especificas relacionadas con la materia, además brindara la asesoría adecuada al Presidente de la Republica.

El 1º de diciembre del año 2000 en México, ingreso en funciones la primera administración emanada de un partido de oposición en 70 años, y esa fue la oportunidad tan deseada para que el Presidente Vicente Fox Quezada, a quién después se le dio el título honorario de Licenciado en Derecho, nombrara a Adolfo Aguilar Singer, como su consejero de seguridad nacional, un flamante puesto, pero no tenía un sustento en la estructura ni jurídico ni administrativo. Por lo que se le consideró un supersecretario que no tenía personal a su cargo, ni tenía un marco normativo y carente de funciones específicas, es decir, un todologo de nada. No obstante, es quizá el primer paso que se conoce para la creación de un verdadero sistema de seguridad nacional.

Ahora bien los delitos informáticos si amenazan la Seguridad Nacional cuando estos se difunden en páginas de Internet, instrucciones para cuestiones de Terrorismo, como lo es el Armado de Bombas, en donde se explica ampliamente como elaborarlas incluso con elementos que se pueden conseguir en cualquier lugar y como detonarlos, cuando nos enseñan el manejo de Armas de Fuego, de Granadas, y explosivos; cuando nuestro Estado no ha controlado los contenidos para controlar el Comercio de Armas, que es otro de los grandes problemas que tiene nuestro país y que aumenta a cada instante, como hemos podido esgrimir a lo largo de esta investigación el desarrollo de la red de redes ha perfilado varios campos de posible conflicto debido a la ausencia de leyes suficientemente claras, y el problema no es sólo legislar, sino también el controlar las nuevas tecnologías, se ha visto que el uso de Internet es un sistema por medio del cual se establecen relaciones no sólo con conocidos sino también con desconocidos y éstos pueden ser utilizados como herramientas que enfoquen un cauce distinto, e inclusive que pueda ser utilizado en contra del propio Estado, como lo serían los ataques sufridos a las vías de comunicación para evitar la circulación en las carreteras de vehículos particulares, de elementos policiacos y militares para evitar los operativos conjuntos de inteligencia de la policía y militares, se han descubierto que los delincuentes organizados tienen acceso a las comunicaciones del Estado, poniendo en riesgo la Seguridad Nacional.

La Delincuencia Organizada es de los grandes problemas que tenemos en Nuestro País, y son precisamente ellos quienes tienen el control de las cuestiones de Narcotráfico,

Pornografía tanto de Adultos como Infantil, Extorsiones, y Secuestros; y vemos como estos delincuentes conocen plenamente las nuevas tecnologías tanto informáticas, telemáticas y radio frecuencia para tener un control del territorio nacional, y así poder saber los movimientos de todos los cuerpos policiacos, y militares; es casi para dar vergüenza que estos tipos de delincuentes incluso tienen redes sociales en donde descaradamente presumen sus actos ilícitos.

Si bien el Legislador estableció en nuestro artículo 16 de Nuestra Ley Suprema, mismo que se transcribió en párrafos con antelación, aquéllos casos de la Averiguación previa de los delitos a que se refiere la delincuencia organizada, o durante un proceso respectivo, el Procurador General de la República o del titular de la Unidad Especializada consideren la intervención de comunicaciones privadas, lo solicitaran por escrito al Juez de Distrito, expresando el objeto y la necesidad de la intervención, los indicios que hagan presumir fundadamente los delitos investigados participa algún miembro de la delincuencia organizada, así como los hechos y circunstancias, datos y demás elementos que se pretendan probar.

De especial interés es para el legislador que en todas las solicitudes de intervención se señalen, además la persona o personas que serán investigadas; y la identificación del lugar o lugares en donde se realizaran; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención, y en su caso la identificación de la persona cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención.

Se constituye que podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

En relación con éste tópico, el Cuarto Tribunal Colegiado en Materia Penal del Primer Circuito, determino: *"Que la limitación establecida por el precepto 16 Constitucional en relación con la figura de intervención de comunicaciones privadas, que el bien jurídico de la infracción penal por intervención de comunicaciones privadas cometidas por servidores públicos recae en el interés común, pues la finalidad perseguida con la incursión de la figura de la intervención de comunicaciones privadas previa autorización judicial, fue precisamente la de proteger a la colectividad contra el constante incremento del crimen organizado, de ahí que la lesión por el ilícito en comento recae en la sociedad, convirtiéndose así en el sujeto pasivo de la infracción punitiva, puesto que la salvaguarda de la seguridad y la privacidad de las comunicaciones, como se dijo, encuentran su límite en la satisfacción del interés común de la sociedad, quien es la interesada en que el derecho a la privacidad no sea violable sino sólo en los casos permitidos por la ley"*.[79]

[79] Tesis I.4º.P21P, Semanario Judicial de la Federación y su Gaceta, Novena Época, T XVIII, Julio de dos mil tres, p 1146.

CAPÍTULO 3 TERCERO. ESTUDIO PANORÁMICO DE LOS DELITOS INFORMÁTICOS.

3.1 DERECHO PANORÁMICO ESTATAL

ACCESO ILÍCITO

Se define el acceso ilícito como el acceso deliberado e ilegítimo a la totalidad o a una parte del sistema informático, infringiendo medidas de seguridad con la intención de obtener datos informáticos o con otra pretensión delictiva o, en relación con un sistema informático que esté conectado a otro.

INTERCEPTACIÓN ILÍCITA.

Se tipifica como delito la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos y, que se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

INTERFERENCIA EN LOS DATOS.

La interferencia de datos se define como aquella conducta que despliega una persona de manera deliberada e ilegítima para dañar, borrar, deteriorar, alterar o suprimir datos informáticos.

ABUSO DE DISPOSITIVOS.

Se sanciona a quien de manera deliberada e ilegitima produce, vende, importa, difunde, utiliza u otra forma de puesta a disposición de datos informáticos o con otra pretensión delictiva o, en relación con un sistema informático que esté conectado a otro.

FALSIFICACIÓN INFORMÁTICA.

Se conoce como tal a forma deliberada e ilegítima, de la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

FRAUDE INFORMÁTICO.

En ese contexto se sanciona cualquier introducción, alteración, borrado o supresión de datos informáticos y, cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES.

Se protege aquellas obras literarias y artísticas, así como las interpretaciones y ejecutantes de los fonogramas cuando se cometen infracciones a la propiedad intelectual a escala comercial y por medio de un sistema informático.

NOMBRE DEL ESTADO	LEGISLACIÓN DEL ESTADO	LEGISLACION QUE REGULA LOS DELITOS INFORMÁTICOS EN EL ESTADO
Legislación Penal Para El Estado De Aguascalientes.	**Si la contempla**	**1. Contempla el acceso ilícito** **2. Revelación de Secretos** **3. Violación de correspondencia** **4. El daño informático** **5. Falsificación informática** **6. Fraude informático**

"Se denomina revelación de secretos, al aprovechamiento o difusión que de una persona realice sobre archivos informáticos de uso personal de otra, sin que ésta dé su consentimiento; también a la difusión de la información confidencial obtenida en los términos que marca la Ley de Video Vigilancia del Estado de Aguascalientes".[80] A la revelación de una comunicación reservada que se conozca o se haya recibido por motivo de empleo, cargo o puesto, sin justa causa, con perjuicio de alguien y sin consentimiento de la víctima.

Dentro de ese catálogo se incluye el tipo de *violación de correspondencia*, que consiste en abrir o interceptar en forma dolosa una comunicación escrita, electrónica, magnética, óptica o informática que éste dirigida al inculpado.

Y, encontramos un supuesto penal denominado *el acceso informático indebido*, que contiene dos hipótesis, una consistente en acceder a la información contenida en un aparato para el procesamiento de datos o cualquier dispositivo de almacenamiento de información, sin

[80] Esa ley tiene como finalidad regular la utilización, por parte de los cuerpos de seguridad pública estatal y municipal o, por prestadores de servicio de seguridad privada, de videocámaras para grabar o captar imágenes con o sin sonido en lugares públicos o privados con acceso al público, así como su posterior tratamiento o, bien por otras autoridades en los inmuebles que estén a su disposición.

autorización de su propietario o poseedor legítimo y, la otra, en el caso que se interfiera con el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo.

Contempla el Acceso sin Autorización y Daño Informático, previstos en los artículos 223, 224, 225 y 226.

DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS Y MAGNÉTICOS

CAPÍTULO PRIMERO ACCESO SIN AUTORIZACIÓN

El Acceso sin Autorización consiste en interceptar, interferir, recibir, usar o ingresar por cualquier medio sin la autorización debida o excediendo la que se tenga a un sistema de red de computadoras, un soporte lógico de programas de software o base de datos.

Cuando el Acceso sin Autorización tenga por objeto causar daño u obtener beneficio, se sancionará al responsable con mayores penas.

También se aplicarán las sanciones más altas cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos accesados sin autorización o excediendo la que se tenga.

DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS Y MAGNÉTICOS

DAÑO INFORMATICO

El Daño Informático consiste en la indebida destrucción o deterioro parcial o total de programas, archivos, bases de datos o cualquier otro elemento intangible contenido en sistemas o redes de computadoras, soportes lógicos o cualquier medio magnético.

Cuando el responsable tenga el carácter de técnico especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos dañados.

Cuando el Acceso sin Autorización o el Daño Informático se cometan culposamente se sancionarán también.

La Falsificación Informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento intangible contenido en sistema de redes de computadoras, base de datos, soporte lógico o programas.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma bienes

informáticos falsificados con conocimiento de esta circunstancia.

Cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos falsificados, se aumentaran las penas.

Código Penal Para El Estado De Baja California. { **Si la contempla** {

1. **Revelación de secretos**
2. **Acceso ilícito**
3. **Infracciones de la propiedad intelectual**

En la codificación de ese estado se establece un Título Tercero, denominado **Delitos Contra La Inviolabilidad Del Secreto Y De Los Sistemas Y Equipos De Informática**; dentro del cual se incorporan los siguientes tipos:

Uno, La Revelación del Secreto, que consiste en que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales, se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno; y dicha conducta se sancionará así como la suspensión en el ejercicio de su profesión; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrá prisión y multa.

En dicha legislación se establece que se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente y, será perseguida por querella de la parte afectada o su representante legal.

Dos, otro de los supuestos contenidos en este capítulo tiene que ver con **El Acceso Ilícito a Sistemas y Equipos de Informática**, en donde se sancionan diversas hipótesis; veamos:

Se regula que, se sanciona a quien sin autorización o indebidamente, modifique, destruya o provoque pérdida de información contenidas en sistemas o equipos de informática protegidos

por algún mecanismo de seguridad. También se sanciona a quien sin autorización o indebidamente, copia o acecé a información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, con prisión y multa. En cualquiera de esos casos, la pena se duplicará cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del estado o los municipios y, en caso de que el sujeto activo sea un servidor público se aumentará hasta la mitad más.

Código Penal Para El Estado De Baja California Sur.

- **Si la contempla**
  1. **Violación de correspondencia y de comunicaciones privadas**

En el Código Penal de esta entidad, encontramos en el Capítulo IV, denominado *Violación de Correspondencia y otras Comunicaciones Privadas,* que sanciona la interceptación de cualquier comunicación verbal, gestual, electrónica o de cualquier otro tipo, sin consentimiento de quien la emite o sin autorización del juez federal, con prisión y multa.

Código Penal Del Estado De Campeche.

- **No los contempla**

Código Penal De Coahuila De Zaragoza.

- **Si los contempla**
  1. **Acceso ilícito**
  2. **Interceptación ilícita**
  3. **Interferencia en los datos**
  4. **Abuso de dispositivos**
  5. **Fraude informático**

En él se dedica el capítulo tercero a los delitos contra la seguridad en los medios informáticos, en donde se define que, por sistema informático se debe entender todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento

automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.

Y, se explica que un dato informático o información es toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

"Ya con relación a los tipos penales se establece que se aplicará prisión y multa"[81], a quien sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita, o se apodere de datos o información reservados, contenidos en el mismo.

O, en su defecto con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

Y, si en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema**,** la sanción será de prisión y multa.

Esos supuestos se agravan al incrementarse la pena en una mitad más si el agente actuó con fines de lucro; si el agente accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.

"De igual manera, se establece que se aplicará prisión y multa a quien sin autorización, acceda, por cualquier medio a un sistema informático a la información de una entidad pública a la administración pública estatal o municipal; al poder legislativo y al poder judicial; los organismos o empresas de cualquiera de los poderes del estado, o del municipio, sean desconcentrados o descentralizados; los organismos o empresas de participación mayoritaria o minoritaria estatal o municipal; las organizaciones y sociedades asimiladas a aquellos; los que manejen bienes o recursos económicos públicos estatales o municipales mediante fideicomisos u otras formas jurídicas, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información

[81] Cabe destacar que los dispositivos que conforman este apartado, no hacen referencia a mínimos y máximos de multa, por lo que nos remitimos al artículo 100 del Código Penal de Coahuila en donde se señala que el mínimo de multa para cualquier delito será el equivalente al de diez días multa y que cada año de prisión o fracción que la ley señale como pena de prisión máxima al delito, equivale a 50 días multa.

propios o relacionados con la institución".[82]

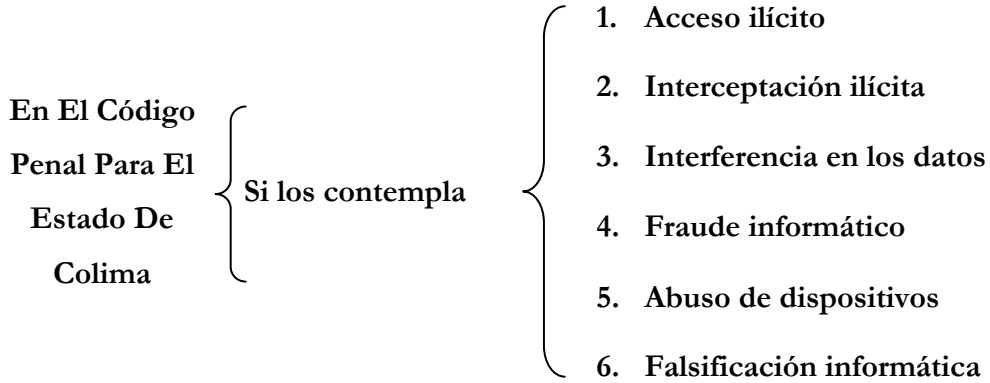
A quien tenga autorización para acceder al sistema informático de una entidad pública de las mencionadas con antelación, indebidamente copie, transmita, imprima, obtenga sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.

Y, si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de prisión y multa.

Además de que, si el sujeto activo del delito es servidor público, se le sancionará, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer.

Dentro de este apartado encontramos que dichas penas se agravaran hasta con una mitad más si el agente atentó contra las políticas y medidas ambientales orientadas a mantener la diversidad genética y la calidad de vida; que no obstante el deber de obtener previamente la constancia o autorización de impacto ambiental, realice obras o actividades sin contar con ella, o no cumpla con las medidas preventivas, condicionantes o correctivas y las demás acciones que le sean requeridas por las autoridades ambientales del Estado o del municipio para llevar a cabo alguna actividad que pudiera afectar el medio ambiente o los recursos naturales de la entidad; con el propósito de obtener un permiso, licencia o autorización de cualquier autoridad ambiental del Estado o del municipio, presente información falsa, o uno o más documentos falsificados o adulterados; con el carácter de perito, laboratorista o prestador de servicios ambientales, proporcione documentos o información falsa u omita datos con el objeto de que las autoridades ambientales del Estado o Municipio, otorguen o avalen cualquier tipo de permiso, autorización o licencia, o valoren el cumplimiento de un deber ambiental; *"si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades públicas ya mencionadas, o por funcionarios o empleados que estén a su servicio y, si la conducta afectó un sistema o dato referente a la salud o seguridad pública o a la prestación de cualquier otro servicio público".* [83] Véase Artículos 281 bis al 281 bis 4

[82] En ese apartado nos remite al artículo 194 bis, del Código Penal de Coahuila.
[83] Este apartado nos remite al artículo 290 bis 1, del Código Penal de Coahuila.



"En el Código Penal de esa entidad, dedica un capítulo a los delitos informáticos, en donde se establece que se le impondrá pena de prisión y multa". [84] Al que de manera dolosa y sin derecho alguno, ni autorización de quien pueda otorgarlo conforme a la Ley, utilice o tenga acceso a una base de datos, sistemas o red de computadoras o a cualquier parte de la misma, con el firme propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información en perjuicio de otro.

De igual forma, la misma sanción del párrafo anterior se impondrá, a quien 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.

También dentro de esa legislación se establece como fraude los siguientes casos:

a) Por el uso indebido de tarjetas o documentos de pago electrónico, esto es al que sin el consentimiento de su titular o de quien esté facultado para ello, haga uso de una tarjeta, título, documento o instrumento de pago electrónico, bien sea para disposición en efectivo o para el pago de bienes y servicios.

Igual pena se impondrá a quien teniendo el consentimiento de su titular o de quien esté facultado para ello, haga un uso indebido de tarjetas, títulos, documentos o instrumentos de

[84] Para efectos de cuantificación de la multa, al importe de un día de salario mínimo general vigente en la región en el momento de la consumación del delito, de la última conducta, en el delito continuado, y en él en que cesó la consumación en el permanente, se le denomina unidad.

pago electrónico, bien sea para el pago de bienes y servicios o para disposición en efectivo.

b) Por el contenido de uso de tarjetas, títulos, documentos o instrumentos para el pago electrónico, falsos; que consiste en que al que a sabiendas de que una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, haga uso de él y obtenga un lucro indebido en perjuicio del titular de la tarjeta, título, documento o instrumento indubitable.

c) Por el acceso indebido a los equipos y sistemas de computo o electromagnéticos, que consiste en que al que con el ánimo de lucro y en perjuicio del titular de una tarjeta, documento o instrumentos para el pago de bienes y servicios o para disposición en efectivo, acceda independientemente a los equipos y servicios de computo o electromagnéticos de las instituciones emisoras de los mismos.

d) Por el uso indebido de información confidencial o reservada de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición en efectivo; es decir, se sanciona a quien obtenga un lucro en perjuicio del titular de una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, mediante la utilización de información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir los mismos.

En ese caso, si el sujeto activo es empleado o dependiente del ofendido, la pena corporal aumentará.

e) También se sanciona al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido.

Y, en el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, la pena se aumentará y en caso de reincidencia aumentara más.

Código Penal Para El Estado De Chiapas. → **Si los contempla**

1. **Fraude informático**
2. **Acceso ilícito**
3. **Interceptación ilícita**
4. **Interferencia en los datos**
5. **Falsificación informática**

"En el código penal de esta entidad, se sanciona como fraude".[85] Al que para obtener algún beneficio para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

Adicional a ello encontramos que, se destina un apartado para regular aquellas conductas que se relacionan con el acceso ilícito a sistemas de informática, dentro del cual encontramos los siguientes supuestos:

I. Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de prisión y de multa.

[85] El artículo 303, del Código Penal para el Estado de Chiapas, establece que el delito de fraude se sancionará:
"I. Con prisión de seis meses a dos años y multa hasta de cien días de salario cuando el valor de lo defraudado no exceda de doscientos días de salario o no sea posible determinar su valor.
II. Con prisión de dos a cinco años y multa de cincuenta a noventa días de salario cuando el valor de lo defraudado fuere mayor de doscientos pero no de mil días de salario.
III. Con prisión de cinco a diez años y multa hasta de ciento ochenta días de salario si el valor de lo defraudado excede de mil días de salario."

Y, en caso de estar autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentará en una mitad.

II. Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de prisión y de multa.

III. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información que contengan se impondrá prisión y multa.

IV. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá prisión y multa.

Adicionando que esos delitos serán sancionados por querella de parte ofendida.

Confróntese Del artículo 284 ter al 284 octer

Código Penal Del Estado De Chihuahua. → **Si los contempla**

1. **Robo**
2. **Fraude informático**
3. **Interceptación ilícita**
4. **Interferencia en los datos**

"Dentro de este cuerpo legamos encontramos que se sanciona como Robo".[86] Cuando el apoderamiento recaiga en un expediente, documento o en cualquier información que se encuentre registrada o archivada en sistema o equipo de informática protegidos por algún mecanismo de seguridad, con afectación de alguna función pública.

"También se considera como Fraude, cuando alguien alcance un lucro indebido para sí o para otro, valiéndose de alguna manipulación informática, alteración de programas sistematizados, del empleo no autorizado de datos o artificio semejante, se le impondrá la punibilidad señalada para el delito de fraude".[87]

También dentro del apartado del delito de Daños, encontramos que se aplicará 6 meses a 6 años al que destruya, altere o provoque pérdida de información contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad.

Podrá aumentarse la pena señalada hasta el doble, según la gravedad del daño que resulte, si no puede reponerse el expediente, la información a que se refiere el párrafo anterior, ni suplirse la falta del documento.

[86] Este ilícito se sanciona de la siguiente manera:
"Artículo 208. A quien con ánimo de dominio y sin consentimiento de quien legalmente pueda otorgarlo, se apodere de una cosa mueble ajena, se le impondrá:
I. Cuando el valor de lo robado no exceda de quinientas veces el salario, se impondrán de seis meses a dos años de prisión y multa de treinta a cien veces el salario.
II. Cuando exceda de quinientas veces el salario, pero no de mil, la sanción será de dos a cuatro años de prisión y multa de cien a doscientas veces el salario.
lII. Cuando exceda de mil veces el salario, la sanción será de cuatro a diez años de prisión y multa de doscientas a quinientas veces el salario.
Para estimar la cuantía del robo se atenderá al valor comercial de la cosa robada, al momento del apoderamiento, pero si por alguna circunstancia no fuera estimable en dinero o si por su naturaleza no fuera posible fijar su valor, se aplicarán de seis meses a cinco años de prisión y multa de treinta a ochenta veces el salario.
En los casos de tentativa de robo, cuando no fuera posible determinar el monto, la pena será de seis meses a dos años de prisión."

[87] En estos casos se sanciona de conformidad con el artículo siguiente:
"Artículo 225. A quien por medio del engaño o aprovechando el error en que otro se halle le cause perjuicio patrimonial, se le impondrán de seis meses a dos años seis meses de prisión y de setenta y cinco a doscientos días multa."

Código Penal Para El Distrito Federal. → **Si los contempla** → **1. Fraude informático**

"En esta legislación se tipifica como fraude".[88] Aquella conducta en que para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.

Código Penal Para El Estado Libre Y Soberano De Durango. → **Si los contempla** →

1. **Fraude informático**
2. **Acceso ilícito**
3. **Interceptación ilícita**
4. **Interferencia en los datos**

"Dentro del Capítulo IV, intitulado Fraude y Exacción Fraudulenta, sanciona como Fraude a quien para obtener algún lucro para sí o un tercero, por cualquier accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores en perjuicio de persona alguna, independientemente de que los recursos no salgan de la institución".[89]

---

[88] En el artículo 230 del Código Penal para el Distrito Federal, señala que el delito de fraude se va a sancionar de la siguiente manera:
"I. De veinticinco a setenta y cinco días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el salario mínimo, o no sea posible determinar su valor;
II. Prisión de cuatro meses a dos años seis meses y de setenta y cinco a doscientos días multa, cuando el valor de lo defraudado exceda de cincuenta pero no de quinientas veces el salario mínimo;
III. Prisión de dos años seis meses a cuatro años y de doscientos a quinientos días multa, cuando el valor de lo defraudado exceda de quinientas pero no de cinco mil veces el salario mínimo;
IV. Prisión de cuatro a seis años y de quinientos a ochocientos días multa, cuando el valor de lo defraudado exceda de cinco mil pero no de diez mil veces el salario mínimo; y
V. Prisión de seis a once años y de ochocientos a mil doscientos días multa, cuando el valor de lo defraudado exceda de diez mil veces el salario mínimo.
Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores."

[89] El catálogo de delitos que se contienen en los numerales 210 y 211, que es donde se incluye el tipo que nos ocupa, se sanciona en los siguientes términos:
"Artículo 212. A quienes cometan el delito de fraude se les impondrán las penas siguientes:
I. De seis meses a dos años de prisión o multa de treinta y seis a ciento cuarenta y cuatro días de salario, cuando el valor de lo defraudado no exceda de quince veces el salario mínimo;

Por otro lado, dentro de esta legislación encontramos un apartado denominado "Delitos contra la Seguridad de los Medios Informáticos", en donde se señala que se aplicará prisión y multa:

l. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita o se apodere de datos o información reservados, contenidos en el mismo; o,

II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

III. Si la conducta que en uno u otro caso se realice es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de prisión y multa y días de salario.

Penas que se incrementarán en una mitad más:

a) Si el sujeto activo actuó con fines de lucro; o,

b) Si el sujeto activo accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.

IV. Se aplicará prisión y multa en salarios, al que:

a) Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad pública, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución; o,

b) Con autorización para acceder al sistema informático de una entidad pública indebidamente copie, transmita, imprima, obtenga, sustraiga, utilice divulgue o se apropie de datos o

---

II. De uno a cuatro años de prisión o multa de setenta y dos a doscientos ochenta y ocho días de salario, cuando el valor de lo defraudado exceda de quince, pero no de noventa veces el salario mínimo;
III. De dos a seis años de prisión y multa de ciento cuarenta y cuatro a cuatrocientos treinta y dos días de salario, cuando el valor de lo defraudado exceda de noventa, pero no de seiscientas veces el salario mínimo;
IV. De cuatro a ocho años de prisión y multa de doscientos ochenta y ocho a quinientos setenta y seis días de salario, cuando el valor de lo defraudado exceda de seiscientos, pero no de tres mil quinientas veces el salario mínimo; y,
V. De seis a doce años de prisión y multa de cuatrocientos treinta dos a ochocientos sesenta y cuatro días de salario, cuando el valor de lo defraudado exceda de tres mil quinientas veces el salario mínimo".

información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de prisión y multa.

Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro.

Penas que se incrementarán en una mitad más:

I. Si el sujeto activo obró valiéndose de alguna de las circunstancias agravantes es decir con fines de lucro o, accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.

II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades públicas o por funcionarios o empleados que estén a su servicio; y,

III. Si la conducta afectó un sistema o dato referente a la salud, administración de justicia, procuración de justicia, seguridad pública o a la prestación de cualquier otro servicio público.

En ese contexto se explica que por sistema informático debemos entender todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio; y,

Dato informático o información es toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

Código Penal Para El Estado De Guanajuato. → **Si los contempla** →
1. **Violación de correspondencia**
2. **Acceso ilícito**
3. **Interferencia en los datos**

TÍTULO TERCERO DE LOS DELITOS CONTRA LAS VÍAS DE COMUNICACIÓN DE USO PÚBLICO Y VIOLACIÓN DE CORRESPONDENCIA

CAPÍTULO II VIOLACIÓN DE CORRESPONDENCIA

Se aplicará prisión y multa, a quien indebidamente:

I.- Abra, intercepte o retenga una comunicación que no le esté dirigida.

II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.

No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.

Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

Código Penal Del Estado De Guerrero. { **Si los contempla** { **1. Robo** **2. Interceptación ilícita** **3. Abuso de dispositivos**

"En esta legislación se sanciona dentro del delito de Robo, a quien aprovechando energía eléctrica, o algún fluido, programas computarizados, señales televisivas o de Internet, sin consentimiento de la persona que legalmente pueda disponer y autorizar de aquéllas". [90]

Código Penal Para El Estado De Hidalgo. { **No los contempla**

[90] En este apartado se hace referencia que se sanciona como tal, con las siguientes penas:
"163.- Al que se apodere de una cosa mueble ajena, con ánimo de dominio, sin consentimiento de quien pueda otorgarlo conforme a la ley, se le aplicarán las siguientes penas: I.- De uno a dos años de prisión y de sesenta a cien días multa, cuando el valor de lo robado no exceda de cien veces el salario; II.- De dos a cinco años de prisión y de ciento veinte a cuatrocientos días multa, cuando el valor de lo robado exceda de cien pero no de quinientas veces el salario, y III.- De cinco a once años de prisión y de trescientos a quinientos días multa, cuando el valor de lo robado exceda de quinientas veces el salario."

Código Penal Para El Estado Libre Y Soberano De Jalisco. — **Si los contempla**

1. **Acceso ilícito**
2. **Falsificación informática**
3. **Infracciones de la propiedad intelectual**
4. **Fraude informático**
5. **Abuso de dispositivos**
6. **Interceptación ilícita**

Dentro de ese ordenamiento legal se destina un capítulo denominado "La Obtención Ilícita de Información Electrónica", en donde se sanciona con prisión a quien sin autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática.

Sanciones que se incrementan en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

También, dentro del Título Noveno, intitulado "Falsedad", se incorpora un apartado que llaman "Falsificación de Medios Electrónicos o Magnéticos", en donde se sancionará con prisión y multa por el equivalente a los salario mínimo general vigente en la época y área geográfica en que se cometa el delito a quien, sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique, aún gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, boletos, contraseñas, fichas, tarjetas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal.

II. Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo.

III. Acceda, obtenga, posea o detente indebidamente información de los equipos

electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I y los destine a alguno de los supuestos que contempla el presente artículo.

IV. Adquiera, utilice, posea o detente equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I.

V. Las mismas penas se impondrán a quien utilice o revele indebidamente información confidencial o reservada de la persona física o jurídica que legalmente esté facultada para emitir los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I, con el propósito de realizar operaciones ilícitas y no autorizadas por la persona emisora, o bien, por los titulares de los boletos, contraseñas, fichas u otros documentos a los que se refiere este artículo.

Explicando que si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.

Véase Artículo 170 bis

Código Penal Del Estado De México. → **No los contempla**

Código Penal Del Estado De Michoacán. → **Si los contempla**

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**

En el artículo 133 ter, de éste código, se sanciona con prisión y multa en salarios mínimos generales vigentes, a quien dolosamente:

I. Ingrese a los bancos de datos del Sistema previstos en la Ley del Sistema de Seguridad Pública del Estado de Michoacán de Ocampo, información errónea, que dañe o que pretenda dañar en cualquier forma los registros, los bancos de datos o los equipos o sistemas que las

contengan.

II. Divulgue información clasificada de los bancos de datos o sistemas informáticos a que se refiere la Ley mencionada en la fracción anterior.

III. Inscriba o registre en los bancos de datos del personal de las instituciones de Seguridad Pública, prevista en la Ley del Sistema de Seguridad Pública del Estado de Michoacán de Ocampo, como miembro o integrante de una institución de Seguridad Pública de cualquier orden de Gobierno, a persona que no cuente con la certificación exigible conforme a la mencionada Ley.

Adicionando que, si el sujeto infractor es o hubiese sido servidor público de las instituciones de Seguridad Pública, se aumentará hasta una mitad más de la pena correspondiente, además, la inhabilitación por un plazo igual al de la pena de prisión impuesta para desempeñarse como servidor público en cualquier orden de Gobierno, y en su caso, la destitución.

Código Penal Para El Estado De Morelos. → **No los contempla**

Código Penal Para El Estado De Nayarit. → **No los contempla**

Código Penal Para El Estado De Nuevo León. → **Si los contempla**

1. **Robo**
2. **Acceso ilícito**
3. **Intercepción ilícita**
4. **Interferencia en los datos**
5. **Abuso de dispositivos**
6. **Falsificación informática**

"En este código se sanciona como Falsedad en Declaraciones y en Informes Dados a una Autoridad, a quien proporcione datos o información a una autoridad pública en ejercicio de sus funciones, utilizando internet o cualquier otro medio de comunicación telefónico o electrónico, afirmando una falsedad o negando la verdad en todo o en parte. A los responsables de ese delito se les sancionará con prisión y multa".[91]

"Dentro de este ordenamiento legal, se establece que se equipara al Robo y se castiga como tal, a quien se apodere materialmente o vía electrónica de los documentos que contengan datos en computadoras o, el aprovechamiento o utilización de esos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos".[92]

También se incorpora un capítulo donde se regulan los delitos por medios electrónicos, sancionándose las conductas que enseguida enunciamos:

I. A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado

[91] En los artículos 50 y 79, de éste código se establece que la multa consiste en pagar al estado la suma pecuniaria que se fije en la sentencia y, para ello, el juzgador deberá tomar en consideración la capacitad económica del sentenciado y, se específica que para fijar el término de la sanción se parte del monto de lo obtenido de acuerdo al valor de reposición o mercado de la cosa, según sea el caso, fijado por peritos, por la comisión del delito o daño causado, atendiendo a las cuotas fijadas por el código.
Explicando que se entiende por cuota el importe del salario mínimo general más bajo, de los que rijan en el estado en el momento de la comisión del delito y, que en las resoluciones basadas en factores de carácter económico que dicten los jueces se tendrá en cuenta el concepto de cuota, cuando sea factible.

[92] Por disposición del artículo 365, fracción IV, que es donde se regula el delito en cita, se atenderá a lo dispuesto en el numeral 367 ambos de ese código, por lo que el delito de Robo simple se sancionará en la forma siguiente:
"I.- Cuando el valor de lo robado no exceda de doscientas cuotas, se impondrán de seis meses a tres años de prisión y multa de cuarenta a cien cuotas.
II.- Si se excede de doscientas pero no de setecientas cuotas, la pena será de dos a seis años de prisión y multa de cien a doscientas cincuenta cuotas.
III.- cuando pase de setecientas cuotas, la sanción será de cinco a quince años de prisión y multa de doscientas cincuenta a quinientas cuotas.
IV.- Se sancionará con pena de dos a siete años de prisión y multa de mil a mil quinientas cuotas en los supuestos contenidos en el artículo 365 fracciones IV y VI de este código.
Para estimar la cuantía del robo se atenderá al valor de reposición de la cosa, misma que no será indispensable tener a vista para determinarlo.
Si por su naturaleza, particularidades o singularidad de la cosa robada no es posible estimar su valor de reposición, se atenderá a su valor de mercado."
Y, se adiciona en el numeral 369 que:
"Cuando la cosa materia de apoderamiento no fuere estimable en dinero, si por su naturaleza no se puede fijar su valor o cantidad, o si por cualquier circunstancia no se pudiere valorizar, se aplicaran de uno a siete años de prisión. Bastara que un solo objeto robado se cuantifique por un monto que corresponda a una sanción superior a la señalada en este articulo, para determinar la aplicación de la prevista por su valor".

de datos, se le impondrá prisión y multa.

II. A quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos, se le impondrá prisión y multa.

III. A quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos, se les impondrá prisión y multa.

DELITOS POR MEDIOS ELECTRÓNICOS

A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos, se le impondrá prisión y multa.

A quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos, se le impondrá prisión y multa.

A quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos, se les impondrá prisión y multa.

Código Penal Para El Estado Libre Y Soberano De Oaxaca.	**No los contempla**
Código De Defensa Social Para El Estado Libre Y Soberano De Puebla.	**No los contempla**

Código Penal Para El Estado De Querétaro. — **Si los contempla**

1. **Falsificación informática**
2. **Acceso ilícito**
3. **Fraude informático**
4. **Abuso de dispositivos**
5. **Interceptación en los datos**
6. **Interferencia en los datos**

Se sanciona como Falsificación y Uso Indebido de Documentos, al que sin consentimiento de quien esté facultado para ello:

a) Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas o boletos, contraseñas, fichas, tarjetas de crédito o débito y otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consignan u obtener cualquier beneficio.

b) Acceda, obtenga, posea, utilice o detente indebidamente información de los equipos electromagnéticos, de módem o cualquier medio de comunicación remota o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas o boletos, contraseñas, fichas, tarjetas de crédito o débito y otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consignan u obtener cualquier beneficio.

c) Adquiera, utilice o detente equipos electromagnéticos, electrónicos o de comunicación remota para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas, tarjetas de crédito, tarjetas de débito u otros documentos a los que se refiere este artículo o de archivos de datos de las emisoras de los documentos.

Las mismas penas se impondrán a quién utilice o revele indebidamente información confidencial o reservada de la persona física o jurídica que legalmente esté facultada para emitir los boletos, contraseñas, fichas u otros documentos a los que se refiere las hipótesis anteriores, con el propósito de obtener beneficio aunque no sea económico y no autorizadas por la persona emisora, o bien, por los titulares de los boletos, contraseñas, fichas u otros

documentos a los que nos hemos referidos

Si el sujeto activo es empleado, dependiente del ofendido o servidor público las penas se aumentaran en una mitad y, en el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso.

Y, cuando alguno de los delitos previstos en este capítulo sea ejecutado por un servidor público en ejercicio de sus funciones, será penado, además, con privación del empleo e inhabilitación para ocupar otro cargo público hasta por 3 años.

De igual manera, dentro de este código se encuentra un apartado en donde se sanciona el acceso ilícito a sistemas de informática; dentro del cual se sancionan las siguientes conductas:

I. Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad, se le impondrán prisión y multa.

II. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos o no por algún sistema de seguridad, se le impondrán prisión y multa.

Las penas señaladas en el párrafo anterior se aplicarán a aquellos que teniendo autorización para ingresar al sistema informático, hagan uso indebido de la información, para sí o para otro.

III. Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado, protegidos o no por algún sistema de seguridad, se le impondrán prisión y multa.

IV. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos o no por algún medio de seguridad, se le impondrán prisión y multa.

V. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido o no por algún medio de seguridad, se le impondrá pena de prisión y multa. Si el

responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de 4 a 10 años para desempeñarse en cualquier empleo, puesto, cargo o comisión de carácter público.

Código Penal Para El Estado Libre Y Soberano De Quintana Roo. → **Si los contempla**

1. **Falsificación informática**
2. **Fraude informático**
3. **Infracciones a la propiedad intelectual**
4. **Acceso ilícito**
5. **Abuso de dispositivos**

"Dentro del catálogo de delitos contenidos en el apartado denominado Falsificación de Documentos y Uso de Documentos Falsos",[93] sanciona las siguientes conductas:

a) A quien copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo.

b) Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Adicionando que, si el sujeto activo es empleo o dependiente del ofendido, las penas se aumentarán hasta en una mitad más y, en el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso.

[93] En los numerales 189 y 189 bis, de éste código, se establece que se impondrá prisión de 6 meses a 3 años y de 15 a 90 días multa; las que se incrementaran hasta una mitad más; a quien incurra en cualquiera de las conductas que describimos.

Código Penal Del Estado De San Luis Potosí. → **Si la contempla** → **1. Robo**

"En esta codificación se equipara al Robo, el apoderamiento material de documentos, datos o información contenidos en computadoras o, el aprovechamiento o utilización de esos datos, sin derecho y sin el consentimiento de la persona que legalmente pueda disponer de los mismos".[94]

Código Penal Para El Estado De Sinaloa. → **Si los contempla** →
1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**

Dentro de esta legislación encontramos un capítulo destinado al delito informático en su numeral 217 y, señala que lo comete la persona que dolosamente y sin derecho:

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

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

[94] En el artículo 197 de ese código, se establece que el Robo se sanciona con las siguientes penas:
"I. Cuando el valor de lo robado no exceda de noventa veces el salario mínimo, se impondrá una pena de seis meses a dos años de prisión y sanción pecuniaria de cincuenta a doscientos días de salario mínimo;
II. Cuando el valor de lo robado exceda de noventa veces el salario mínimo, pero no de ciento cincuenta, se impondrá una pena de uno a tres años de prisión y sanción pecuniaria de cien a trescientos días de salario mínimo;
III. Cuando el valor de lo robado exceda de ciento cincuenta veces el salario mínimo, pero no de quinientas, se impondrá una pena de tres a cinco años de prisión y sanción pecuniaria de trescientos a quinientos días de salario mínimo;
IV. Cuando el valor de lo robado exceda de quinientas veces el salario mínimo, pero no de un mil quinientas, se impondrá una pena de cuatro a ocho años de prisión y sanción pecuniaria de cuatrocientos a ochocientos días de salario mínimo, y
V. Cuando el valor de lo robado exceda de un mil quinientas veces el salario mínimo, se impondrá una pena de cinco a diez años de prisión y sanción pecuniaria de quinientos a un mil días de salario mínimo".

Al responsable éste delito se le impondrá una pena de prisión y de multa.

Código Penal Del Estado De Sonora. → **No los contempla**

Código Penal Del Estado De Tabasco. → **Si los contempla**

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**

Del análisis de este código encontramos un apartado destinado a los delitos contra la seguridad de los medios informáticos y magnéticos; dentro del cual encontramos clasificadas varias conductas y, que enseguida enunciamos:

I. Acceso sin autorización. Se sanciona al que intercepte, interfiera, reciba, use o ingrese por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal, o a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos, con prisión y días multa.

II. Daño informático. Se pune a quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético, se le sancionará con penas de prisión y de días multa.

Si el sujeto activo tiene el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más.

III. Falsificación informática, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este Título

Cuando esos ilícitos se cometan utilizando el equipo de cómputo de terceras personas, las penas se incrementarán en una mitad.

Código Penal Para El Estado De Tamaulipas. → **Si los contempla**

1. **Robo**
2. **Acceso ilícito**
3. **Interceptación ilícita**
4. **Interferencia en los datos**
5. **Abuso de dispositivos**
6. **Falsificación informática**

"Dentro de esa legislación encontramos que se sanciona como Robo, a quien se apodere materialmente de los documentos que contengan datos de computadoras o el aprovechamiento o utilización de dichos datos, sin consentimiento de la persona que legalmente pueda disponer de los mismos".[95]

Más adelante, se incorpora un apartado especializado en delitos que sancionan el acceso ilícito a sistemas y equipo de informática; dentro del cual se contemplan las siguientes hipótesis:

I. Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a él. En ese caso se impondrá una sanción de prisión y multa en días

[95] Dicho ilícito se sanciona bajo las reglas contenidas en el código en los siguientes términos:
"ARTICULO **402.-** El delito de robo simple se sancionará en la forma siguiente:
I**.-** Cuando el valor de lo robado no exceda de cien días de salario, se impondrá una sanción de dos meses a dos años de prisión y multa de cinco a cuarenta días salario;
II**.-** Si excede de cien, pero no de doscientos días salario, la pena será de dos a seis años de prisión y multa de cuarenta a ochenta días salario; y
III**.-** Cuando excediere de doscientos días salario, la sanción será de seis a doce años de prisión y multa de ochenta a ciento cuarenta días salario.
ARTÍCULO **403.-** Para estimar la cuantía del robo se atenderá al valor intrínseco de la cosa robada en el momento de su consumación. Si no fuere estimable en dinero, si por su naturaleza no se puede fijar su valor, o cantidad, o si por cualquier circunstancia no se haya valorizado, se aplicarán de seis meses a cinco años de prisión. Igualmente se atenderá al valor intrínseco de la cosa que se intentó robar en el momento del último acto tendiente a la ejecución; en los casos de tentativa de robo, cuando no se pueda determinar su monto se aplicarán de seis meses a dos años de prisión".

salario.

II. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo; aquí se le impondrá al sujeto infractor una sanción de prisión y multa en días de salario.

III. Al que sin autorización conozca o copié información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo; en ese supuesto se le impondrá al sujeto activo una sanción de prisión y multa en días salario.

IV. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan; en ese caso se impondrá al sujeto infractor, una sanción de prisión y multa de días salario.

V. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá prisión y multa de días salario.

Esas hipótesis serán sancionadas por querella de la parte ofendida.

DELITOS COMETIDOS POR SERVIDORES PÚBLICOS
ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Al que sin autorización modifique, destruya, o provoque perdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a él, se le impondrá una sanción de prisión y multa de días salario.

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistema o equipo de informática de alguna dependencia publica, protegida por algún mecanismo se le impondrá una sanción de prisión y multa de días salario.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia publica, protegida por algún mecanismo se le impondrá una sanción de prisión y multa de días salario.

Al que estando autorizado para acceder a sistemas y equipos de informática de alguna

dependencia publica, indebidamente modifique, destruye o provoque perdida de información que contengan se impondrá una sanción de prisión y multa de días salario.

Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia publica, indebidamente copie, transmita o imprima información que contengan se le impondrá prisión y multa de días salario.

Los delitos previstos en este TÍTULO serán sancionados por querella de la parte ofendida.

Para los efectos de este TÍTULO y el subsecuente se considera servidor público toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza para:

I. Los tres poderes del estado;

II. Los ayuntamientos de los municipios del estado;

III. Los organismos descentralizados de las entidades referidas en las dos fracciones que anteceden.

Se impondrán las mismas sanciones previstas para el delito de que se trate a cualquier persona que participe en la perpetración de alguno de los delitos previstos en este TÍTULO o el subsecuente.

Véase artículo 207 al 208

Código Penal Para El Estado Libre y Soberano de Tlaxcala. → **No los contempla**

Código Penal Para El Estado Libre Y Soberano De Veracruz De Ignacio De La Llave. → **Si los contempla**

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Fraude informático**

En este cuerpo legal se destina un capítulo a los delitos informáticos, en donde se sanciona a quien, sin derecho y con perjuicio de tercero:

I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o

II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable se le impondrán prisión y multa de días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad.

DELITOS CONTRA LA INTIMIDAD PERSONAL Y LA INVIOLABILIDAD DEL SECRETO

DELITOS INFORMÁTICOS

Artículo 181.-Comete delito informático quien, sin derecho y con perjuicio de tercero:
I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementaran en una mitad.

Código Penal Del Estado De Yucatán. → **Si los contempla**

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Robo**
7. **Fraude informático**

Dentro de este código encontramos que sanciona como falsificación de documentos en general, al que:

I. Acceda indebidamente a los equipos de electrónicos de las instituciones emisoras de tarjetas bancarias o comerciales y vales para el pago de bienes o servicios o para disposición de efectivo, con el fin de utilizarlos u obtener información con fines indebidos.

II. Al que sin causa legal adquiera, utilice o posea equipos electromagnéticos que sirvan para sustentar la información contenida en la cinta o banda magnética de tarjetas bancarias o comerciales, títulos o documentos para el pago de bienes y servicios o disposición de efectivo, así como a quien posea o utilice indebidamente la información sustraída en esta forma.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas bancarias o comerciales y vales utilizados para el pago de bienes y servicios y, si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

En el caso de que se actualicen otros delitos con motivo de las conductas a las que nos referimos, se aplicarán las reglas del concurso.

Código Penal Del Estado De Zacatecas.	**No los contempla**

Lo anterior nos arroja que 11 entidades federativas no se contemplan ninguna hipótesis que involucre los delitos informáticos y que son materia de este trabajo.

No dejamos de lado que, en todas las legislaciones se sancionan aquellas conductas que involucra el empleo del internet o uso de equipos de computadora en la comisión de delitos como Pornografía Infantil, Secuestro, Fraude, entre otros, pero no propiamente nos encontramos en presencia de un delito de esa naturaleza.

Michoacán se encuentra dentro de este grupo de entidades, en las que incluso se sanciona aquellas conductas relacionadas con los ciber-delitos, siempre y cuando atente contra el sistema de seguridad local, dejando si regulación cuando el afectado sea un particular.

Es de llamar la atención que en otras entidades federativas, los delitos informáticos se regulan dentro de los apartados como violación de correspondencia, falsificación de documentos, delitos que atenten contra la intimidad, robo, fraude o algún otro similar y, sólo en tres de ellas se contienen en dos o más delitos (ejemplo Robo y Delito informático).

Y, un dato más para la reflexión es el hecho de que las sanciones para estos tipos de ilícitos son bajas; por tanto, ello nos lleva a plantear que dada la gravedad y el daño social que se causa con ese tipo de conductas, las penas deben ser más severas.

3.2 DERECHO PANORÁMICO EN AMÉRICA SOBRE LOS DELITOS INFORMÁTICOS

Una de las preocupaciones que ha expresado la Organización de Estados Americanos es la alza en los delitos cibernéticos; razón por la cual a través del Departamento de Cooperación Jurídica se han generado las estrategias y un frente común entre los países miembros para combatirlos y ajustar las legislaciones locales a las necesidades imperantes.

En ese contexto se han clasificado esa clase de ilícitos, en la parte sustantiva, en acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos, falsificación informática, fraude informático e infracciones de la propiedad intelectual y de los derechos afines; apoyados en el Convenio del Consejo de Europa sobre la Delincuencia Cibernética.

Y, en al ámbito procesal, se han abordado aspectos como la conservación rápida de los datos informáticos almacenados, conservación y revelación parcial rápida de datos sobre el tráfico, orden de presentación, registro y confiscación de datos informáticos almacenados, obtención en tiempo real de datos sobre el tráfico e interceptación de datos sobre el contenido.

Sobre esas mismas bases nos ocuparemos en este capítulo del análisis de algunas relaciones legislaciones vigentes en América Latina que contemplan.

ARGENTINA

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Fraude informático**
7. **Infracciones de la propiedad intelectual**

Se sanciona como tal en los artículos 153 y 157 del Código Penal; ya que en el primero se dispone que el infractor será reprimido con prisión de 15 días a 6 meses (siempre y cuando no hubiese concurso de delitos), al que a sabiendas accediere por cualquier medio y sin la debida autorización o excediendo la que posee a un sistema o dato informático de acceso restringido y, con 1 mes a un 1 año de prisión, si ese acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

En el segundo dispositivo en cita, se dispone que será reprimido con prisión de 1 mes a 2 años e inhabilitación especial de 1 a 4 años, al funcionario público que revele hechos, actuaciones, documentos o datos que por ley deban ser secretos.

En Argentina se contempla en el artículo 153 del Código Penal y, se sanciona con 15 días a 6 meses de prisión, a quien abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de

acceso restringido.

Agregando que la pena se incrementa de 1 mes a 1 año de prisión, si el autor comunicara a otro o publicase el contenido de la comunicación electrónica y, en caso de que el sujeto activo fuese funcionario, se le inhabilitara por el doble del tiempo de la condena.

La interferencia en datos en Argentina se regula en los numerales 183 y 184 del Código Penal; en el primer dispositivo se establece que será reprimido con prisión de quince días a un año, el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008).

Y, en el segundo dispositivo, se establece que la pena será de tres meses a cuatro años de prisión, si fuere ejecutado en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

"El abuso de dispositivos en Argentina, lo encontramos en el artículo 183 del Código Penal, en donde se lee que será reprimido con prisión de quince días a un año, el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".[96]

"La falsificación informática lo encontramos en el Código Penal de Argentina, en el artículo 157 bis".[97] En donde se lee que será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente o, violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

[96] Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008.

[97] Artículo sustituido por art. 8° de la Ley N° 26.388, B.O. 25/6/2008.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

El fraude informático lo, encontramos en el Código Penal de Argentina, se contiene en los numerales 172 y 173, estableciendo en el primero de ellos que, será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

"Y, en segundo dispositivo se señala que se impondrá la misma pena al que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.[98] *"Y, al que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".*[99]

Las infracciones de la propiedad intelectual lo encontramos en la Ley de la Propiedad Intelectual (11.723), de Argentina, en el artículo 71, en donde se dispone que sería reprimido con prisión de un mes a seis años, al que de cualquier manera y en cualquier forma defraude los derechos de propiedad que se reconoce en esa ley.

BAHAMAS

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Fraude informático**

[98] Inciso incorporado por art. 1° de la Ley N° 25.930 B.O. 21/9/2004.

[99] Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008

Se regula en la Ley de Informática, en las secciones 3, 4 al 6, de la siguiente manera: queda sujeto a esos disposiciones la persona que a sabiendas de que carece de autorización ingrese a cualquier programa o datos contenidos en cualquier ordenador y, será sancionado en juicio sumario con una multa que no exceda de cinco mil dólares o reclusión por un término que no será superior a 6 meses o, ambas; en caso de reincidencia, la multa no será superior a diez mil dólares o, encarcelamiento no superior de 1 año, o ambos.

Si se advierte que se causó algún daño en el equipo o la información, el infractor será castigado con una multa que no exceda de veinte mil dórales o, prisión por un período no superior a los 3 años, o ambas.

De igual manera, se sancionada a la persona que ingrese a una computadora con la intención de cometer algún delito (ya sea por sí o por un tercero; generalmente, se explica dentro de ese apartado que se aplica en los delitos relacionados con la propiedad, fraude, deshonestidad o que cause daño físico y que se castiga en caso de condena con prisión de un término no menor de dos años.

En este supuesto el infractor es sometido a juicio sumario y las sanciones van de una multa no superior a diez mil dólares o prisión por un período no superior a 3 años, o ambos.

Y, dentro de este apartado se dispone que se sanciona a la persona que a sabiendas asegura el acceso, sin autorización a cualquier ordenador con el fin de obtener, directa o indirectamente, cualquier servicio informático; intercepta o hace que intercepte, sin autorización cualquier función de un ordenador por un dispositivo electromagnético, acústicos, mecánicos o por otros o, utiliza o hace que se utilicen, directa o indirectamente un ordenador o cualquier otro dispositivo con el propósito de cometer un delito a los que enunciamos con antelación.

En este caso el sujeto activo será sometido a juicio sumario y de ser culpable sancionado con una multa que no exceda de diez mil dólares o cárcel que no será superior a 3 años o ambas; en caso de reincidencia, a una multa que no exceda de veinte mil dólares o prisión por un período que no será superior a 3 años o, ambas.

De igual manera, en caso de haber dañado el equipo o la información, el infractor será sancionado con una multa que no excede de cincuenta mil dólares o prisión por un período no

superior a 5 años, o ambas.

Bahamas, se contiene en la sección 6 de The Computer Misuse Act, 2003, en donde se establece que cualquier persona que, a sabiendas modifique los datos contenidos en cualquier sistema de cómputo será sancionada con una multa que no excede de 100.00 rubias y pena de servidumbre por un término no mayor de 10 años.

En caso de que resultará dañado el funcionamiento del sistema informático, el programa o los datos almacenados en el equipo; el infractor será sancionado con una multa que no exceda de 200.000 rupias y trabajos forzados por un plazo no mayor de 20 años.

La interferencia en los datos en Bahamas, se regula en la sección 7, de The Computer Misuse Act, 2003, en donde se establece que se sanciona a la persona que a sabiendas y sin autoridad o excusa legal interfiera o interrumpa u obstaculice el uso legal de una computadora, o impide o evita el acceso a, o menoscaba la utilidad o eficacia de cualquier programa o datos almacenados en una computadora, con una multa que no exceda de diez mil dólares o prisión por un período no superior a tres años o con multa y prisión y, en el caso de una condena segunda o posterior, a una multa que no exceda de veinte mil dólares o prisión por un período no superior a cinco años, o ambas, multa y encarcelamiento.

El abuso de dispositivos en Bahamas, lo encontramos previsto en la sección 6, The Computer Misuse Act, 2003, en donde se lee que se sanciona a la persona que a sabiendas de que el acceso es seguro, sin autorización ingrese al ordenador con el fin de obtener, directa o indirectamente, cualquier servicio informático; intercepta directa o indirectamente y sin autorización cualquier función de un ordenador medio de un electro-magnéticos, acústicos, dispositivo mecánico o de otra índole, o utiliza o permite su utilización, directa o indirectamente, el ordenador o en cualquier otro dispositivo con el propósito de cometer un delito.

Y, será sancionado con una multa que no exceda de diez mil dólares o prisión por un período no superior a tres años o ambas; en el caso de una condena segunda o posterior, con una multa que no exceda de veinte mil dólares o prisión por un período no superior a tres años o con multa y encarcelamiento.

La falsificación informática en Bahamas, se prevé en la sección 4, The Computer Misuse Act 2003, se señala que se pune a la persona que, sin autoridad y a sabiendas hace una computadora para realizar cualquier función con el fin de garantizar el acceso a cualquier programa o datos contenidos en cualquier ordenador, con una multa que no exceda de cinco mil dólares o prisión por un período no superior a seis meses o con ambas y, en el caso de una condena segunda o posterior, con una multa no superior a diez mil dólares o reclusión por un término no superior a un año o multa y encarcelamiento.

Y, en caso de causar algún daño, o será castigado con una multa que no exceda de veinte mil dólares o prisión por un período no superior a tres años, o ambas.

También se sanciona a la persona que garantiza el acceso a cualquier programa o los datos almacenados en cualquier equipo que tenga la intención de cometer un delito (ya sea por sí o por cualquier otra persona) para que este sección se aplica, será culpable de un delito; lo cual aplica para los delitos relacionados con la propiedad, fraude, deshonestidad o que causa daño físico y que es punible en caso de condena con una pena de prisión de no menor de dos años; en esos casos se le sancionara con una multa no superior a diez mil dólares o prisión por un período no superior a tres años o con multa y encarcelamiento.

De igual manera se reprime a la persona que de manera intencional asegura el acceso sin autorización a cualquier ordenador con el fin de obtener, directa o indirectamente, cualquier servicio informático; intercepte o hace que se intercepte sin autorización, directa o indirectamente, cualquier función de un ordenador por medio de un dispositivo electro-magnéticos, acústicos, mecánicos o por otros, o utiliza o hace que se utilizan, directa o indirectamente, el ordenador o cualquier otro dispositivo con el propósito de cometer un delito; por lo que, de ser culpable se le sancionara con una multa no superior a diez mil dólares o prisión por un período no superior a tres años o ambas; en el segunda o posterior, a una caso de una condena multa que no exceda de veinte mil dólares o prisión por un período no superior a tres años, o ambas, multa y encarcelamiento.

Si se causa algún daño, con motivo de esas acciones, la persona será castigada con una multa que no exceda de cincuenta mil dólares o prisión por un período no superior a cinco años, o ambas.

El fraude informático en las Bahamas lo encontramos en la sección 4, The Computer Misuse Act, 2003, en donde se lee que se sanciona a la persona que utiliza una computadora para realizar cualquier función con el fin de garantizar el acceso a cualquier programa o los datos almacenados en cualquier equipo que tenga la intención de cometer un delito (ya sea por sí o por cualquier otra persona); lo cual se aplica a los delitos relacionados con la propiedad, fraude, deshonestidad o que causa daño físico y que es punible en caso de condena con una pena de prisión de no menos de dos años.

Y, se explica que la persona que se declare culpable se le aplicará una multa no superior a diez mil dólares o prisión por un período no superior a tres años o con multa y encarcelamiento.

BARBADOS

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Fraude informático**

Se regula dicha conducta en la sección 4, de "The Computer Misuse, Act, 2005", que se traduce como la Ley de Abuso de la Informática y, en ese apartado se dispone que una persona que a sabiendas o imprudencialmente y sin legal excusa o justificación:

a) Tenga acceso a la totalidad o parte de un sistema informático.

b) Hace que se ejecute un programa.

c) Utiliza el programa para acceder a los datos.

d) Copia o mueve el programa o los datos a cualquier otro medio de almacenamiento de aquel en que se lleva a cabo ese programa o datos a una ubicación diferente en el medio de almacenamiento en el que se lleva a cabo ese programa o datos; o, altera o borra el programa o los datos; sin importar la forma en que sea capaz de ser ejecutado.

En esos supuestos será sancionado con una multa de veinticinco mil dólares o, reclusión por un término de 2 años o, ambas.

En Barbados se regula en la sección 7, de Computer Misuse Act, en donde se lee que se sanciona a la persona que a sabiendas y sin excusa legítima, intercepte datos informáticos que no estén disponibles para el público con una multa de 000 S50 dólares o reclusión por un término de 5 años, o ambas.

La interferencia en los datos en Barbados, se regula en la sección 5 de The Computer Misuse Act, 2005, en donde se dispone que se sanciona a la persona que de manera intencional o imprudente, sin excusa legal o justificación destruya o altere los datos; hace que los datos sin sentido, inútiles o ineficaces; obstruya, interrumpa o interfiera con el uso legítimo de los datos; obstruya, interrumpa o interfiera con cualquier persona en el uso legítimo de los datos, o niega el acceso a los datos a cualquier persona con derecho a la información con una multa de 000 S50 o reclusión por un término de 5 años, o ambas.

El abuso en dispositivos en Barbados, lo encontramos en la sección 8, The Computer Misuse Act, 2005, en donde se sanciona a la persona que a sabiendas o de manera imprudente, sin justificación legal haga disponible o distribuya un dispositivo, incluido un programa informático, con el propósito de cometer un delito; proporciona una contraseña, el código de acceso o datos similares mediante el cual la totalidad o parte de un sistema informático que es capaz de ser visitado, con la intención de que sea utilizado por cualquier persona con el propósito de cometer un delito con una multa de 000 S50 o reclusión por un término de 5 años, o, ambas.

La falsificación informática en Barbados, se regula en la sección 9, The Computer Misuse Act 2005, de donde se extrae que se pune a la persona que a sabiendas utiliza una computadora para realizar cualquier función con el fin de asegurar el acceso a cualquier programa o datos contenidos en ese ordenador o en cualquier otro equipo, con la intención de cometer un delito contra la propiedad, fraude o deshonestidad, con una multa de $ 50 000 o encarcelamiento por un término de 5 años, o ambas.

Mientras que en Barbados el fraude informático está, en la sección 9, The Computer Misuse Act, 2005, se pune a la persona que a sabiendas utiliza una computadora para realizar cualquier

función con el fin de asegurar el acceso a cualquier programa o datos contenidos en ese ordenador o en cualquier otro equipo con la intención de cometer un delito contra la propiedad, fraude o deshonestidad, con una multa de $ 50 000 o encarcelamiento por un término de 5 años, o ambas.

BOLIVIA.

1. **Acceso ilícito**
2. **Interferencia en los datos**

Dicha conducta la encontramos regulada en el artículo 363 Ter, denominado "Alteración, Acceso y Uso Indebido de Datos Informáticos"; en donde se lee que se sanciona aquella persona que, sin estar autorizado, se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, con prestación de trabajo hasta 1 año o multa hasta de 200 días.

La interferencia en los datos en Bolivia lo encontramos en el artículo 363 del Código Penal, con el nombre de alteración de acceso y uso indebido de datos informáticos y, se sanciona a quien sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, con prestación de trabajo hasta un año o multa hasta de doscientos días.

EN ANTIGUA Y BARBUDA.

1. **Acceso ilícito**
2. **Interferencia en los datos**
3. **Abuso de dispositivos**

"En el documento The Computer Misuse Act".[100] 2006. No. Of. 206, emitida para prohibir el acceso no autorizado, del uso o de la interferencia de cualquier programa o los datos almacenados en una computadora y una computadora en sí misma y para facilitar la recopilación y el uso de las pruebas electrónicas, en las secciones 3 y 4 del abuso a la

[100] Se traduce como Ley de Abuso a la Informática.

informática, se sanciona a la persona que a sabiendas y sin autorización hace una computadora para desempeñar cualquier otra función con el fin de garantizar el acceso a cualquier programa o datos contenidos en ese equipo o en cualquier otro; por lo que será sancionado con una multa de quince mil dórales y dos años de prisión o ambos; en caso de reincidencia la multa aumenta hasta treinta mil dólares y prisión de tres años o ambas.

Se explica que ello aplica para una persona que asegura las ganancias o el acceso a cualquier programa o datos contenidos en un equipo modifica o borra el programa de datos; copia o mueve cualquier medio de almacenamiento distinto a aquel en que se encuentra; que utiliza o hace que sea la salida del equipo en el que se lleva a cabo, ya sea porque se muestra el acceso a ese programa o base de datos o, tenga la intención de asegurar ese acceso.

Y, se sanciona a la persona que utiliza una computadora para garantizar el acceso a cualquier programa o extraer datos contenidos en ese ordenador, con la intención de cometer un delito relacionado con la propiedad, el fraude, la deshonestidad o que cause un daño físico; que se castigue con penas de prisión por más de un año.

Dicha ilicitud será sancionada con una multa de quince mil dólares y prisión de dos años, o ambas.

La interferencia en datos, se contiene en la sección 5 a la 7, en The Computer Misuse Act, 2006, en donde se sanciona la persona que directa o indirectamente y sin autorización modifique cualquier programa o datos contenidos en un equipo con una multa de quince mil dólares y dos años de prisión y, en el caso de un segundo o posterior condena a una multa de treinta mil dólares y prisión de tres años, o ambas.

Y, en caso de que se origine un daño mayor, el responsable podrá ser condenado a una multa adicional de treinta mil dólares y prisión de tres años, o ambas.

También dentro de este apartado se establece que se sanciona a la persona que a sabiendas y sin autorización interfiera o dificulte el uso legal de una computadora, impida el acceso, menoscabe la utilidad o eficacia de cualquier programa o datos contenidos en un ordenador con una multa de quince mil dólares y dos años de prisión, o ambas, y en el caso de reincidencia, con una multa de treinta mil dólares y prisión por tres años o ambas cosas.

En caso de haber ocasionado un daño mayor será sancionado con una multa adicional de veinte mil dólares y prisión de tres años, o ambas.

El abuso de dispositivos lo encontramos regulado en la legislación de Antigua y Barbuda, en la sección 13, The Computer Misuse Act 2006, en donde se lee que se pune a la persona que intencionalmente o por imprudencia y sin excusa legal o justificación, vende, adquiere para su uso, importa, exporta, distribuye o hace disponible un dispositivo, incluido un programa informático que está diseñado o adoptado para el propósito de cometer un delito; altere la contraseña, código de acceso o datos similares mediante el cual la totalidad o cualquier parte de un sistema informático es capaz de ser visitada con la intención de que sea utilizado por cualquier persona con el fin de cometer un delito y, el responsable será condenado a una multa de cincuenta mil dólares y prisión de diez años, o ambas.

CHILE.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**

"Se contiene en el artículo 2, de la Ley relativa a Delitos Informáticos (19.233), en donde se lee que se sanciona a quién con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, con presidio menor en su grado mínimo a medio".[101] En Chile, esa conducta se encuentra tipificada en el artículo 2, de la Ley Relativa a Delitos Informáticos (19.33), ya que se sanciona a quien con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, con presidio menor en su grado mínimo a medio.

La interferencia en los datos en Chile, lo encontramos en el artículo 3, de la Ley Relativa de

[101] En el Código Penal de la República de Chile, se expone que las penas divisibles constan de tres grados: mínimo, medio y máximo, cuya extensión se determina en la siguiente tabla:

Penas	*Tiempo que comprende pena*	*Tiempo de su grado mínimo*	*Tiempo de su grado medio*	*Tiempo de su grado mínimo*
Presidio, reclusión, confinamiento, extrañamiento y relegación mayores.	De cinco años y un día a veinte años.	De cinco años y un día a diez años.	De diez años y un día a quince años.	De quince años y un día a veinte años.
Inhabilitación absoluta y especial temporales	De tres años y un día a diez años	De tres años y un día a cinco años	De cinco años y un día a siete años	De siete años y un día a diez años.
Presidio, reclusión, confinamiento, extrañamiento y relegación menores y destierro.	De sesenta y un días a cinco años.	De sesenta y uno a quinientos cuarenta días.	De quinientos cuarenta y un días a tres años.	De tres años y un día a cinco años.
Suspensión de cargo y oficio público y profesión titular.	De sesenta y un días a tres años.	De sesenta y un día a un año.	De un año y un día a dos año.	De dos años y un día a tres años.
Prisión	De uno a sesenta días.	De uno a veinte días.	De veintiuno a cuarenta días.	De cuarenta y uno a sesenta días.

Y, se explica que en cada grado de una pena divisible constituye una pena distinta; en los casos en que la ley señale una pena compuesta de dos o más distintas, cada una de éstas forma un grado de penalidad, la más leve de ellas el mínimo y la más grave el máximo.

Delitos Informáticos (19.233); en donde se dispone que se sanciona a quien maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, con presidio menor en su grado medio.

COLOMBIA.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Fraude informático**

Dicha ilicitud se encuentra contenida en el artículo 195, del Código Penal (Ley 599 de 2000), que se denomina *"Acceso Abusivo a un Sistema Informático; en donde se lee que se sancionara a quien abusivamente introduzca un sistema informático protegido con una medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, con una pena de 5 a 8 años de prisión".*[102]

En Colombia, se regula en el artículo 269C, de la Ley 1273 de 2009, con el nombre de interceptación de datos informáticos y, se pune el hecho de que un sujeto, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte, con prisión de treinta y seis a setenta y dos meses.

Mientras que en Colombia, la interferencia en los datos lo encontramos en el artículo 269D, de la Ley 1273 de 2009, bajo la denominación de daño informático y, se tipifica como tal, el hecho de que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, por lo que incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

El abuso en dispositivos en Colombia, lo encontramos previsto en el artículo 193 del Código Penal (Ley 599 de 2000), con el nombre de ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas y, se sanciona a quien sin permiso de

[102] Este artículo fue modificado por el artículo 25 de la Ley 1288, de 2009.

la autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

En tanto que, en Colombia el fraude informático está, en el artículo 269J de la Ley 1273 de 2009, se le ubica como transferencia no consentida de activos y, en ese caso se sanciona al que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, con una pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los párrafos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

COSTA RICA.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Falsificación informática**
5. **Fraude informático**
6. **Infracciones de la propiedad intelectual**

Se contiene en el artículo 94 del Código de Normas y Procedimientos Tributarios (Ley 4755, del 3 de mayo de 1971), denominado ***"Acceso Desautorizado a la Información; en donde se describe que será sancionado con prisión de 1 a 3 años a quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de de la administración tributaria, sin la autorización correspondiente"***.[103]

[103] Así fue reformado por el artículo 2° de la Ye 7900, del 3 de agosto de 1999.

También en el artículo 221 de la Ley General de Aduanas (Ley 7557, del 20 de octubre de 1995), intitulado "Delitos Informáticos", se establece que será reprimido con prisión de 1 a 3 años, a quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.

d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

Y, finalmente en el numeral 196 bis, del Código Penal, se le denomina "Violación de Comunicaciones Electrónicas", en donde se señala que será sancionado con pena de prisión de 6 meses a 2 años a la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes electrónicos, informáticos, magnéticos y telemáticos.

Adicionando que la pena será de 1 a 3 años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes electrónicos, informáticos, magnéticos y telemáticos.

En Costa Rica, lo encontramos en el artículo 196bis, del Código Penal, denominado violación de comunicaciones electrónicas y, se sanciona con prisión de seis meses a dos años a la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de

su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos.

Adicionando que la pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes electrónicos, informáticos, magnéticos y telemáticos.

En Costa Rica la interferencia en los datos lo encontramos en el artículo 229bis, del Código Penal, con el nombre de alteración de datos y sabotaje informático, en donde se establece que se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, *borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.*

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

En Costa Rica, lo encontramos en el artículo 217bis, del Código Penal, identificado con el nombre de fraude informático, en donde se lee que se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

En Costa Rica, el fraude informático se contiene en el artículo 217bis, del Código Penal, y se le denomina fraude informático, en donde se explica que se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

"Mientras que en Costa Rica, las infracciones de la propiedad intelectual las encontramos en el artículo 51".[104] de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual (N°

[104] Así Reformado Por El Artículo 1° Parte De La Ley 8656 De 18 De Julio De 2008.

8039, del 12 de octubre de 2000), dentro del rubro intitulado delitos contra derechos de autos y derechos conexos y, se sanciona a quien represente o comunique al público obras literarias o artísticas protegidas, directa o indirectamente, ya sea por medios alámbricos o inalámbricos, incluida la puesta a disposición del público de sus obras, en tal forma que los miembros del público puedan acceder a estas obras desde el lugar y en el momento en que ellos elijan, sin autorización del autor, el titular o el representante del derecho, será sancionado de la siguiente manera:

a) Con multa de cinco a veinte salarios base, cuando el monto del perjuicio no sobrepase los cinco salarios base.

b) Con seis meses a dos años de prisión o multa de veinte a ochenta salarios base, cuando el monto del perjuicio sea superior a los cinco salarios base y no sobrepase los veinte salarios base.

c) Con uno a cuatro años de prisión o multa de ochenta a doscientos salarios base, cuando el monto del perjuicio sea superior a los veinte salarios base y no sobrepase los cincuenta salarios base.

d) Con tres a cinco años de prisión o multa de doscientos a quinientos salarios base, cuando el monto del perjuicio sobrepase los cincuenta salarios base.

NICARAGUA.

1. **Acceso ilícito**
2. **La falsificación informática**

Encontramos dentro del Código Penal, en el artículo 198, intitulado "Acceso y Uso no Autorizado de Información", en donde se lee que a quien sin la debida autorización utilice los registros informáticos de otro o, ingrese por cualquier medio a su banco de datos o archivos electrónicos, será penado con prisión de 1 a 2 años, y de 200 a 500 días.

La falsificación informática en Nicaragua, lo encontramos en el artículo 284 del Código Penal, dentro del apartado de falsificación material y, se sanciona a quien haga en todo o en parte un documento falso o altere uno verdadero, con prisión de uno a cuatro años, si se trata de un documento o instrumento público, y con prisión de seis meses a dos años si se trata de un

documento privado.

PANAMÁ.

1. **Acceso ilícito**
2. **El fraude informático**
3. **Infracciones de la propiedad intelectual**

Se contiene en el precepto 283 del Código Penal, en donde se lee que será sancionado con 2 a 4 años de prisión, a quien indebidamente ingrese o utilice una base de datos, red o sistema informático.

En Panamá, el fraude informático lo encontramos en el artículo 220 del Código Penal y se sanciona a quien para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, con cuatro a seis años de prisión.

La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada.

En Panamá, las infracciones a la propiedad intelectual se localizan en los artículos 258 y 259 del Código Penal; el primero de esos dispositivos encontramos que se impondrá la pena de cuatro a seis años de prisión a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, ejecute alguna de las siguientes conductas:

1. Almacene, distribuya, exporte, ensamble, fabrique, venda, alquile o ponga en circulación de cualquier otra manera reproducción ilícita de una obra protegida por el Derecho de Autor y Derechos Conexos.

2. Introduzca en el país cantidades significativas, con fines comerciales, reproducciones ilícitas de obras protegidas por el Derecho de Autor y Derechos Conexos.

3. Reproduzca, copie o modifique, con carácter industrial o mediante laboratorios o mediante procesos automatizados, obras protegidas por el Derecho de Autor y Derechos Conexos.

Y, en el segundo dispositivo, se establece que la misma pena prevista en el artículo anterior se le aplicará a quien sin autorización reproduzca o copie, por cualquier medio, la actuación de un intérprete o ejecutante, un fonograma, videograma, programas de ordenador o una emisión de radiodifusión en todo o en parte, o introduzca en el país, almacene, distribuya, exporte, venda, alquile o ponga en circulación, de cualquier otra manera, dichas reproducciones o copias.

REPÚBLICA DOMINICANA.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Abuso de dispositivos**
5. **Falsificación informática**
6. **Fraude informático**
7. **Infracciones a la propiedad intelectual**

En el artículo 6 de la Ley 53/07, contra Crímenes y Delitos de Alta Tecnología, se le conoce a esa conducta como acceso ilícito y, se regula como tal el hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización; misma que se sancionará con las penas de 3 meses a un 1 año de prisión y multa desde una vez a 200 veces el salario mínimo.

En República Dominicana, se encuentra regulado en el artículo 10 de la Ley 53/07, Contra Crímenes y Delitos de Alta Tecnología, con el nombre de daños o alteración de datos y se incluye ahí el hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, lo que se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas

veces el salario mínimo.

Y, cuando ese hecho sea realizado por un empleado, ex-empleado o una persona que preste servicios directa o indirectamente a la persona física o jurídica afectada, las penas se elevaran desde uno a tres años de prisión y multa desde seis hasta quinientas veces el salario mínimo.

La interferencia en los datos En República Dominicana, la encontramos en el artículo 10 de la Ley 53/07, Contra Crímenes y Delitos de Alta Tecnología, con el nombre de daño o alteración de datos, y se pune el hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, con penas de tres meses a un ario de prisión y multa desde tres hasta quinientas veces el salario mínimo.

Y, cuando este hecho sea realizado por un empleado, ex-empleado o una persona que preste servicios directa o indirectamente a la persona física o jurídica afectada, las penas se elevaran desde uno a tres años de prisión y multa desde seis hasta quinientas veces el salario mínimo.

El abuso de dispositivos en la República Dominicana, lo encontramos en el artículo 8, de la Ley 53/07, contra el Delito Cibernético, y se le denomina dispositivos fraudulentos, en donde se señala que el hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

La falsificación informática en República Dominicana lo encontramos previsto en el artículo 18 de la Ley 53/07, contra el Delito Cibernético, con el rubro de falsedad de documentos y firmas, en donde se lee que se reprime a quien falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a tres arios de prisión y multa de cincuenta a doscientas veces el salario mínimo.

En República Dominicana, el fraude informático se encuentra en los artículos 13 al 16 de la

Ley 53/07 contra el Delito Cibernético, con el nombre, en el primero de los dispositivos de robo mediante la utilización de alta tecnología, en donde se señala que se considera robo cuando se comete por medio de la utilización de sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología, se sancionará con la pena de dos a cinco años prisión y multa de veinte a quinientas veces el salario mínimo.

En el siguiente dispositivo se le denomina obtención ilícita de fondos, en donde se lee que se sanciona el hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo.

Adicionando un párrafo en donde se sanciona el hecho de que se realicen transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo.

De igual manera, se le denomina estafa a la realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, y se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.

Y, el chantaje que se realiza a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, se sancionará con la pena de uno a cinco años de prisión y multa de diez a doscientas veces el salario mínimo.

En República Dominicana, las infracciones a la propiedad intelectual se regulan en el numeral 25 de la Ley 53/07 contra el Delito Cibernético, y se le conoce con el nombre de delitos

relacionados a la propiedad intelectual y afines, en donde se establece que cuando se infrinjan las normas de derechos de autor, empleando sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

TRINIDAD Y TOBAGO.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **Interferencia en los datos**
4. **Fraude informático**

Se regula en la sección 3, de *"The Computer Misuse Act, 2003"*.[105] En donde se lee que será sancionada en juicio sumario la persona que a sabiendas y sin autorización utiliza una ordenador o un programa con el fin de garantizar el acceso a los datos contenidos en otro equipo, con una multa de quince mil dólares y 2 años de prisión y, en el caso de reincidencia con una multa de treinta mil dólares y prisión de 4 años.

Se entiende que, para los efectos a los que se alude en ese apartado una persona asegura o tiene acceso a cualquier programa o a los datos contenidos en una computadora, si modifica o borra el programa o los datos; copia o se mueve a cualquier medio de almacenamiento distinto de aquel en el que se lleva a cabo o en una ubicación diferente en el medio de almacenamiento en el que se lleva a cabo; utiliza o hace que sea la salida del equipo en el que se lleva a cabo para hacer que el programa sea ejecutado o al menos una función del mismo.

Explicando que se debe probar la forma en que cualquier programa o salida de datos representa o no una forma en la que un programa es capaz de ser ejecutado o, en el caso es capaz de procesar los datos por un ordenador externo.

Mientras que en Trinidad y Tobago, en la sección 5, The Computer Misuse Act, 2003, se sanciona con multa de quince mil dólares y dos años de prisión, a quien directa o indirectamente y sin autorización hace una modificación a cualquier programa o datos contenidos en un equipo y, se le sigue juicio sumario; en caso de reincidencia, la multa asciende

[105] Que se traduce como Ley de Abuso de la Informática.

a treinta mil dólares y cuatro años de cárcel.

Si se causa un daño como consecuencia del delito, la persona que sea declarada culpable se le sancionará con una multa adicional de veinte mil dólares y prisión de tres años.

La interferencia en los datos en Trinidad y Tobago, se encuentra en la sección 5, de The Computer Misuse Acta, 2003, y, se sanciona a la persona que directa o indirectamente sin autorización modifica cualquier programa o datos contenidos en un equipo con una multa de quince mil dólares y dos años de prisión y, en el caso de una condena segunda o posterior, con una multa de treinta mil dólares y prisión de cuatro años; adicionando que, de originarse un daño, se le reprimirá con una multa adicional de veinte mil dólares y prisión de tres años.

En Trinidad y Tobago, el fraude informático lo encontramos en la sección 4, de The Computer Misuse Act, 2003, de la que se extrae que se sanciona a la persona que a sabiendas utiliza una computadora para realizar cualquier función con el fin de garantizar el acceso a cualquier programa o datos contenidos en ese ordenador o en cualquier otro equipo con la intención de cometer un delito relacionado con la propiedad, fraude, deshonestidad o que cause daño físico; con una multa de quince mil dólares y dos años de prisión.

VENEZUELA.

1. **Acceso ilícito**
2. **Interceptación ilícita**
3. **La interferencia en los datos**
4. **Abuso de dispositivos**
5. **La falsificación informática**
6. **Fraude informático**
7. **Infracciones a la propiedad intelectual**

"Se contiene en el artículo 6, de la Ley Especial Contra los Delitos Informáticos, denominándole acceso indebido, sancionando a quien sin la debida autorización o excediendo la que hubiere obtenido acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, con prisión de 1 a 5 años y multa de

10 a 50 unidades tributarias. [106]

Y, en Venezuela, se encuentra contenido en el artículo 7, de la Ley Especial contra los Delitos Informáticos, bajo el nombre de sabotaje o daño a sistemas y se sanciona a quien destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que emplee tecnologías de información o cualquiera de los componentes que lo conforman con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

E, incurrirá en la misma pena a quien destruya, dañe, modifique o inutilice la información contenida en cualquier sistema que emplee tecnologías de información o en cualquiera de sus componentes; en este caso, la pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, siempre que ello se realice mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

La interferencia en los datos en Venezuela lo encontramos previsto en el artículo 7, de la Ley Especial contra los Delitos Informáticos, con el nombre de sabotaje o daño a sistemas, en donde se lee que se reprime a quien destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

E, incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

El abuso de dispositivos, en Venezuela la encontramos en el artículo 10 de la Ley Especial

[106] En el Código Penal de Venezuela se define la multa en los siguientes términos:

"Artículo 30° La pena de multa consiste en la obligación de pagar al Fisco del respectivo Estado, o a las Rentas Municipales del Distrito Federal en sus casos o al Fisco Nacional si el juicio se inició en un Territorio Federal, la cantidad que conforme a la ley determine la sentencia. Si el juicio ha sido por falta, la multa será en beneficio del respectivo Fisco Municipal."

contra los Delitos Informáticos, con el nombre de posesión de equipos o prestación de servicios de sabotaje y, se lee que se sanciona a quien con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

La falsificación informática en Venezuela, lo localizamos en el artículo 12 de la Ley Especial contra los Delitos Informáticos, con el título de falsificación de documentos, en donde se lee que el que a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad y el aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Y, en Venezuela, el fraude informático se regula en el artículo 14 de la Ley Especial contra los Delitos Informáticos, denominando fraude, y, se sanciona a quien, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Y, en Venezuela, las infracciones a la propiedad intelectual lo encontramos en el artículo 25 de la Ley Especial contra los Delitos Informáticos, con el nombre de apropiación de propiedad intelectual, en donde se establece que, al que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

3.3DERECHO PANORÁMICO INTERNACIONAL SOBRE LOS DELITOS INFORMÁTICOS

Como hemos podido vislumbrar, legislar en materia de internet no es una función fácil e incluso se ha dicho que la fuerza de Internet está precisamente en el caos que lleva inmerso en él y que la red Internet no puede ser censurada, ni restringida y no puede ser controlada, tampoco detenida, empero lo anterior, los Estados Unidos de Norte América han hecho varios intentos por legislar y regular esta enorme red de comunicaciones en la cual es difícil definir de donde procede la información se encuentra contenida en ella, quien la coloca en la red y cuál es la veracidad y finalidad de la misma, con todas estas limitantes que rebasan las fronteras y recursos estatales hemos considerado necesario apuntar de manera general lo que algunos Estados han implementado para legislar y por tanto controlar lo que sucede en Internet, como lo precisamos en el capítulo seis de la presente tesis.

Para lograr lo anterior tomamos como Países para realizar un sistema comparado como lo es Estados Unidos, Unión Europea, China y la Unión Europea; que si bien no es un Estado como tal si están instituidos por un cúmulo de ellos y lo que en su seno se disponga se adoptadora en lo que respecta a sus Estados miembros.

Cabe precisar que las valoraciones que resultan del análisis de cada Estado se realizaran una vez que se hayan plasmado todos los contenidos oportunos para entender lo que se ha hecho en cada país y hacer una reflexión final que nos admita la debida comparación.

ALEMANIA *"En la República Federal de Alemania, es el lugar de Europa donde se ha realizado las mejores reformas legales que son pertinentes para incluir los delitos informáticos en el Código Penal, de allí que desde el 15 de mayo de año 1986 entró en vigencia la segunda Ley en contra de la Criminalidad Económica, que estipula dentro de ella los siguientes delitos".*[107]

El Espionaje de datos.

La Estafa informática.

La Alteración de datos.

El Sabotaje informático.

[107] El texto completo del Código Penal Alemán en idioma inglés, 23 de febrero del 2013 puede consultarse en: *http://wings.buffalo.edu/law/bclc/germind.htm. Del Centro de Leyes Penales de Búfalo, Estados Unidos de América.*

Examinemos los dispositivos de la precitada Ley de Alemania:

Parágrafo 202ª StGB: El Espionaje de datos.

1. - El que sin autorización se procure para sí o para terceros datos que no estén destinados a él y que se encuentren especialmente protegidos contra un acceso no autorizado, serán castigados con la privación de libertad de hasta tres años o con multa.

2. - Son datos en el sentido del parágrafo 1. - únicamente aquellos que estén almacenados o son transmitidos electrónica, magnéticamente o de otra forma no perceptible directamente.

Parágrafo 263ª StGB: La Estafa informática.

1. - El que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial antijurídico, causare un perjuicio en el patrimonio de otro, determinado el resultado de una operación de proceso de datos mediante la incorrecta configuración del programa, el empleo de datos incorrectos o incompletos, el empleo no autorizado de datos o cualquier otra intervención ilegítima en el curso del proceso será sancionado con una pena de prisión de hasta cinco años o pena de multa.

2. - El parágrafo 263, apartados 2 a 5, es aplicable en lo que corresponda.

Parágrafo 269 StGB. La Falsificación de datos probatorios.

1. - El que, para producir un engaño en el tráfico jurídico, almacene o altere datos probatorios de tal modo que, de ser percibidos, resultare un documento no auténtico o falseado, o se sirva de datos almacenados o alterados del modo referido, será castigado con pena privativa de libertad de hasta cinco años o con pena de multa.

2. - La tentativa es punible

3. - Debe aplicarse el Parágrafo 267, Parágrafo 3.

Parágrafo 303ª. La Alteración de Datos.

1. -"El que, de modo antijurídico, borre, oculte, haga inutilizable o altere datos (Parágrafo 202ª, Párrafo 2), será castigado con pena de prisión de hasta dos años o pena de multa.

2. - La tentativa es punible.

Parágrafo 303. El Sabotaje informático.

1. - El que perturbare un proceso de datos que sea de importancia esencial para una empresa o establecimiento industrial ajeno o para la administración. -Cometiendo un hecho de los referidos en el parágrafo 303ª, párrafo 1, ó

2. - destruyendo, dañando, inutilizando, eliminando o alterando un equipo de proceso de datos o un soporte, será sancionado con pena de prisión de hasta cinco años o de multa.

3. - La tentativa es punible.

CHINA

Las autoridades gubernamentales han tratado de controlar el acceso a la Internet determinando cuales son las páginas de internet y sitios a los cuales sus gobernados pueden tener acceso y por tanto están regularmente monitoreando a los ciudadanos que se conectan a la Internet.

No obstante, lo anterior no ha sido logrado de manera exitosa dado el rol tan importante que juegan los hackers en virtud de que estos han logrado crear un software al cual se le ha llamado (Camera Shy) el cual consiente acceder a la navegación libre por la red de forma anónima y a través del sistema de encriptación, además de que sus fuentes y ejecutables están aprovechables y disponibles de forma gratuita, de tal manera que dichos sitios surgen o aparecen como si fueran inofensivos ante cualquier programa de censura.

A pesar de lo anterior en el año 2000 entró en vigencia en el marco de la Ley de Telecomunicaciones un Código que prohíbe la divulgación de aquellos mensajes que pongan en riesgo o peligro la seguridad del Estado, por medio de lo cual el gobierno exige a todos los proveedores del Internet a suspender o interrumpir este tipo de mensajes además debe comunicar inmediatamente a las autoridades; si omite hacerlo se le cancelara definitivamente el portal se le establecerá una multa de hasta un millón de yuanes (120, 500 usd.).

ESPAÑA *"En el nuevo Código Penal español (aprobado por la Ley Orgánica 10/1995, de 23 de Noviembre BOE (boletín Oficial Español) número 281, de 24 de Noviembre de 1.995 se encuentran varios artículos que se encuentran relacionados con los delitos informáticos, de esta forma procedemos a reproducirlos".*[108]

Artículo 197.

1. - El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. - Las 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.

3. - Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. - Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la

[108] El texto completo del Código Penal Español, 24 de febrero del 2013 puede verse en: *http://www.law.unican.es/incade/lex/cpint.htm, del Instituto Cántabro de Derecho.*

pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. - Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. - Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198. La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199.

1. - El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. - El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200. Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201.

1. - Para proceder por los delitos previstos en este capítulo será necesaria

denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. - No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. - El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211. La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212. En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238. Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1º. –Escalamiento.

2º. - Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º. - Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.

4º. - Uso de llaves falsas.

5º. - Inutilización de sistemas específicos de alarma o guarda.

Artículo 239. Se considerarán llaves falsas:

1º. - Las ganzúas u otros instrumentos análogos.

2º. - Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.

3º. - Cualesquiera otras que no sean las destinadas por el propietario para

abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248.

1. - Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. - También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255.

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º. - Valiéndose de mecanismos instalados para realizar la defraudación.

2º. - Alterando maliciosamente las indicaciones o aparatos contadores.

3º. - Empleando cualesquiera otros medios clandestinos.

Artículo 256. El que hiciere uso de cualquier equipo terminal de telecomunicación, 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.

Artículo 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.

Artículo 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 concurriera alguno de los supuestos siguientes:

1º. - Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º. - Que se cause por cualquier medio infección o contagio de ganado.

3º. - Que se empleen sustancias venenosas o corrosivas.

4º. - Que afecten a bienes de dominio o uso público o comunal.

5º. - Que arruinen al perjudicado o se le coloque en grave situación económica.

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

Artículo 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 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 específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de

ordenador.

Artículo 278.

1. - El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. - Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. - Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400. La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536. La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

ESTADOS UNIDOS DE AMÉRICA

Este es uno de los principales países en adoptar en el año de 1994 el Acta Federal de Abuso Informático (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Lo anterior con la intención de eliminar algunos conceptos de lo que son los virus informáticos, los gusanos informáticos, los caballo de Troya informático y en que distinguen de los virus, en el acta de 1994 proscribe la transferencia de los programas, la información, los códigos o los comandos que efectúan daños a la computadora, o a sus sistemas informáticos, o a las redes, a la información, o a los datos o programas (18 U.S.C.:Sec. 1030 (a) (5) (A).

La legislación penal en comento resulta un avance porque tipifica notoriamente los delitos de transmisión de virus informáticos. Establece la distinción y el tratamiento a aquellos que de forma temeraria arrojan ataques de virus de aquellos que lo realizan con todo el propósito de hacer estragos o daños. Puntualiza dos niveles para establecer el tratamiento de quienes crean virus:

a) Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

El acta de 1994 es el un acercamiento más comprometido al aumento de los problemas de los virus informáticos, concretamente no definiendo a los virus sino relatando el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Distinguiendo los niveles de delitos, la nueva legislación dará lugar a que se contemple qué se debe entender como un acto delictivo.

En materia de fraudes y de estafas electrónicas, y otros actos dolosos vinculados respecto de los dispositivos de acceso a sistemas informáticos, la legislación norteamericana castiga con pena de prisión y con multa, a la o las personas que defrauden a otro individuo mediante el uso o la utilización de

una computadora o de una red informática. Para comprender mejor cuál es la percepción que se tiene en este país es trascendente examinar dos leyes:

• Ley de decencia de las Comunicaciones. La cual fue ratificada como ley federal el 8 de febrero del año de 1996, esta legislación prohibía el acceso a sitios en Internet, el cual contenía material que se estimaba como ostensiblemente ofensivo o indecente, para las personas menores de 18 años. Se estableció que la sanción o pena sería de 250.000 dólares e incluía 2 años de prisión a todo aquel que propagara, o difundiera o colocara dicho material en un foro en línea es decir (on-line) que son (redes abiertas). En este rubro la Asociación de Libertades Civiles de E.U.A mantuvo su inconstitucionalidad por que la consideraron una violación a la libertad expresión. En el mismo mes de febrero la aplicación de la comentada ley entró en receso y en el año 1997 esta se anuló.

• Ley para la protección en línea de la privacidad de los menores. Se bosquejó por medio de una iniciativa propuesta por la senadora Patty Murray misma que fue promulgada por el Congreso estadounidense en octubre de 1998. La antes citada ley contemplaba el uso de programas filtro o de selección de contenidos; establecía que los encargados o los operadores de los sitios web (websites) comerciales deben exhibir claramente notas explicativas sobre la recopilación y la utilización de la información, y que deben de exigir la autorización obligatoria de los padres para los datos que les son proporcionados o facilitados por los menores de 12 años.

La Corte Suprema de los Estados Unidos de América se pronunció al respecto al decir que: no se debería sancionar ninguna ley que restrinja la libertad de expresión; la red de Internet puede ser determinada como una conversación mundial carente de barreras. Es por esto que el gobierno no puede a través de ningún medio obstaculizar o interrumpir o interferir esa conversación, y como es la forma más participativa de disertaciones en masa que se ha desarrollado, la red de Internet se merece mayor salvaguarda ante cualquier intrusión gubernamental.

FRANCIA En este rubro Francia a través de su Tribunal de Gran Instancia de París, decretó una medida cautelar en donde se logro aplicar por primera vez la Ley de reforma del régimen de comunicaciones francés (Ley del primero de agosto del año 2000) en el que exigía a todos los especialistas y a los operadores de la Internet a recopilar y almacenar los datos personales de cada uno de los usuarios que crean páginas de Internet e informarse ampliamente en caso de que exista algún litigio, por el autor del sitio determinado.

"El legislador francés estableció nuevos tipos penales los cuales están vinculados y relacionados con la delincuencia informática, mediante la Ley No.88-19 respecto del Fraude Informático, y lo incorporo al Código Penal Francés, dentro de la siguiente denominación".[109]

"DE VARIAS TRANSGRESIONES EN MATERIA INFORMÁTICA".

Examinemos ahora el texto de la legislación en referencia:

Art.462-2 Código Penal. Acceso fraudulento a un sistema de elaboración de datos. Quien fraudulentamente acceda a todo o parte de un sistema de tratamiento automático de datos o se mantenga en él será castigado con prisión de dos meses a un año y con multa de 2.000 a 50.000 francos o con una de las dos penas.

Si de ello resulta la supresión o modificación de datos contenidos en un sistema o resulta la alteración del funcionamiento del sistema, la prisión será de dos meses a dos años y la multa de 10.000 a 100.000 francos.

Art. 462-3 Código Penal.- el sabotaje informático. Quien, intencionalmente y con menosprecio de los derechos de los demás, impida o falsee el funcionamiento de un sistema de tratamiento automático de datos será castigado con prisión de tres meses a tres años y con multa de 10.000 francos o con una de las dos penas.

[109] El texto completo del Código Penal Francés, 24 de febrero del 2013 puede revisarse en: *http://www.legifrance.gouv.fr/citoyen/code.ow*

Art. 462-4 Código Penal.- La destrucción de datos. Quien intencionalmente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de las dos penas.

Art. 462-5 Código Penal.- La falsificación de documentos informáticos. Quien de cualquier modo falsifique documentos informatizados, con la intención de causar un perjuicio a otro, será castigado con prisión de un año a cinco años y con multa de 20.000 a 2'000.000 de francos, o con una de estas dos penas.

Art. 462-6 Código Penal. El uso de documentos informatizados falsos. Quien conscientemente haga uso de documentos falsos del Art. 462-5 será castigado con prisión de un año a cinco años y con multa de 20.000 a 2'000.000 de francos o con una de las dos penas.

Art. 462-7 Código Penal. La tentativa. Dispone que la tentativa se castiga con la misma pena que el delito mismo (o consumado)

Art. 462-8 Código Penal. La sanción. Sanciona a los que han participado en una asociación formada o en u acuerdo tendiente a la preparación o concreción por uno o varios hechos materiales, de uno o varios de estos delitos, con la pena más severa en ellos establecida.

Art. 462-9 Código Penal. Las facultades. Este artículo faculta al tribunal para confiscar los materiales utilizados en la comisión de estos delitos, o que hayan servido para ello.

GRAN BRETAÑA. Derivado de un caso de hacking en la anualidad de 1991, se inició a regir en este país la Computer Misuse Act (Que es la Ley de Abusos Informáticos). Por medio de esta ley surge el intento, exitoso o no, de alterar datos informáticos que va a ser sancionado con hasta cinco años de prisión o multas. Y ésta ley tiene un apartado que determinaba la modificación de datos sin autorización o consentimiento. Y los virus también están

incorporados en esa calidad. El liberar dentro de la red un virus tiene la penalidad desde un mes a cinco años, esto dependiendo del daño que ocasionen.

HOLANDA. El primero de Marzo del año de 1993 entró en vigor la Ley de Delitos Informáticos, en la cual se penaliza el hacking, y la utilización de los servicios de telecomunicaciones evadiendo el pago ya sea total o parcial de dicho servicio, dentro de la ingeniería social (que es el arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la colocación de los virus.

La distribución de virus está penada de muy diversa forma si se escaparon por error o si éstos se liberaron con la finalidad de causar un daño. Si se comprueba que el virus se disperso por un error, la pena no superará el mes de prisión; pero, si se patentiza que fueron liberados con todo el propósito de ocasionar o causar un daño, la pena puede alcanzar hasta los cuatro años de prisión.

LA UNIÓN EUROPEA El 27 de septiembre de 1996 el Consejo de Telecomunicaciones de la Unión Europea acogió una Resolución para parar y frenar la difusión de contenidos ilícitos en Internet, especialmente en tratándose de la pornografía infantil.

Dicho organismo dilucido que no obstante que la legislación nacional de cada uno de los países que son miembros era aplicable a la red, haciendo la fundada reflexión de que lo que es ilícito fuera de la línea, lo es también en línea; se necesita alcanzar un acuerdo mucho más amplio para afrontar los desafíos que día a día dispone la Internet, mismos que provienen de su carácter transnacional, y de su manifiesta resistencia a la manipulación y de la gran descentralización de los servidores desde los cuales se crea, y se distribuye toda la información ilícita.

"Todo esto apunta a que cada uno de los estados miembros incorpore normas que regulen los nuevos servicios de Internet, no obstante, persistentemente se pone mayor hincapié en legislar la actividad y la responsabilidad de los proveedores del servicio. La comunidad

europea dio como soporte en los siguientes documentos".[110]

DOCUMENTO 399D0276

Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la cual se apruebo un plan plurianual de acción comunitaria para propugnar por una mayor seguridad dentro de la utilización y el uso del Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.

DIARIO OFICIAL N° L 033 DE 06/02/1999 P. 0001 – 0011.

DECISIÓN N° 276/1999/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una más seguridad en la utilización y el uso del Internet para luchar en contra los contenidos ilícitos y perjudiciales en las redes mundiales.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1 Precisa:

1. Se aprueba el plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet (denominado en lo sucesivo el plan de acción), tal como se describe en el anexo I.

2. El plan de acción abarcará un período de cuatro años, desde el 1 de enero de 1999 hasta el 31 de diciembre de 2002.

3. La dotación financiera para la ejecución del plan de acción para el período comprendido entre el 1 de enero de 1999 y el 31 de diciembre de 2002 será de 25 millones de euros.

La Autoridad Presupuestaria autorizará los créditos anuales ajustándose a las perspectivas financieras. En el anexo II figura un desglose indicativo del gasto.

Artículo 2. El plan de acción tiene el objetivo de propiciar una mayor

[110] Legislación Europea Comunitaria, Documento 399D0276, 25 de febrero del 2013, *http://europa.eu.int/eurlex/es/lif/index.html*

seguridad en la utilización de Internet y fomentar a nivel europeo la creación de un entorno favorable para el desarrollo de la industria vinculada a Internet.

Artículo 3. Para cumplir el objetivo mencionado en el artículo 2, se llevarán a cabo las acciones siguientes de apoyo y promoción de las medidas que adopten los Estados miembros bajo la dirección de la Comisión y, de conformidad con las líneas de actuación que se establecen en el anexo I y los medios de ejecución del plan de acción que se establecen en el anexo III:

- fomentar la autorregulación del sector y los mecanismos de supervisión de los contenidos (por ejemplo, los relativos a contenidos tales como la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico).
- alentar al sector a ofrecer medios de filtro y sistemas de clasificación que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo, y a los adultos decidir a qué contenidos lícitos desean tener acceso, y que tengan en cuenta la diversidad cultural y lingüística,
- mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet,
- llevar a cabo medidas de apoyo como la evaluación de las implicaciones jurídicas,
- realizar actividades para fomentar la cooperación internacional de los campos mencionados,
- efectuar otras actividades que contribuyan a la consecución de los objetivos establecidos en el artículo 2.

Artículo 4.

1. La Comisión será responsable de la ejecución del plan de acción.
2. El procedimiento que se establece en el artículo 5 se aplicará a:
    a) El programa de trabajo, incluido todo gasto en las actividades

descritas en el punto 9 del anexo III

b) El desglose de los gastos presupuestarios,

c) Los criterios y contenidos de las convocatorias de propuestas,

d) La evaluación de los proyectos presentados con arreglo a las convocatorias de propuestas para su financiación por la Comunidad y del importe estimado de la aportación comunitaria a cada proyecto cuando dicho importe sea igual o superior a 300 000 euros,

e) Las medidas para la evaluación del programa,

f) Cualquier apartamiento de las reglas que se establecen en el anexo III,

g) La participación en cualquier proyecto de personas jurídicas de terceros países y de las organizaciones internacionales mencionadas en el apartado 3 del artículo 7,

h) Otras acciones que pudieran emprenderse conforme a lo dispuesto en el último guión del artículo 3.

3. Cuando, según lo previsto en el cuarto guión del apartado 2, el importe de la aportación comunitaria sea inferior a 300 000 euros, la Comisión informará al Comité contemplado en el artículo 5 sobre los proyectos y los resultados de su evaluación.

4. La Comisión informará periódicamente al Comité contemplado en el artículo 5 de los avances en la ejecución del programa en su conjunto.

Artículo 5. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

El representante de la Comisión presentará al Comité un proyecto de las medidas que deban tomarse. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate. El dictamen se emitirá según la mayoría prevista en apartado 2 del artículo 148 del Tratado para adoptar aquellas decisiones que el Consejo deba tomar a propuesta de la Comisión.

Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán de la manera definida en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas previstas cuando sean conformes al dictamen del Comité. Cuando las medidas previstas no sean conformes al dictamen del Comité o en caso de ausencia de dictamen, la Comisión someterá sin demora al Consejo una propuesta relativa a las medidas que deban tomarse. El Consejo se pronunciará por mayoría cualificada. Si, transcurrido un plazo de tres meses a partir del momento en que la propuesta se encuentre sometido al Consejo, éste no se hubiere pronunciado, la Comisión adoptará las medidas propuestas.

Artículo 6. 1. Para garantizar la utilización eficaz de la ayuda comunitaria, la Comisión velará por que las acciones emprendidas con arreglo a la presente Decisión estén de manera efectiva sujetas a valoración previa, supervisión y evaluación posterior.

2. Durante la ejecución de los proyectos y una vez concluidos, la Comisión evaluará la forma en que se han llevado a cabo y su impacto, para determinar si se han alcanzado los objetivos iniciales.

3. Los beneficiarios deberán presentar un informe anual a la Comisión.

4. Transcurrido un período de dos años y al concluir el plan de acción, la Comisión presentará al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, previo examen por el Comité contemplado en el artículo 5, un informe de evaluación de los resultados de la ejecución de las líneas de actuación enunciadas en el anexo I. Deberá hacerse referencia a las conclusiones generales aplicables a todas las categorías de contenidos ilícitos. La Comisión podrá presentar, con arreglo a dichos resultados, propuestas para reorientar el plan de acción.

Artículo 7. Dice: 1. Podrán participar en el plan de acción personas jurídicas establecidas en los Estados de la AELC que sean Estados miembros del Espacio Económico Europeo (EEE) de conformidad con lo

dispuesto en el Acuerdo EEE. 2. Asimismo podrán participar personas jurídicas establecidas en Estados asociados de Europa Central y Oriental, de conformidad con las condiciones establecidas en los protocolos adicionales de los acuerdos de asociación, entre otras las de tipo financiero y las relativas a la participación en programas comunitarios. También podrán participar personas jurídicas establecidas en Chipre sobre la base de los créditos suplementarios y con arreglo a la misma normativa que se aplica en los Estados de la AELC miembros del EEE, de conformidad con los procedimientos que se acuerden con dicho país. 3. Podrán participar, de conformidad con el procedimiento establecido en el artículo 5 y sin asistencia financiera de la Comunidad en el marco del plan de acción, personas jurídicas establecidas en otros terceros países y organizaciones internacionales, cuando su participación contribuya de manera eficaz a la ejecución del plan de acción y teniendo en cuenta el principio de beneficio mutuo.

Artículo 8. Los destinatarios de la presente Decisión serán los Estados miembros. Hecho en Bruselas, el 25 de enero de 1999.

3.4 ORGANISMOS INTERNACIONALES

En relación a la normatividad internacional cabe indicar que los Organismos Internacionales son fundamentales en virtud de que trabajan en forma conjunta, con las autoridades del Estado y aunque tienen objetivos particulares a seguir, son de gran auxilio para el descubrimiento de los ilícitos informáticos.

Para la Organización para la Cooperación Económica en Asia/Pacifico (**APEC**) estos se encargan de la regulación de los Proveedores de los Servicios de Internet (ISP´s); se facultan para el examen de las tarifas de cobro de los ISP´s (de acuerdo a la región en la que laboren, el desarrollo, funcionalidad y condiciones de los proveedores) y lo relacionado al tráfico de los flujos de información.

Para la Comisión de Regulación de Telecomunicaciones de Colombia (**REGULATEL**), www.regulatel.org/, la seguridad es el tema de interés.

La Unión Internacional de Telecomunicaciones (**UIT**). www.itu.int/es/about/Pages/default.aspx, trata de englobar todos los conflictos como el órgano máximo en materia de telecomunicaciones. Y se encauza primordialmente en los problemas del sistema de nombres de dominio.

"La Organización para la Cooperación y el Desarrollo Económico (OCDE) es una de las organizaciones más activa, puesto que aborda en términos generales la problemática del ciberespacio, esto es, desagrega todos los componentes del fenómeno y los estudia por partes y por países, identifica los puntos clave, elabora propuestas y las ofrece a sus países miembros".[111]

Respecto del comercio electrónico, el documento fundamental de ordenación lo constituye la Ley Modelo de las Naciones Unidas para el Derecho Mercantil (**CNUDMI**), www.uncitral.org, en virtud de que es una de las áreas con mayor avance. Ésta legislación contempla la estipulación y la importancia y trascendencia que tiene el comercio electrónico y su regulación.

También la Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (**AHCIET**). www.ahciet.net/. Incluye dos características para encuadrar el marco regulatorio de Internet: 1. principios que definan el marco de Internet y los servicios,

[111] Villanueva Romero, Sandra, "*La Organización Internacional ante el Derecho y Regulación del Ciberespacio, inserción de México en la Internet"*, Facultad de Ciencias Políticas y Sociales, UNAM, México 2001.

y 2. acceso y servicios ofrecidos. Ya que es importante tener una noción clara de lo que se debe regular y por qué.

"A partir del año 2004 la Organización de las Naciones Unidas (ONU) llevó a cabo un Foro para la gobernabilidad de Internet".[112] Para dilucidar la gobernabilidad y la regulación adecuada de Internet, así como asegurar que los modelos de gestión de este nuevo medio sean 'incluyentes y participativos'. Se reflexionó sobre el increíble potencial que tiene Internet, no sólo como un instrumento de intercambio y de comunicación humana, sino en el desarrollo social y económico.

"En lo que respecta a latinoamericana se realizó la Conferencia del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC)".[113] www.lacnic.net. Organización que dispone y gestiona los recursos de Internet en América Latina y el Caribe en donde se hizo un debate que perfeccionó con un llamado a la mayor internacionalización de los gobiernos de la red de intercomunicación electrónica. Se esclareció que no existe un 'gobierno de Internet' ya que Internet es absolutamente ingobernable como un todo', y existen muchísimos y muy diversos aspectos vinculados a la red que se discuten en varios ámbitos y organizaciones, y otros que están especificados por regulaciones internacionales y legislación locales.

Por lo tanto se determino que no hay una organización o un único ámbito para los múltiples aspectos relacionados a la red (comercio electrónico, propiedad intelectual, las comunicaciones, los derechos humanos, la educación, la privacidad y otros), ni un solo u único organismo en donde se tomen decisiones o se fijen o establezcan estándares, por lo tanto, no existe el tan famoso gobierno de Internet.

La Comisión Europea aprobó el día 26 de noviembre de 1997 la propuesta que se hizo respecto de un **Plan de acción para el uso seguro de la red de la Unión Europea,** el plan indica las áreas en las que se considera muy necesaria la aplicación de medidas específicas que acogiesen el apoyo de la Unión Europea.

Entre las áreas de acción figuran las siguientes:

• La creación de una red europea de centros de asistencia para recibir la Información de aquellos usuarios que localicen contenidos en Internet que consideren ilegales.

112 La Crónica de Hoy, 28 de Marzo del 2004.
113 La Crónica de Hoy, 1 de Abril del 2004.

• El desarrollo de sistemas de autorregulación por parte de los proveedores de acceso, proveedores de contenidos y operadores de redes.

• El uso de sistemas internacionalmente compatibles para clasificar y filtrar contenidos y proteger a los usuarios, especialmente a los niños, de contenidos no deseables.

• La aplicación de medidas que incrementen el nivel de alerta de padres, profesores, niños y otros usuarios, y que les ayuden a utilizar las redes de manera selectiva, escogiendo los contenidos más apropiados y ejerciendo un nivel razonable de control.

Business Software Alliance (BSA). www.bsa.mx/**.** Es la organización que ha logrado sobresalir sobre todo por promover y promocionar un mundo en línea que sea seguro y legal. Los miembros de BSA representan a las industrias de más rápido crecimiento en el mundo. Fue instituida en el año de 1988, BSA tiene programas en más de 60 países, incluido dentro de estos México. Uno de los temas más relevantes para la BSA es el fomentar una fuerte protección y tutela de la propiedad intelectual esto por medio del establecimiento y la ejecución de las leyes.

Considerando que el software es uno de los pilares tecnológicos más apreciados dentro de la era de la información, puesto que rige el funcionamiento del mundo de los ordenadores y de Internet, por tal virtud y por la habilidad con la que se pueden crear copias idénticas de los programas en tan solo cuestión de unos segundos, la piratería de los programas de computación denominado software se encuentra muy ampliada. Los piratas cibernéticos no sólo dañan y perjudican a las compañías que elaboran los software, sino que, al no ser posible recapitalizar el dinero que éstas obtienen para la investigación y desarrollo de nuevos programas mucho más avanzados, quienes no obtienen un mejoramiento del producto son todos los usuarios. Por esta razón, cualquier tipo de piratería de software (incluso una réplica de un programa para un amigo) se consideraría ilegal.

La Business Software Alliance y el Instituto Mexicano de la Propiedad Industrial (**IMPI**) www.tumarca.com.mx/, ésta última una institución mexicana informaron que se intensificarían los operativos para el combate efectivo de la piratería de software en todo el país para el año 2003.

Esto mediante el marco de una campaña llamada 'Cero Tolerancia', la BSA y el IMPI harán uso de todas las herramientas legales de las cuales pueden disponer para cumplir una intensa y amplia comprobación de la legalidad del software utilizado y vendido y distribuido

por todas las empresas del país. Se llevarán a cabo acciones legales contra miles de empresas en todo México sin distinción alguna del tamaño o giro que sustenten.

A pesar de la laguna legal que existe sobre este tema y que por tanto devela la inexistencia de un centro de control directo sobre el Internet podemos hacer evocación de múltiples organizaciones que si bien son privadas, y responden primordialmente a intereses no lucrativos, y han determinado indiscutibles reglas que son muy específicas sobre el uso de Internet determinando con esto un sistema de complicados controles recíprocos; y por otro lado es importante resaltar que las leyes que de ellas emanan tienen un origen eminentemente contractual y podrían ser esgrimidas desde otra perspectiva, sin embargo dada su relevancia se ha determinado incorporarlas en el presente trabajo.

3.5 ORGANIZACIONES NO GUBERNAMENTALES

Las Organizaciones No Gubernamentales que han instituido normas para el uso de Internet son:

ISOC (Sociedad de Internet). www.internetsociety.org/es. Es una organización establecida por profesionales que son grandes expertos en Internet, quienes aconsejan y evalúan las políticas y las prácticas que deben de ser adoptadas, y trabajan supervisando a otras organizaciones. Está incorporada por más de ciento setenta y cinco organizaciones y ocho mil seiscientos miembros, que corresponden a ciento setenta países del mundo. Su trabajo está fundamentado en cuatro pilares básicos: las normas, la política pública, la educación y entrenamiento y la membrecía.

IAB (Plantel de arquitectura de Internet). www.iabmexico.com/. Sus encargos van a incluir lo siguiente: a) el cuidado de la arquitectura: para los procedimientos y procesos que son utilizados en Internet y b) actuar como un consejo de apelación para resolver controversias emanadas de la ejecución inadecuada de los procesos de los estándares.

ISTF (Fuerza social de Internet). istf.ucf.edu/. Es una organización abierta de personas a quienes se les encomienda la ejecución y la misión de la ISOC es decir, aseverar un abierto desarrollo, y evolución en el uso de la Internet, para el beneficio de toda la gente alrededor del mundo. Esta organización se va a encargar de implementar la manera de beneficiar al máximo la Red a nivel mundial; para ello caracteriza las dificultades sociales y

económicas vinculándolas con el progreso y la utilización de la red, como la identificación y descripción de contextos locales, regionales y globales para ayudar al uso y la disponibilidad de Internet.

IANA (Autoridad de Asignación de Números de Internet). www.iana.org/. La sede la podemos localizar en el Instituto de Ciencias del Sur de California, la cual está a cargo de todos los parámetros originales de Internet, incluidas las direcciones (IP). La IANA es la autoridad encargada de: a) la vigilancia del alojamiento de las direcciones IP; y b) se encarga de la designación y asignación de los dominios en la red.

No obstante, con todo esto es substancial el remarcar que no se puede asimilar este control a un control en términos meramente políticos y jurídicos sino más bien en términos económicos y técnicos. Esto nos lleva a comprender que los únicos controles que se realizan en cuanto a Internet se refiere, son los hechos por empresas especializadas u organizaciones y estos generalmente hacen referencia a aspectos de carácter tecnológico o política de expansión, entendida primordialmente en términos comerciales y por tanto de mercado.

En este sentido, es trascendental cuestionarnos si es o no posible el regulamiento del Internet a nivel internacional, en virtud de que este ha crecido y se ha desarrollado al margen de toda legislación, su carácter a territorial que no respeta los límites fronterizos, así como las normas locales o estatales y lo cual nos pone frente a un mundo libre e intercomunicado sin ningún tipo real de restricciones, limitantes ni censuras.

Si concebimos lo anterior es posible que podamos estar a favor de la autorregulación que pueda generarse respecto de esta materia, empero un fenómeno de tal dimensión pensamos que es necesario que se atienda y conciba a nivel internacional bien para establecer que significa Internet para el mundo, y cuáles son sus ventajas y desventajas, y cuál es el compromiso de nosotros como usuarios y ver que si no se busca regular en la materia estos no tienen ninguna garantía sobre lo que se hace, ve y transfiere en Internet y por tanto no tienen ante quien plantear una denuncia o una queja o inconformidad.

El mecanismo jurídico-político que debe ofertarse como ya se aludió son los Tratados Internacionales, puesto que hasta el momento es la vía más idónea para buscar regular el Internet.

La comunidad internacional no ha planteado una postura significativa que precise el compromiso por afrontar esta materia de manera vinculada y responsable que pueda favorecer

al establecimiento de una determinada legislación, no obstante, si ha hecho alusión a la necesidad de instaurar la Sociedad de la Información, está comprendida como un reto global para el nuevo milenio en la cual el acceso a la Internet y a todos los recursos que se desprenden de él es un tema de relevancia primordial.

CAPÍTULO CUARTO. LA INCORPORACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL DE MICHOACÁN.

4.1 PLANTEAMIENTO DE LA INVESTIGACIÓN

A fin de dar una mayor certeza jurídica a todos los usuarios del internet que son víctimas de fraudes electrónicos, falsificación informática, daños o modificaciones de programas o datos computarizados, es necesario incorporar a la legislación michoacana un catálogo de de delitos cibernéticos.

Se justifica ampliamente la necesidad de incorporar los delitos cibernéticos al código penal en el Estado de Michoacán, bajo la premisa de que cada vez son más los afectados por particulares u organizaciones que se dedican a delinquir en el ciberespacio, ante la ausencia de una normatividad que sancione todas esas conductas; se genera una gran incertidumbre y fomenta cada vez más el sentimiento de impunidad en el usuario del internet desvirtuándose su naturaleza, como una herramienta de comunicación, difusión, comercio y servicio.

Por lo que debemos conocer los conceptos básicos para entender qué es el internet, cuál es su alcance y sus efectos en la sociedad; así como los principios que rigen para los usuarios de ese medio de comunicación.

Delimitamos los antecedentes y qué conductas deberán de incorporarse como delitos cibernéticos, a partir de los bienes jurídicos que se buscan tutelar, como la intimidad, la información y el patrimonio.

Planteamos el marco legal nacional e internacional para determinar que conductas deben ser tipificadas como delitos cibernéticos, y cómo se han sancionado.

Demarcamos la competencia y jurisdicción de los delitos cibernéticos.

Comparamos los cuerpos normativos de otras entidades que tienen una legislación específica sobre delitos cibernéticos a nivel Nacional, Latinoamérica e Internacional.

Establecimos la imperante necesidad de un catálogo de delitos cibernéticos en el Código Penal del Estado de Michoacán.

4.2 COMPROBACIÓN DE LA HIPÓTESIS

"Los Delitos Informáticos", son las conductas ilícitas que van a ser susceptibles de ser incorporadas y sancionadas por el derecho sustantivo penal y que en su ejecución se valen de las computadoras como medio o fin para su comisión".

En México no se cuenta con una amplia legislación que verse sobre los delitos Informáticos, por lo que las conductas ilícitas que se realizan quedan en su gran mayoría impunes y, nuestro Estado no queda exento de ello.

Una de las cuestiones fundamentales que debemos tomar en consideración para prevenir y sobre todo combatir los delitos informáticos es la capacitación y actualización adecuada de todos los "Legisladores" tanto en la esfera Federal como en la Local, puesto que las innovaciones tecnologías avanzan cada vez con mayor rapidez, involucrando ramas tan trascendentales en el devenir diario como son: La Cibernética, La Informática y, lo que nos ocupa, el Derecho.

Hemos observado que el legislador debería de contar con toda la educación que le pueda ofertar el Derecho Informático, campo que nos es básico para nuestra actividad diaria; y que esos conocimientos más la realidad social que tenemos, es lo que se pretende regular; debemos de formar una legislación ajustada en torno a toda la problemática del derecho y crear figuras delictivas apropiadas tanto a nivel Federal como Estatal; hay que hacer la connotación de que hay materias en que el legislador local no puede tener injerencia, como serían los delitos patrimoniales vinculados con las Instituciones financieras y de crédito, y la confidencialidad de la información, así como los delitos contra la delincuencia organizada. Es muy conveniente que se limiten las respectivas competencias y que se legisle en materia local los ilícitos informáticos, sin afectar obviamente a la exclusividad federal.

Dentro de la legislación sustantiva penal debe precisarse claramente la clasificación de los delitos informáticos en base a los bienes jurídicos que se pretenden tutelar o proteger, que serían la Información, la intimidad y la confidencialidad, el patrimonio y la seguridad nacional, ya sea cuando se hace mención a la confidencialidad de la información contenida en los medios informáticos en relación a la protección de éstos medios informáticos; o bien, cuando se refieren a los sistemas de cómputo como medio o instrumento para cometer delitos.

Se deben instituir políticas muy especializadas y precisadas por los medios informáticos por medio de los cuales se pueden cometer delitos informáticos, por lo que deberán estar vinculados los tres poderes del Estado, el Ejecutivo, el Legislativo y el Judicial.

Debemos incorporar como delitos cibernéticos en nuestra legislación penal local a todos aquellos que hemos analizado en capítulos antes expuestos, a partir de los bienes jurídicos que se buscan tutelar.

Se ha demostrado la necesidad de establecer la competencia local y la jurisdicción de los delitos cibernéticos.

Y comprobamos la imperante necesidad de un catálogo de delitos cibernéticos en el Código Penal del Estado de Michoacán.

4.3 PROPUESTAS

PRIMERA. Considero sumamente importante proteger **el Derecho a la Intimidad o a la Confidencialidad,** el cual tiene dos acepciones en la informática y en la telemática, por un lado en sentido "estricto sensu" que se refiere a la información sensible que es el nombre, el domicilio, el origen racial, la preferencia sexual, las creencias religiosas; información que no puede ni debe ser procesada electrónicamente y por el otro lado, el manejo y registro de información pública, que es el que analizaremos y se encuentra contemplado en el artículo 6 Constitucional; de igual forma la Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo, prevé cuál información debe ser enterada de oficio por las entidades públicas; que información debe ser clasificada como confidencia y bajo qué criterios podrá clasificarse la información como reservada de o en posesión de las entidades públicas.

La Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán y su Reglamento, al enterar de oficio la información pública, a través de su sitio web *http://www.congresomich.gob.mx/Modulos/mod_Biblioteca/archivos/373_bib.pdf*; así como también viene dando respuesta y proporcionando la información que le es solicitada y que no está considerada restringida.

Que el artículo 45 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo dispone: Se considera información reservada, la así clasificada mediante acuerdo del titular de cada uno de los sujetos obligados, previo dictamen de procedencia emitido por el Instituto; en este orden de ideas el numeral 46 de la Ley en cita. El numeral 54 de la Transparencia y Acceso a la Información Pública del Estado determina que: La información que contenga datos de carácter personal debe sistematizarse con fines lícitos y legítimos. La información necesaria para proteger la seguridad pública o la vida de las personas, su familia o patrimonio no deberá registrarse ni será obligatorio proporcionar datos. El dispositivo 47 de la ley en comento señala el acuerdo que clasifique información como reservada debe demostrar que:

I. La información encuadra en alguna de las hipótesis de excepción;

II. La publicidad de la información puede amenazar el interés protegido por la Ley; y,

III. El daño que puede producirse con la publicidad de la información es mayor que el interés público de conocerla.

Por lo expuesto observamos que esta ley Estatal en los artículos 1, 44, 45, 46, 47, y 53 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo; 1, 2, 39, 40, 41, 43, 51, 52 y 54, del Reglamento de la Ley de Transparencia y Acceso a la Información del Poder Ejecutivo del Estado de Michoacán de Ocampo, protegemos ampliamente el bien jurídico de tutela que es la **"Intimidad"**; cabe hacer la precisión que el numeral 54 de la ley en comento dice: que La información que contenga datos de carácter personal debe sistematizarse con fines lícitos y legítimos. La información necesaria para proteger la seguridad pública o la vida de las personas, su familia o patrimonio no deberá registrarse ni será obligatorio proporcionar datos.

Pero no menciona de qué forma se protegerá esta información sistematizada en la ley antes analizada. El Derecho a la Intimidad o privacidad de las personas, es una hipótesis que no se ha contemplado respecto de las computadoras y el internet, ya que no sólo las personas físicas cuentan con información en sus bases de datos información confidencial, sino también las Empresas particulares y, de igual forma, las Instituciones públicas, evadiendo contraseñas e introduciéndose al sistema informático sin la autorización de su creador o de mandamiento judicial.

La propuesta que intento es adicionar en la Ley de Transparencia y Acceso a la Información del Poder Ejecutivo del Estado de Michoacán de Ocampo, el artículo 112 la fracción I para incorporar la fracción I bis: "cuando una o varias personas se introduzca o use un sistema de red o de computadoras sin tener derecho a ello, con el objeto o fin de obtener de manera dolosa información pública que se encuentre bajo custodia o reservada".

CAPÍTULO DÉCIMO PRIMERO

RESPONSABILIDADES Y SANCIONES ADMINISTRATIVAS

ARTÍCULO 112.- Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en esta Ley, las siguientes:

I. Usar, sustraer, ocultar, inutilizar, divulgar o alterar, total o parcialmente de manera dolosa la información pública que se encuentre bajo custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
II. Actuar con negligencia, dolo o mala fe en la atención de las solicitudes de acceso a la información pública o en la difusión de la información pública a que están obligados conforme a esta Ley;
III. Denegar intencionalmente información pública no clasificada como reservada o no considerada confidencial conforme a esta Ley;
IV. Clasificar como reservada o confidencial, información pública que no cumple con las características señaladas en esta Ley;
V. Entregar información clasificada como reservada o confidencial;
VI. Entregar dolosamente de manera incompleta información pública requerida en una solicitud de información;
VII. No proporcionar la información pública cuya entrega haya sido ordenada por la autoridad correspondiente; o,
VIII. Demorar injustificadamente la entrega de información pública solicitada.

SEGUNDA. Por lo que agregaría también el Capítulo I del Título Décimo Tercero del Código Penal del Estado de Michoacán, se pudiese adicionar el final del mismo, como Delito contra la Libertad y Seguridad de las Personas una cuestión referente a la informática, tomando como base lo siguiente:

Será estimado como Delito contra la Libertad de las Personas:

"Cuando un individuo almacene, comunique, modifique o cancele un proceso de una base de datos a partir de registros informatizados con datos personales, sin la autorización de su autor o de mandato judicial, deberá sancionársele con la penalidad de 1 uno a 4 cuatro años de prisión y multa de cien a quinientos días de salario al momento en que se haya cometido el delito".

A manera de explicación, consideré que debería señalar esta hipótesis por principio, en este Título Décimo Tercero de los Delitos contra la Libertad y Seguridad de las Personas, en virtud, de que los delitos informáticos van más allá de una escueta violación a los derechos patrimoniales de las víctimas, pues debido a las diferentes formas de comisión de éstos, no solamente se dan las lesiones de esos derechos sino otros, como son el Derecho a la intimidad o privacidad de las personas.

Lo más sustancial sería que se proteja la base de datos que pudiera tener una persona, ya que ésta es sumamente confidencial, el que agredería el bien jurídico tutelado de la privacidad e intimidad y, por las características de dicha conducta, pueden provocar múltiples pérdidas económicas, con o sin beneficio para los que realizan la conducta ilegal; en la mayoría de los casos, es una conducta que se realiza con la intención de transformar o difundir una información contenida en una base de datos; siendo trascendente señalar que son muchos los casos en que se produce este tipo de conductas, por lo que considero apropiada la penalidad que pretendo en dicha hipótesis. La imposición de sanciones mayores no desalienta la comisión de estos delitos, es por ello que sancionar con una pena, no va a implicar que el sujeto suprima la realización de su conducta e intente hacerlo de nuevo, pero si es sabedor de que será una pena, además de una reparación del daño que será indudablemente mayor, que el beneficio que haya obtenido de su conducta, se limitara, o lo pensara un poco más.

TERCERA. Uno de los bienes jurídicos tutelados más vulnerados es el del "Patrimonio", puesto que el objetivo para el sujeto activo en este tipo de ilícitos es el detrimento patrimonial de sus víctimas; estos delitos se realizan con más frecuencia en virtud de que no van a la par los avances tecnológicos respecto de la regulación de los mismos y éstas conductas son facilísimas de cometer para los Hackers y los Crackers y muy difíciles de descubrir. Muchos de los Fraudes y de los Robos son cometidos mediante la manipulación de los equipos de cómputo y son normalmente acciones de oportunidad del sujeto activo, ocasionando pérdidas económicas cuantiosas y convirtiéndose automáticamente en beneficios para los delincuentes.

Son conductas que no exigen una presencia próxima a su objetivo ilícito, se consuman de forma inmediata, son muy sofisticados los conocimientos que tiene que tener el delincuente

y son muy difíciles de comprobar los delitos causando un fenómeno que en México no nos es nada desconocido, "La Impunidad".

Quiénes son más atacados por este tipo de ilícitos y sufren mayores daños patrimoniales, son Las Instituciones Financieras y de Crédito por lo que ya han tomado acciones para defenderse e incluso, la Suprema Corte de Justicia de la Nación vio el problema tan álgido, que resolvió que: sólo el Congreso de la Unión puede legislar en cuestiones de fraude por acceso informático al sistema financiero, lo que a mi muy particular punto de vista, causa imprecisión en el ilícito, puesto que no en todos los casos sería fraude, sino que puede ser robo, porque no se puede nunca engañar a un sistema de cómputo, pues esto sólo es susceptible para los individuos y el Legislador debería tomarlo en consideración.

También quienes sufren daños patrimoniales multimillonarios son los llamados "Derechos de autor" y "La Propiedad Intelectual", mismos que son fundamentales para el desarrollo creativo, Tecnológico y económico de las Naciones.

Por lo que propongo que se adicione en:

EN EL TÍTULO DÉCIMOOCTAVO DE LOS DELITOS CONTRA EL PATRIMONIO EN EL CÓDIGO PENAL DEL ESTADO:

I. Al que sin autorización conozca, copie, utilice, altere o dañe Información personal, íntima o confidencial contenida en Sistemas o Equipos de Informática se le impondrá de 1 uno a 4 cuatro años de prisión y de doscientos a cuatrocientos días de multa.

II. Cuando una persona se introduzca o use un sistema o red de computadoras sin tener derecho a ello, con el objeto de obtener un lucro indebido, o información delicada. Igualmente al que altere el funcionamiento de sistemas informáticos o telemáticos procurando una ventaja injusta, causando daño a otro.

III.- Al que de forma dolosa causen perjuicio a un soporte lógico, sistema de red de computación o los datos contenidos en la misma, o introduzca virus que causen daños al sistema ya sea bloqueando, modificando o destruyendo datos o dañando el hardware.

Al responsable de estos delitos se le impondrá una sanción de 3 tres a 8 ocho años de prisión y multa de cien a quinientos días de salario mínimo vigentes en el momento de la comisión del delito.

CUARTA. Otro de los bienes jurídicos tutelados en el Delito Informático es uno de los más vulnerados en nuestro país y es el de Seguridad Nacional; esto a raíz de la denominada delincuencia organizada que es la que se encarga del control de los ilícitos que con más frecuencia se presentan en el Internet, que son: el terrorismo, el fraude a Instituciones Bancarias, la prostitución de adultos y más de menores, el narcotráfico e inclusive las formulas para la elaboración de estupefacientes, cabe precisar que a raíz de las reformas del 18 de Junio del 2008, la delincuencia organizada quedó indebidamente legislada en la Constitución Política de los Estados Unidos, cometiendo un error en técnica legislativa, pues ninguna constitución debe tener tipicidad en ella. Pero fue la única salida que encontró el Constituyente para atacar a este tipo de delincuencia.

QUINTA. Hay delitos que, como hemos examinado en el párrafo anterior, son más susceptibles a que se realicen mediante, o como instrumento sistemas o equipos informáticos para realizar otro ilícito y son los que controla la delincuencia organizada y son también "Delitos Informáticos"; en los cuales podemos hacer adiciones para mayor protección en el Estado.

CAPITULO II

PORNOGRAFÍA Y TURISMO SEXUAL DE PERSONAS MENORES DE EDAD O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA COMPRENDER EL SIGNIFICADO DEL HECHO

PORNOGRAFÍA INFANTIL

Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos, promoverlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en sistemas o equipos informáticos, electrónicos o o de

cómputo, en la red pública o privada de telecomunicaciones. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, videograbe, fotografié, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad.

La misma pena se impondrá a quien reproduzca mediante cualquier Sistema o equipo informático, electrónico o de cómputo, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

TURISMO SEXUAL

Comete el delito de turismo sexual quien promueva, publicite, condicione, invite, facilite o gestione mediante cualquier Sistema o equipo informático o electrónico o de cómputo o por cualquier medio a que una o más personas viajen al interior o exterior del territorio nacional con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de dieciocho años de edad, o con una o varias personas que no tienen capacidad para comprender el significado del hecho o con una o varias personas que no tienen capacidad para resistirlo.

Al autor de este delito se le impondrá una pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

SEXTA. Otra propuesta que considero importante es la creación de la Policía Cibernética Estatal, que es uno de los puntos medulares que debemos de tomar en cuenta, y resaltarlos puesto que éstos solo los tenemos a nivel Federal y no son suficientes para tener un debido control de toda la información que tiene la red de redes, Internet, debemos tener personal altamente calificado no sólo en la Federación sino también en los Estados, para auxilio para una mejor persecución del o de los delincuentes, por eso propongo también **la creación de la policía cibernética del Estado de Michoacán.**

Es necesario que México pueda tener el control y la vigilancia de la información e incluso, que tenga la facultad para que pueda bloquear información que atente en contra del Estado. Incorporarse a Organismos Internacionales para llevar a cabo el combate efectivo de la delincuencia tanto organizada como la globalizada, conservando y aplicando siempre y en todo

momento nuestros principios constitucionales y tratados internacionales que México ha suscrito, y sobre todo los relativos a derechos fundamentales.

CONCLUSIONES

PRIMERA. Desde el siglo XX el avance tecnológico ha sido tan impresionante que cosas que podrían considerarse ciencia ficción, son ahora una realidad, por tanto es de vital trascendencia conocer sobre uno de los descubrimientos más increíbles y que ahora se encuentran en casi todos los hogares y que han hecho que la vida del hombre sea algo más fácil, simple y hasta divertido, y es la "Computadora", para ello la describimos internamente (software) y externamente (hardware); y distinguimos ampliamente lo que es la Informática que es la base toral de ésta tesis de grado, diferenciándola de la electrónica y de la cibernética.

Examinamos el surgimiento del internet, como medio de comunicación, como foro de discusión, como mensajería instantánea (e-mail) o (Chat) e incluso como medio de información (periódicos, revistas electrónicas e incluso redes sociales).

SEGUNDA. Vinculamos la Informática a varias ramas del conocimiento iniciando con las ciencias naturales y posteriormente con las ciencias sociales, que son en las que enfocamos nuestro análisis como la educación; el derecho desprendiéndose de ésta el registral, el operacional, la decisional, la jurídica documentaria, el control de gestión, la administración pública, en la jurídica documentaria y otros; exaltamos la importancia del internet en el derecho, tanto en el auxilio de búsqueda y descarga de información, como en herramientas como el correo electrónico (e-mail), para el envió de información jurídica, que ya es parte de nuestro quehacer profesional diario.

TERCERA. La protección de datos personales e institucionales es un tema que tomamos con seriedad, por eso se ha dicho desde siempre que conocimiento es poder, y debe de haber tipos penales que protejan nuestra información y nuestros datos personales: "Información personal" como nombre, edad, domicilio, estado civil, preferencias sexuales, expedientes médicos, cuentas bancarias etc.

CUARTA. Desarrollamos un análisis de la Norma Constitucional y de las Leyes Federales, para poder determinar la incorporación los delitos informáticos en el Estado de Michoacán, separando los que la propia Constitución ya reservo para su competencia a saber:

la delincuencia organizada, el terrorismo y el secuestro; de igual forma la Federación hizo lo conducente para su tutela y protección en las siguientes leyes: Ley de Propiedad Industrial, La Ley Federal de Derecho de Autor, Ley de Instituciones de Crédito, Ley Federal de Telecomunicaciones, Ley Federal de Protección al Consumidor, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de Información y Estadística Geográfica, Ley Orgánica del Poder Judicial de la Federación, Ley Federal contra la Delincuencia Organizada, Código Fiscal de la Federación, Código Penal Federal, etc.

QUINTA. Esbozamos cuántos y cuáles son los tipos de delincuentes informáticos y que características tienen estos delitos, y cuáles son los que reconoce las Naciones Unidas como:

1. Fraude: Datos falsos o engañosos: Caballos de Troya, la Técnica de Salami, Falsificaciones Informáticas, Datos de salida, Phising
2. Sabotaje Informático: Bombas Lógicas, Gusanos, Virus informáticos, Ciberterrorismo, Ataques de denegación de servicio.
3. El Espionaje Informático Robo o Hurto de Software: Fuga de Datos, Reproducción de programas Informáticos de protección legal.
4. El Robo de servicios: Hurto de tiempo de computador, Apropiación de Información Residual, Parasitismo Informático y suplantación de personalidad.
5. El Acceso no Autorizado: Puertas Falsas, Llave Maestra, Pinchado de Líneas, Piratas informáticos.

SEXTA. Determinamos que Bienes Jurídicos lesionan los Delitos Informáticos:

1. Derecho a la Intimidad y Confidencialidad
2. Derecho a la Información
3. Derechos Patrimoniales
4. Seguridad Nacional

SEPTIMA. Después de analizar el Derecho Panorámico Estatal observamos qué delitos son los que más se cometen en México y que se han tipificado, los que son: Acceso Ilícito, Interceptación Ilícita, Interferencia en los Datos, Abuso de dispositivos, Falsificación

Informática, Fraude Informático e Infracciones de la Propiedad Intelectual y los derechos afines.

OCTAVA. Como vislumbramos no sólo a nivel Nacional, sino Internacional, legislar y vigilar no ha sido una función fácil, en tal virtud varios países han intentado censurando el internet e incluso las redes sociales, y han puesto mucha vigilancia a través de sus policías para prevenir el delito, en lo que estoy completamente de acuerdo e incluso, es parte de la propuesta de la presente tesis.

GLOSARIO DE ABREVIATURAS PARA LAS NOTAS AL PIE DE PÁGINA

Abreviatura	Significado
Cfr	Confrontar, Confróntese
comp, comps	Compilador, Compiladores
coord, coords	Coordinador, Coordinadores
ed, eds	editor, editores
et al.	y otros
Ibidem	Mismo autor, distinta página
Ídem	Mismo autor, misma página
No	Número
núm, núms	número, números
Ob. Cit	Obra citada
p, pp	página, páginas
s.a	sin año de publicación
s.e	sin editorial
s.f	sin fecha de edición
s.l.i	sin lugar de impresión
s.p.i	sin pie de imprenta
ss.	Siguientes
t, ts	tomo, tomos
Véase	vér, verificar
vol, vols	volumen, volúmenes

GLOSARIO DE TÉRMINOS

Término	Significado
@ (arroba)	Que en inglés significa "en"
Abaco	Es una palabra latina del griego "abax" o "abakon", que significa "superficie plana" o "tabla".
Abaq	Significa "polvo"
Abstract	Consiste en almacenar los textos Consiste en almacenar los textos complejos de forma lógica a través de restrictores de distancia en el cual puede ser organizado y consultado con mayor facilidad complejos de forma lógica a través de restrictores de distancia en el cual puede ser organizado y consultado con mayor facilidad
Abuso de Dispositivos	Se sanciona a quien de manera deliberada e ilegitima produce, vende, importa, difunde, utiliza u otra forma de puesta a disposición de datos informáticos o con otra pretensión delictiva o, en relación con un sistema informático que esté conectado a otro
Acceso Ilícito	Se define el acceso ilícito como el acceso deliberado e ilegítimo a la totalidad o a una parte del sistema informático, infringiendo medidas de seguridad con la intención de obtener datos informáticos o con otra pretensión delictiva o, en relación con un sistema informático que esté conectado a otro
AHCIET	Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones
Analfabetismo Tecnológico	Privación a las personas de las nuevas tecnologías
Antivirus	Son programas cuyo objetivo es detectar y/o eliminar virus informáticos
APEC	Organización para la Cooperación Económica en Asia/Pacifico

ARPANET	(Advanced Research Project Agency Network) Es una de las redes de internet creada por encargo del departamento de defensa de los Estados Unidos para establecer un importante nexo de comunicación entre los distintos organismos gubernamentales de la Nación
Ataques de Denegación de Servicio	Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios
Attached	Es la posibilidad que ofrece para poder enviar Documentos Adjuntos al correo
Automatique	Proviene del francés, que significa automatización
Automatización	Es un sistema donde se transfieren tareas de producción, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos
Backbone	Se refiere a las principales conexiones troncales de internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países mediante cables de fibra óptica
Ban Tuan o Ban Tien	Significa Abaco en Vietnamita
BANAMEX	(Banco Nacional de México) Institución Bancaria
Banda Ancha	Es la transmisión de datos simétricos por el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva
Banda de Frecuencias	Es la porción del espectro radioeléctrico que contiene un conjunto de frecuencias determinadas
BESTNET	(La mejor red)
BITNET	(Red de bits) La primera red que recibe información en México

BLUE-RAY	También conocido como Blu-ray o BD, es un formato de disco óptico de nueva generación desarrollado por la BDA (siglas en inglés de Blu-ray Disc Association), empleado para vídeo de alta definición y con una capacidad de almacenamiento de datos de alta densidad mayor que la del DVD
BOE	Boletín Oficial Español
BSA	(Business Software Alliance) Es la organización que ha logrado sobresalir sobre todo por promover y promocionar un mundo en línea que sea seguro y legal
Calculadora	Es un dispositivo que se utiliza para realizar cálculos aritméticos
Camera Shy	Es un software el cual consiente acceder a la navegación libre por la red de forma anónima y a través del sistema de encriptación, además de que sus fuentes y ejecutables están aprovechables y disponibles de forma gratuita
CcTLD	(Country code Top Level Domain) Dominio en la Red
CD ROM, Unidades de Disco y DVD	Lectores de discos compactos
Centro Comercial Virtual	Es el lugar virtual en el cual en un solo sitio se ofrecen diferentes productos por zonas específicas dentro del mismo sitio, este modelo es utilizado por las cadenas comerciales y constan con las mismas garantías y seguridades que ofrecerían una tienda departamental de la misma cadena, como Liverpool
CERN	Centro Europeo para la investigación Nuclear
Certificado	Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica
Chat	Es una comunicación escrita realizada de manera instantánea mediante el uso de un software y a través de internet
Choreb	Significa Abaco en Armenio
Ciberterrorismo	Terrorismo informático es el acto por medio del cual se pretende desestabilizar un país o aplicar presión a un gobierno

Cintas Magnéticas	Son cintas adheridas que contienen información del usuario como las encontradas en las tarjetas de crédito
Circuito	Es una red eléctrica, una interconexión de dos o más componentes tales como resistencias, inductores, etc., que tiene al menos una trayectoria cerrada
CITYBANK	Nombre de una Institución Bancaria
CLI	Cyberspace Law Instituto (Instituto de Derecho en el ciberespacio)
CNUDMI	Ley Modelo de las Naciones Unidas para el Derecho Mercantil
Codificación	El término codificación es tanto la acción de codificar, es decir, de transformar un contenido a un código
Computer Misuse Act	Que es la Ley de Abusos Informáticos
Comunicación Vía Satélite	Es por medio de las ondas electromagnéticas que se transmiten gracias a la presencia en el espacio de satélites artificiales situados en órbita alrededor de la Tierra
CONACYT	Es el Consejo Nacional de Ciencia y Tecnología
Contrato Electrónico de Arrendamiento	Este aplica principalmente en los equipos de cómputo así como accesorios y elementos periféricos de tales equipos, el cual es fundamental fijar el nombre y modelos de los equipos descripción, renta que no necesariamente puede ser mensual, duración término y condiciones del contrato
Contrato Electrónico de Servicios Electrónicos	Este contrato se asemeja al contrato de prestación de servicios profesionales, que consiste en el servicio que ofrece un profesional a una persona denominada cliente el cual está obligado al pago de una llamada retribución
Correo Electrónico (e-mail)	Es la comunicación a través de foros de discusión, servidores de lista y mensajeros instantáneos
Coulba	Significa Abaco en Turco
Cyber-Court	Cibertribunal

Cybernetics, or control and communication in the animal and machina	Cibernética o el control y comunicación en animales y máquinas
Data diddling	Conocidos también como introducción de datos falsos, esta es una manipulación de datos de entrada al computador con el fin de provocar o alcanzar movimientos falsos en las transacciones que tiene una empresa, este tipo de fraude informático es denominado como manipulación de datos de entrada
Datos de Creación de Firma Electrónica	Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante
Datos Personales	Cualquier información concerniente a una persona física identificada o identificable
Delincuencia Organizada	Se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia
Derecho	El conjunto de normas jurídicas que tienen por objeto regular la conducta humana
Derecho Privado	Es aquel que regula las relaciones entre los particulares
Derecho Público	Es aquel que regula las relaciones entre el Estado y los particulares
Destinatario	La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje
Dispositivos Móviles Inalámbricos	También conocidos como computadora de mano, son aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a

	cabo otras funciones más generales
Documentos	Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico
Documentos Electrónicos o Informáticos	Son el conjunto de impulsos electrónicos o lumínicos que se encuentran almacenados en soportes de la misma naturaleza, los cuales para ser leídos son necesarios la traducción hecha por una computadora para que esta pueda ser entendida por el hombre, otra connotación más fácil de entender sobre los documentos electrónicos son todos aquellos documentos creados por el hombre de manera directa o indirecta encontrados en soportes informáticos
DOF	Diario Oficial de la Federación
E-Books	Libros Electrónicos
El Acceso Remoto a Sistemas y Bases de Datos	WI-FI
El Comercio Electrónico	Se entiende como la compraventa de productos realizada a través de la Internet, con la que debe de contar con diferentes fases, la primera consiste en la entrada de paginas especializadas en el comercio electrónico, la segunda fase consta en la manifestación de la voluntad de comprador en adquirir el producto en cuestión, la tercer fase es la aceptación por el vendedor al extender la orden de compra, por último el comprador realiza el pago, se realiza la entrega y se extiende recibo por la compra

El Contrato de Compra-venta en Internet	En el contrato de compraventa a través de la Internet interviene la manifestación de voluntades que son la oferta y la aceptación
El Cracker	Son los más peligrosos en el mundo de la informática, en muchos casos son Hackers al mismo tiempo, poseen gran capacidad de programación, amplios conocimientos en criptografías y criptoanálisis
El Fax	Es la transmisión telefónica de material escaneado impreso, tanto texto como imagen
El Hacker	Es el Intruso o Pirata informático son los mismos programadores o personas que sólo se dedican a cometer ilícitos con las computadoras, o bien persona experta en una rama de la informática y las telecomunicaciones como: programación, software, hardware
El Hardware	Son los componentes físicos y materiales, en conjunto o separados, electrónicos, electromecánicos o mixtos, que compone el equipo lógico e informático en una computadora
El Internet	Es un conjunto de servidores conectados entre sí mediante un sistema maestro de computadoras dentro de una red alrededor de todo el mundo
El Lamer	Son personas que no poseen el gran conocimiento, por lo regular sus ataques son por diversión y presumir sus pocas habilidades
El Malware	Es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos
El Microprocesador	Es el circuito integrado central y más complejo de un sistema informático, se le suele llamar cerebro

El Phreaker	Son los usuarios que realizan actividades ilegales para enriquecerse, destruir o actos terroristas contra equipos informáticos, sólo atacan sistemas de telefonía fija o móvil celular, televisión de paga para obtener servicio gratuito mediante tecnología de avanzada comprada o creada por ellos mismos, después se enfocaron en el robo bancario por medio de tarjetas de crédito, o incluso de crear números de cuentas usando programas originales de las empresas de tarjetas de crédito y siempre son auxiliados con grandes sistemas de cómputo armados por ellos mismos
El Portal Comercial	Es un sitio en donde se presentan diversos servicios que no son necesariamente es compra-venta de productos, estos servicios pueden ser juegos, comunicación, descarga de programas de cómputos, noticias e información de interés, como es más o prodigy
El Rider	Son todos los usuarios que dejaron prácticas ilícitas y trabajan para empresas de seguridad informática, gobiernos y empresas para emplear sus conocimientos y capacidades como especialistas en la seguridad
El Sabotaje Informático	Es el acto por medio del cual se borran, suprimen o modifican sin autorización funciones o datos de computadora con la intención de obstaculizar el funcionamiento normal del sistema
El Script-Kiddie	Son personas que se consideran Crackers, pero poseen menores conocimientos que los mismos, presumen de sus conocimientos utilizando programas de terceros para hacer daño que en la mayoría del caso son el reflejo de actos de vandalismo
El Software	Es la parte intangible de una computadora como un conjunto de instrucciones con las que el usuario y el sistema informativo interactúan para realizar determinadas tareas
El Speaker	Considerado como el máximo espía de la informática; son usuarios con grandes conocimientos y capacidades, son relativamente indetectables debido a que no provocan daño, sólo cuando es realmente necesario, generalmente trabajan para organismos

	gubernamentales
El Transistor	Es un dispositivo electrónico, semi conductor que cumple funciones de amplificador, oscilador, conmutador o rectificador
El Wracker	Shareware o Freeware navegando por Internet, en muchos casos no poseen conocimientos amplios sobre informática y llegan a causar daño sin querer y en otros casos lo hacen sin saber
Emisor	Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario
Empresa Compuserve	Empresa de capitales alemanes y norteamericanos que brindaba desde sus servidores en Alemania acceso mundial a varios sitios de contenidos pedófilos
ENIAC	(Electronic Numerical Integrator And Computer)
Espectro Radioeléctrico	Es el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz
Estación Terrena	Es la antena y el equipo asociado a ésta que se utiliza para transmitir o recibir señales de comunicación vía satélite
ETA	(EUSKADI TA ASKATASUNA) Es una organización terrorista vasca que se proclama independentista, abertzale, socialista y revolucionaria
European Molecular Biology Laboratory	El primer Laboratorio Europeo de Biología a Molecular
EXCEL	Hoja de Cálculo
Falsificación Informática	Se conoce como tal a forma deliberada e ilegítima, de la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles

Fibra Óptica	Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente por el que se envían pulsos de luz que representan los datos a transmitir
Firma Electrónica	Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio
Firma Electrónica Avanzada o Fiable	Aquella Firma Electrónica o digital que cumpla con los requisitos contemplados en las leyes
Firmante	La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa
Floppy Disck	Son soportes móviles que comprenden tarjetas de memoria
Fraude Informático	En ese contexto se sanciona cualquier introducción, alteración, borrado o supresión de datos informáticos y, cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona
Frecuencia	Es el número de ciclos que por segundo efectúa una onda del espectro radioeléctrico
Full-Text	Que consiste en el almacenamiento del texto en su totalidad en las máquinas
GAFI	Grupo de Acción Financiera
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse
Hard Disck Drive	Disco Duro de la Computadora

Heurística o Método Heurístico	Es el conjunto de procedimientos, técnicas y actividades dirigidas para facilitar el descubrimiento de la verdad
Home Page	Página de Inicio es la manera más fácil en que se puede acceder a información mediante sistemas de búsqueda
Homologación	Acto por el cual la Secretaría reconoce oficialmente que las especificaciones de un producto destinado a telecomunicaciones satisfacen las normas y requisitos establecidos, por lo que puede ser conectado a una red pública de telecomunicaciones, o hacer uso del espectro radioeléctrico
HTML	Lenguaje de Marcación de Hipertextos un método para codificar la información de los documentos y sus enlaces
HTTP	Protocolo de transferencia de Hipertexto que especifica cómo el navegador y el servidor intercambian información en forma de peticiones y respuestas
Hurto del Tiempo del Computador	Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo
IAB	(Plantel de arquitectura de Internet). Sus encargos van a incluir lo siguiente: a) el cuidado de la arquitectura: para los procedimientos y procesos que son utilizados en Internet y b) actuar como un consejo de apelación para resolver controversias emanadas de la ejecución inadecuada de los procesos de los estándares
IANA	(Autoridad de Asignación de Números de Internet). La sede la podemos localizar en el Instituto de Ciencias del Sur de California, la cual está a cargo de todos los parámetros originales de Internet, incluidas las direcciones (IP). La IANA es la autoridad encargada de: a) la vigilancia del alojamiento de las direcciones IP; y b) se encarga de la

	designación y asignación de los dominios en la red
IBM	(Internacional Business Machines) que significa (máquinas de negocios internacionales)
ICRAI	Unidad cuya finalidad y objetivo esencial es el análisis exhaustivo de los sistemas informáticos a través de los sistemas de cómputo forense, por medio de los cuales pueden estudiar los múltiples registros anteriores de las computadoras, y así también llevan a cabo la investigación y reconocimiento de las computadoras que en el momento en que se están utilizando
IFAI	El Instituto Federal de Acceso a la Información y Protección de Datos
IMP	Procesadores de Masaje de Interfaz
IMPI	Instituto Mexicano de la Propiedad Industrial
Indexaconección	En el cual crea una lista y calificando e individualizando la información designado por una o varias palabras o claves numéricas lo que permite su fácil ubicación y consulta
Informática Desicional	La considera la más difícil de comprender debido a que no se busca una "Juscibernética" y no pasar a una automatización de las decisiones, sino en que la misma información proporcione facilidades para evitar trabajo repetitivo al momento de redacción de escritos por medio de formatos preimpresos donde exclusivamente se cambian datos variables, permitiendo al Juzgador ahorro de tiempo y continuar llevando sus labores decisorias
Informática en la Administración Pública	Debido al crecimiento demográfico y económico la Administración Pública ha sido orillada al uso de estas nuevas tecnologías para mejorar la estructura jurídico Administrativo y los sistemas de operación, con el fin de agilizar los trámites, disminuir la burocracia y la corrupción
Informática Jurídica	La técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicable a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de

	información jurídica necesarios para lograr dicha recuperación
Informática Jurídica de Apoyo en la Decisión	Consiste en la interacción hombre-máquina para la toma de decisiones jurídicas y el aprendizaje del Derecho, por medio de proporcionar banco de datos con hechos experiencias e información jurídica. Además de facilitar el trabajo mediante el proporcionamiento de elementos considerados repetitivos y tediosos con lo que permite enfocar a los juristas a realizar trabajo creativo en el campo del Derecho
Informática Jurídica de Ayuda a la Decisión	En este caso los ordenadores facilitan la información adecuada para la toma de decisiones mediante el tratamiento y recuperación de información jurídica, siendo ésta la parte fundamental de la informática jurídica
Informática Jurídica De Gestión	Consiste en todas las facilidades que proporcionan los sistemas informáticos en la organización, administración y control de la información, documentos, expedientes y libros jurídicos mediante programas o sistemas de clasificación, utilizado en el área pública y privada, utilizada en el seguimiento de trámites y procesos, el uso rápido de registros contenidos en base de datos, facilitar actuaciones y actividades administrativas
Informática Jurídica Documentaria	Es la aplicación de métodos y técnicas de la informática en los textos jurídicos a bancos de datos, así como su procesamiento, que para poderlo lograr es necesario la recolección, organización, almacenamiento, recuperación, interpretación, identificación y el uso del documento Jurídico
Informática Operacional	Consiste en facilitar las actividades en las áreas públicas como lo son los juzgados y en el área privada como los consorcios de abogados, permitiendo que las máquinas lleven todas las actividades, el control de asuntos y pleitos, contabilidad y registros
Informática Registral	Consiste en la rapidez y facilidad de accesibilidad a registros públicos en especial, dando como ventajas del recuperar dichos registros de

	papel utilizado y facilitar los trámites
Informatique	Proviene del francés, que significa información
Infracciones de la Propiedad Intelectual y de los Derechos Afines	Se protege aquellas obras literarias y artísticas, así como las interpretaciones y ejecutantes de los fonogramas cuando se cometen infracciones a la propiedad intelectual a escala comercial y por medio de un sistema informático
Inteligencia Artificial	Es la capacidad de razonar de un agente no vivo
Interceptación Ilícita	Se tipifica como delito la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos y, que se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático
Interferencia en los Datos	La interferencia de datos se define como aquella conducta que despliega una persona de manera deliberada e ilegítima para dañar, borrar, deteriorar, alterar o suprimir datos informáticos
Intermediario	En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él
International Nucleotide Sequence Database Collaboration	Base de datos de secuencias genéticas nuevas que está a disposición de las instituciones educativas y el público en general
Inventarios	Es una relación detallada de bienes y existencias de una entidad o empresa, a una fecha determinada
Investigación o Informática Jurídica Analítica	Consta de las elementos matemáticos para aumentar las posibilidades de resultados, pero sin éxito por la complejidad y la ausencia de resultados exitosos. Este tipo de Informática usa las computadoras

	para poner a prueba las hipótesis y teorías
IP	Es una etiqueta numérica que identifica de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red
IPN	Instituto Politécnico Nacional
IRA	Ejército Republicano Irlandés
ISOC	(Sociedad de Internet). Es una organización establecida por profesionales que son grandes expertos en Internet, quienes aconsejan y evalúan las políticas y las prácticas que deben de ser adoptadas, y trabajan supervisando a otras organizaciones
ISP´s	Reguladores de los Proveedores de los Servicios de Internet
ISTF	(Fuerza social de Internet). Es una organización abierta de personas a quienes se les encomienda la ejecución y la misión de la ISOC es decir, aseverar un abierto desarrollo, y evolución en el uso de la Internet, para el beneficio de toda la gente alrededor del mundo
ITAM	Instituto Tecnológico Autónomo de México
ITESM	Instituto Tecnológico de Estudios Superiores en Monterrey
ITESO	Instituto Tecnológico de Estudios Superiores de Occidente
KGB	(Komitet gosudárstvennoy bezopásnosti) Comité para la Seguridad del Estado, fue el nombre de la agencia de inteligencia, así como de la agencia principal de policía secreta de la Unión Soviética
Know-how	(del inglés *saber-cómo*) o Conocimiento Fundamental es una forma de transferencia de tecnología
La Cibernética	Estudio de las analogías entre los sistemas de control y de comunicación de los seres vivos y los de las maquinas y en particular, el de las aplicaciones de los mecanismos de regulación biológicas a las tecnológicas

La Cibernética Jurídica	Los avances en la ciencia nos han llevado a un mundo de maravillas tecnológicas que antes nunca pudieron ser imaginadas, con lo que ha llevado a mejorar la calidad de vida de los hombres en todos sus aspectos y aunque parece difícil de creer y de ciencia ficción, la posibilidad de que en una mañana las computadoras puedan tomar decisiones por sí mismas sin simular los pensamientos humanos ni ser manipulada o la necesidad de intervención humana para lograr complejas decisiones conocido como "Inteligencia Artificial"
La Computadora	Una máquina electrónica análoga y digital, dotado de una memoria de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas
La Eléctrica	Es el flujo de estos electrones generada por una corriente y esta a su vez usada en dispositivos cambian la energía en calor, luz o movimiento
La Electrónica	Es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacio, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos
La Informática	Es una rama del saber humano que se ocupa de todo lo relacionado con las computadoras, su comportamiento, su diseño y desarrollo de todo tipo de programas de computadoras desde los sistemas operativos hasta los más modestos programas de aplicación operación y uso de las computadoras
La Programación	Es el proceso de diseñar, codificar, depurar y mantener el código fuente de programas computacionales
La Robótica	Es una rama de la tecnología que se dedica al diseño, construcción, operación, disposición estructural, manufactura y aplicación de los robots
La Unidad de Entrada	Esta constituida de todos aquellos dispositivos con los cuales se permite ingresar datos e información además del manejo de programas informáticos

LACNIC	Conferencia del Registro de Direcciones de Internet para América Latina y el Caribe
Las Unidades de Salida	Son todos los dispositivos físicos en los cuales permite representar la información susceptible a ser apreciados
Leakage	Fuga de Datos Data, es la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera
Leasing	El arrendamiento financiero o contrato de leasing (de alquiler con derecho de compra) es un contrato mediante el cual, el arrendador traspasa el derecho a usar un bien a un arrendatario, a cambio del pago de rentas de arrendamiento durante un plazo determinado, al término del cual el arrendatario tiene la opción de comprar el bien arrendado pagando un precio determinado, devolverlo o renovar el contrato
Lingüística	Es el estudio científico tanto de la estructura de las lenguas naturales y de aspectos relacionados con ellas como su evolución histórica, su estructura interna así como el conocimiento que los hablantes poseen de su propia lengua
Localización Geográfica en Tiempo Real	Es la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada
Logic Bombs	Bombas Lógicas Es una especie de bomba de tiempo que debe producir daños posteriormente, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño
Los Bienes Informáticos	En el estricto sentido comprenden todo lo que es el Hardware o equipo de cómputo tanto como interno como externo
Los Cassettes	Son cintas magnéticas, el cual su funcionamiento básicamente consistía en que a través de esta cinta plástica queda un registro magnético entre una combinación lógica y ordenada de cargas

	positivas y negativas en audio distribuido según las vibraciones generadas por el sonido.
Los Códigos Impresos o Códigos de Barras	Es un código basado en la representación mediante un conjunto de líneas paralelas verticales de distinto grosor y espaciado que en su conjunto contienen una determinada información, es decir, las barras y espacios del código representan pequeñas cadenas de caracteres. De este modo, el código de barras permite reconocer rápidamente un artículo de forma única, global y no ambigua en un punto de la cadena logística y así poder realizar inventario o consultar sus características asociadas. Actualmente, el código de barras está implantado masivamente de forma global
Los Contratos Informáticos	Son todos aquellos contratos que abarcan transacciones con bienes y servicios mediante la Informática, los objetos de estos contratos son: servicios Informáticos y bienes informáticos que incluyen a los suministros y programas
Los Discos Flexibles o Disquetes	Son relaciones ordenadas de cargas, y son comprendidos como "ceros y unos" en el lenguaje vinario; están procesadas y comprendidas lógicas y matemáticamente a través de una computadora permitiendo reproducir o guardar información.
Los Programas de Aplicación	Estos se encuentran en equipos externos los cuales para realizar su funcionamiento necesitan de estos programas o incluso para interactuar con equipos de cómputo convencional
Los Programas Fuentes o Sistemas Operativos	Los cuales en muchos casos se encuentran integrados en los equipos de cómputo que tienen por objeto el control y el uso de los diferentes componentes que integran el sistema central de una computadora
Los Programas Objetivos	Son todos aquellos que tienen la función específica para satisfacer determinadas necesidades de los usuarios
Los Servicios Informáticos	Son todos aquellos elementos que intervienen en el auxilio de la actividad informática en la vida diaria, estos servicios son la consultoría

	la asesoría o el uso de equipos de cómputo
Los Sistemas Ópticos	Que comprenden los discos compactos CD, DVD, BLUE-RAY
Los Suministros Informáticos	Comprenden todos aquellos elementos que son conocidos como "Consumibles" en las labores informáticas, como papel y los medios magnéticos, tintas, toallas o líquidos limpiadores
Manipulación de los Datos de Salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático.
Máquina Diferencial	Es una calculadora mecánica de propósito especial, diseñada para calcular funciones polinómicas
Memorias USB Flash, SD, Mini SD, Discos Compactos	Unidades de almacenamiento, Micro procesadores y Sistemas de lectores de tarjeta
Mensaje de Datos	La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología
MEX-net	Es el encargado de decodificar, propiciar y contribuir en el desarrollo de internet en México
Microcomputadoras	Es una computadora que tiene un microprocesador y como mínimo algún tipo de memoria semiconductora
Microondas	Se denomina así a las ondas electromagnéticas definidas en un rango de frecuencias determinado
MODEM	Es un dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portadora, es decir es un demodulador
NASA	(National Aeronautics and Space Administration) Administración Nacional de Aeronáutica y del Espacio de los Estados Unidos, que es la agencia gubernamental responsable de los programas espaciales
NCAIR	Nacional Center of Automated Information Research
NCAR	El Centro Nacional de Investigación Atmosférica EE.UU

NIC-México	(El Network Information Center-México) es el Centro de Información de Redes de México, Es la organización encargada de la administración del nombre de dominio territorial (ccTLD, country code Top Level Domain) .MX, el código de dos letras asignado a cada país según el ISO 3166, entre sus funciones están el proveer los servicios de información y registro para .MX así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso
NIP	Número Inter Personal
NPC	Network Control Protocol
NSFNET	(National Science Foundation´s Network) Es la fundación Nacional de la Ciencia de redes y fue el reemplazo de ARPANET
Obra de Autor Anónimo	No hace mención del nombre, signo o firma que identifica al autor, bien por voluntad del mismo, bien por no ser posible tal identificación
Obra de Autor Conocido	Contienen la mención del nombre, signo o firma con que se identifica a su autor
Obra de Seudónimo	Las divulgadas con un nombre, signo o firma que no revele la identidad del autor
OCDE	La Organización para la Cooperación y el Desarrollo Económico
On Line	En línea
ONU	Organización de las Naciones Unidas
Orbita satelital	Es la trayectoria que recorre un satélite al girar alrededor de la tierra
Ordenadores	Es una máquina electrónica que recibe y procesa datos para convertirlos en información útil
OTAN	(North Atlantic Treaty Organization), también denominada la Alianza del Atlántico o del Atlántico Norte es una alianza militar intergubernamental basada en el Tratado del Atlántico Norte firmado el 4 de abril de 1949. La organización constituye un sistema de defensa colectiva en la cual los estados miembros acuerdan defender a cualquiera de sus miembros si son atacados por una facción externa

PAN	Partido Acción Nacional
Parte que Confía	La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica
Patentes	Es un conjunto de derechos exclusivos concedidos por un Estado al inventor (o su cesionario) de un nuevo producto susceptible de ser explotado industrialmente, por un período limitado de tiempo a cambio de la divulgación de la invención
Pentágono	(The Pentagon) Es la sede del Departamento de Defensa de los Estados Unidos. El edificio tiene forma de pentágono, y trabajan aproximadamente 23.000 empleados militares y civiles
Pishing	Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo
Posiciones Orbitales Geoestacionarias	Son ubicaciones en una órbita circular sobre el Ecuador que permiten que un satélite gire a la misma velocidad de rotación de la tierra, permitiendo que el satélite mantenga en forma permanente la misma latitud y longitud
PRD	Partido de la Revolución Democrática
Prestador de Servicios de Certificación	La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso
PRI	Partido Revolucionario Institucional
PRIVACY	Privacidad de las personas
PROFECO	Procuraduría Federal del Consumidor
RAM	(Random Acceses Memory) cuya traducción es (acceso de memoria aleatoria)
Recursos Multimedia	Como su nombre dice se presenta la combinación de textos, medios audiovisuales, medios interactivos, animaciones, audio, video analógico o video digital; las cuales no podrían ser presentadas en muchos casos por medios tradicionales

Red de Telecomunicaciones	Es el sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario
Red Privada de Telecomunicaciones	Es la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red
Red Pública de Telecomunicaciones	Es la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal
RED-MEX	Es el organismo creado y constituido por diversas instituciones académicas que se dedicaba a discutir políticas, estatutos y procedimientos con el fin de reglamentar el desarrollo de las redes de comunicación electrónica en México
REGULATEL	Comisión de Regulación de Telecomunicaciones de Colombia
ROM	(Read Only Memory) cuya traducción es (memoria sólo de lectura)
Salami Technique/Rounching Down	La Técnica de salami produce las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada de transacciones financieras se van sacando repetidamente cantidades de una cuenta y se transfieren a otra
Scavenging	Apropiación de Informaciones Residuales es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado
Schoty	Significa Abaco en Ruso
SCJN	Suprema Corte de Justicia de la Nación
SCT	La Secretaría de Comunicaciones y Transportes

SE	La Secretaría de Economía
Secreto Industrial	Es toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma
Seguridad Nacional	Acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado Mexicano, la gobernabilidad democrática, la defensa exterior y la seguridad interior de la Federación, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado constitucional
Servicio de Radio y Televisión	Es el servicio de audio o de audio y video asociado que se presta a través de redes públicas de telecomunicaciones, así como el servicio de radiodifusión
Servicios de Valor Agregado	Son los que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada
Servidores	Es un programa informático que procesa una aplicación realizando conexiones bidireccionales y/o unidireccionales generando o cediendo una respuesta en cualquier lenguaje
SIDA	Síndrome de Inmuno Deficiencia Adquirida
Sistema de Comunicación Vía Satélite	Es el que permite el envío de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envía de regreso a la Tierra para ser captadas por estación receptora
Sistema de Información	Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos

Sistema Digital	Es un conjunto de dispositivos destinados a la generación, transmisión, procesamiento o almacenamiento de señales digitales. También, y a diferencia de un sistema analógico, un sistema digital es una combinación de dispositivos diseñados para manipular cantidades físicas o información que estén representadas en forma digital; es decir, que sólo puedan tomar valores discretos
Skimming	Es la transferencia de la información de una tarjeta a otra que es falsa
Soroban	Significa Abaco en Japonés
Spear Pishing o Pishing segmentado	Este ataca a grupos determinados, es decir se busca grupos de personas vulnerables
Suan Pan	Significa Abaco en Chino
Superzapping	La Llave Maestra Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador, es como una especie de llave que abre cualquier rincón del computador
Tabla de Logaritmos	Es la representación gráfica del logaritmo, es decir es el exponente de un número al cual hay que elevar la base para obtener dicho número
Tarjetas Perforadas y/o Fotografías Perforadas	Tarjeta la cual pueda guardar de manera automática el registro de las personas censadas mediante perforaciones en los rasgos de las personas
Telecomunicaciones	Es toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos
Telefonía Celular	La telefonía móvil, también llamada telefonía celular, básicamente está formada por dos grandes partes: una red de comunicaciones (o red de telefonía móvil) y los terminales (o teléfonos móviles) que permiten el acceso a dicha red
The Online Ombuds	Cibertribunal

Office	
Tiendas Virtuales	Es el lugar virtual de comercio electrónico debido a que exclusivamente se ofrece el producto y las herramientas de pago por cualquier persona interesada, como de remate
Titular del Certificado	Se entenderá a la persona a cuyo favor fue expedido el Certificado
Toscavenge	Se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos
Transferencia de Datos	Envió de flujo de Datos
Transferencia Electrónica	Se denomina así a la transferencia por medio de un circuito en la relación numérica (razón) entre dos variables cualesquiera del circuito, generalmente la entrada y la salida del mismo
Transmission Control Protocol	(en español *Protocolo de Control de Transmisión*) o TCP, es uno de los protocolos fundamentales en Internet, muchos programas dentro de una red de datos compuesta por computadoras, pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto
Trap Doors	Las Puertas Falsas Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante

Troya Horses	Los Caballos de Troya Es extremadamente difíciles de descubrir y por lo general van a pasar inadvertidos debido a que el delincuente debe tener conocimientos técnicos especializados que son precisos de la informática, este ilícito reside en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas, que consiste en insertar un sin número de instrucciones de computadora de forma encubierta u oculta en los programas informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal
Tschu Pan	Significa Abaco en Coreano
UIT	La Unión Internacional de Telecomunicaciones
UNAM	Universidad Nacional Autónoma de México
UNICEF	(United Nations Children's Fund) Fundación Infantil de las Naciones Unidas
URL	Localizador Uniforme de Recursos, que detalla a cada página de información se asocia a una única y en dónde encontrarla
Virus	Son pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de auto reproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar
WEB	Página de Internet (WWW, World Wide Web) en sus siglas en inglés, creado en 1989 por las investigaciones del Sir Timothy "Tim" John Berners-Lee
WI-FI	Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un Smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica

Wiretapping	Pinchado de Líneas Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora
WORD	Procesador de Palabras

FUENTES DE INFORMACIÓN Y DE CONSULTA

BIBLIOGRAFÍA

1. AGUAYO, Sergio, Chiapas: *Las Amenazas A La Seguridad Nacional*, centro Latinoamericano de Estudios Estratégicos A.C. México Junio de 1987.
2. ALESTUEY Dobón, María del Carmen, *Apuntes sobre la Perspectiva Criminológica de los Delitos Informáticos*, Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.
3. ÁLVAREZ de los Ríos, José Luis, *Delitos Informáticos*, ponencia en las Jornadas sobre Marco Legal y Deontológico de la Informática, Mérida 17 de septiembre de 1997.
4. ANDRADE Santander, Diana, *El Derecho a la Intimidad*, Centro Editorial Andino, Quito –Ecuador, 1998.
5. AZPILCUETA Hermilio, Tomas, *Derecho Informático,* Editorial Abeledo/Perrot, Buenos Aires, Argentina 1996.
6. BAÓN Ramírez, Rogelio, *Visión General de la Informática en el nuevo Código Penal*, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996.
7. BARATTA, Alessandro, *Derecho Penal Mínimo*, Editorial Temis S.A, Santa Fe de Bogotá, Colombia, 1999.
8. BARBIERI, Pablo, *Contratos de Empresa*, Editorial Universidad, Buenos Aires, Argentina, 1998.
9. BARRIUSO Ruiz, Carlos, *Interacción Del Derecho y la Informática*, Editorial Dykinson, Madrid, 1996, pp. 245 a 252.
10. BECCARIA, Alessandro, De los Delitos y las Penas, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1997.
11. BERDUGO Gómez de la Torre, Ignacio, *Honor Y Libertad De Expresión,* Tecnos. Madrid, 1987.
12. BETTIOL, Giusseppe, Derecho Penal, Editorial Temis, Bogotá, Colombia 1990.

13. BUENO Arús, Francisco, *El Delito Informático*, Actualidad Informática Aranzadi Nº 11, abril de 1994.
14. BUSTOS Ramírez Juan, et al, *Derecho Penal Latinoamericano Comparado Parte General*, Buenos Aires, Argentina 1981.
15. CABANELLAS, Guillermo, Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta 1990.
16. CAMACHO Losa, Luis, *El Delito Informático,* Madrid, España 1987.
17. CÁMPOLI, Gabriel Andrés, *Derecho Penal Informático en México,* Editorial INACIPE, México 2004.
18. CANO, Jeimy, *Inseguridad Informática: Un concepto dual de la Seguridad Informática,* Universidad UNIANDES 1994.
19. CARRANCÁ y Trujillo, et al, *Derecho Penal Mexicano (Parte general)*, Vigésima tercera edición, Editorial Porrúa, México 2007.
20. CARRILLO, Marc, *Los Límites A La Libertad De Prensa En La Constitución Española De 1978,* Promociones y Publicaciones Universitarias (PPU).
21. CASTELLANOS Tena, Fernando, *Lineamientos elementales de Derecho Penal. (Parte General),* Cuadragésima séptima edición actualizada por Horacio Sánchez Sodi, Primera reimpresión, Editorial Porrúa, México 2007.
22. CASTILLO Jiménez, María Cinta, et al, *El Delito Informático*, Facultad de Derecho de Zaragoza, Congreso sobre Derecho Informático, 22 al 24 junio 1989.
23. CHOCLAN Montalvo, José Antonio, *Estafa Por Computación Y Criminalidad Económica Vinculada A La Informática*, Actualidad Penal Nº 47, 22-28 Diciembre 1997.
24. CORREA, Carlos, *Derecho Informático,* Editorial Desalma Buenos Aires Argentina 1994.
25. CORREA, Carlos María, *El Derecho Informático en América Latina, Publicado en Derecho y Tecnología Informática,* Editorial Temis, Bogotá, Mayo de 1990.
26. CREUS, Carlos, *Derecho Penal Parte Especial*, Editorial Astrea, Buenos Aires, 1998, Tomo número 2.
27. CUELLO Calón, Eugenio, *Derecho Penal. Parte General, D*écima octava edición, Editorial Nacional, México 1980.
28. CUERVO José, *Delitos Informáticos y Protección Penal a la Intimidad*, Publicación hecha en Internet URL: www.derecho.org.

29. DALLAGLIO, Edgardo Jorge, *La Responsabilidad Derivada de la Introducción y Propagación del Virus de las Computadoras,* Publicado en El Derecho, año 1990.
30. DAVARA Rodríguez, Miguel Ángel, *Análisis de la Ley de Fraude Informático*, Revista de Derecho de la UNAM, México 1990.
31. DAVARA Rodríguez, Miguel Ángel, *De las Autopistas de la Información a la Sociedad Virtual*, Editorial Aranzadi, 1996.
32. DAVARA Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, Editorial Aranzadi, Pamplona, 1997.
33. DONOSO Abarca, Lorena, *Análisis del tratamiento de las figuras Relativas a la Informática tratadas en el título XIII del Código Penal Español de 1995*,
34. FERNÁNDEZ Calvo, Rafael, *El Tratamiento del llamado "Delito Informático,* en el proyecto de Ley Orgánica de Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática), Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.
35. FERREYROS Soto, Carlos, *Aspectos Metodológicos del Delito Informático*, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
36. FÍGOLI Pacheco, Andrés, *El Acceso No Autorizado a Sistemas Informáticos,* Uruguay 1998, Publicación hecha en Internet, URL: http//www.derecho.org.
37. FROSINI Vitorio, *Informática y Derecho,* Editorial Temis, Bogotá, Colombia, 1988.
38. FUMIS, Federico, *Informática y Derecho de Daños*, Boletín Hispanoamericano de Informática y Derecho, 1998, Buenos Aires, Argentina, URL: Http//www.ulpiano.com.
39. GARCÍA Gil, F. Javier, *Código Penal y su Jurisprudencia,* Adaptada a la Ley Orgánica 10/1995, de 23 de noviembre", Editorial Edijus, Zaragoza, 1996.
40. GARCÍA Vitoria, Aurora, *El Derecho a la Intimidad en el Derecho Penal y en la Constitución de 1978,* Editorial Aranzadi, Pamplona–España, 1983.
41. GÓMEZ Perals, Miguel, *Los Delitos Informáticos en el Derecho Español*, Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21 al 25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.

42. GUASTAVINO, Elías P, *Responsabilidad Civil Y Otros Problemas Jurídicos En Computación*, Ediciones La Rocca, Buenos Aires, 1987.
43. GUIBOURG Ricardo, et al, *Manual de Informática Jurídica*, Editorial Astrea, 1996, Buenos Aires, Argentina.
44. GUTIÉRREZ Francés, Mª Luz, *Fraude Informático Y Estafa*, Centro Publicaciones del Ministerio de Justicia, Madrid, 1991.
45. HANCE Olivier, *Leyes y Negocios en Internet,* Editorial McGraw Hill, Sociedad Internet, México 1996.
46. HANSSENER Winfried, *Derecho Penal*, Editorial Azalea, 1998.
47. HASKIN, David, *Multimedia Fácil*, (Traducción. Sánchez García Gabriel), Editorial Prentice Hall, México 1995.
48. HEREDERO Higueras, Manuel, *Los Delitos Informáticos en el Proyecto de Código Penal de 1994*, Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.
49. HERNÁNDEZ Guerrero, Francisco, *Delitos Informáticos,* Ponencia Jornadas sobre el Marco Legal y Deontológico de la Informática, Mérida, 17 de septiembre de 1997.
50. HERRERA-LASSO, Luis, et al, *Balance y Perspectiva del uso del Concepto de da Seguridad Nacional en el Caso de México,* Editores Siglo XXI, México 1990.
51. HUERTA Miranda, Marcelo, et al, *Los Delitos Informáticos,* Editorial Jurídica Cono Sur.
52. HULSMANN, Louk, Derecho Penal, 1982
53. JIJENA Leiva, Renato, *Chile: Protección Penal a la Intimidad y los Delitos Informáticos*, Editorial Jurídica de Chile, 1993.
54. JIMÉNEZ DE ASÚA, Luis. *La Ley y el Delito*, Décima primera edición, Editorial Sudamericana, Buenos Aires Argentina. Mayo 1980.
55. JIMÉNEZ DE ASÚA, Luis, *Tratado de Derecho Penal*, Tomo III, Tercera edición actualizada. Editorial Losada, S.A. Buenos Aires 1965.
56. JIMÉNEZ Huerta, Mariano, *Derecho Penal Mexicano*, Tomo I, Quinta edición, Editorial Porrúa. México 1992.
57. JOVER Padró, Joseph, *El Código Penal De La Informática*, X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática

Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi Editorial, Pamplona, 1997.

58. LARREA Holguín, Juan, *Derecho Civil Del Ecuador, Los Bienes Y La Posesión*, Tercera Edición. Corporación de Estudios y Publicaciones.
59. LIMA, De La Luz María, *Delitos Electrónicos*, en Criminalia México, Academia Mexicana de Ciencias Penales, Ed. Porrúa, No. 1-6. Año L. Enero - Junio 1984.
60. LÓPEZ Betancourt, Eduardo, *Teoría del Delito*, Décima cuarta edición, Editorial Porrúa, México 2007.
61. MADRID-MALO, Garizabal Mario, *Derechos Fundamentales,* Escuela Superior de Administración Pública, Santa Fe de Bogotá – Colombia, 1992.
62. MAGLIONA, Markovicth, Claudio Paúl, et al, *Delincuencia y Fraude Informático,* Editorial Jurídica de Chile 1999.
63. MALO Camacho, Gustavo, *Derecho penal mexicano. teoría general de la ley penal. Teoría general del delito. Teoría de la culpabilidad y el sujeto responsable, teoría de la pena,* Sexta edición Editorial Porrúa, México 2005.
64. MANZANARES, José Luis, et al, *Comentarios al Código Penal*, La Ley Actualidad, Las Rozas (Madrid), 1996.
65. MÁRQUEZ Piñero, Rafael, *Derecho Penal. Parte General,* Cuarta edición. Primera reimpresión Agosto 1999, Editorial Trillas, México 2006.
66. MÁRQUEZ Romero, Raúl, *Lineamientos y Criterios del Proceso Editorial*, Primera Edición, Editorial UNAM, México 2008.
67. MATEOS Muñoz, Agustín, *Compendio De Etimologías Greco-Latinas Del Español,* Editorial Esfinge, Cuadragésima sexta edición, México 2007.
68. MERLAT, Máximo, *Seguridad Informática: Los Hackers*, Buenos Aires Argentina, 1999, Publicación hecha en Internet. URL: http//www.monografías.com
69. MEZGER, Edmundo, *Tratado de Derecho Penal*, Tomo I, Traducción de J. Arturo Rodríguez Muñoz, Editorial Revista de Derecho Privado, Madrid España 1955.
70. MIR, Puig Santiago, *Función de la Pena y la Teoría del Delito en el Estado Social y Democrático de Derecho,* Bosch, 1979.
71. MONTIEL Sosa, Juventino, *Criminalística,* Editorial Limusa, Segunda edición, México 2007.

72. MORAL Torres, Anselmo, *Aspectos Sociales y Legales de la Seguridad Informática*, Ponencia 1ª Jornadas sobre "Seguridad en Entornos Informáticos", Instituto Universitario "General Gutiérrez Mellado", Madrid 12 de marzo de 1998.
73. MORALES Prats, Fermín, *El Código Penal de 1995 y la Protección de los Datos Personales,* Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28 al 30 octubre de 1996, Agencia de Protección de Datos, Madrid, 1996, pp. 211 a 250.
74. MORENO Martín, Arturo, *Diccionario de Informático y Telecomunicaciones inglés y español,* Editorial Ariel, Barcelona 2001.
75. MUÑOZ Conde, Francisco, Teoría General Del Delito, Segunda edición. Editorial Toblandú. 2005.
76. NOVOA Monreal, Eduardo, *Curso de Derecho Penal,* 1966, Universidad de Chile.
77. PALAZZI Pablo Andrés, *Virus Informáticos y Responsabilidad Penal,* Sección doctrina del diario La Ley, 16 de diciembre de 1992. URL Http://www.ulpiano.com.
78. PARELLADA, Carlos Alberto, *Daños En La Actividad Judicial E Informática Desde La Responsabilidad Profesional*, Editorial Astrea, Buenos Aires, 1990.
79. PAVÓN Vasconcelos, Francisco, *Manual de Derecho Penal Mexicano*, Décima edición debidamente corregida y puesta al día, Editorial Porrúa. México 1991.
80. PÉREZ Luño, Antonio Enrique, *Ensayos De Informática Jurídica*, Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996.
81. PÉREZ Luño, Antonio Enrique, *Manual De Informática Y Derecho*, Editorial Ariel S.A., Barcelona, 1996.
82. PIERINI Alicia, et al, *Hábeas Data, Derecho a la Intimidad,* Editorial Universidad, Buenos Aires, Argentina 1998.
83. PORTE PETIT Candalaup, Celestino, *Apuntamientos de la parte general de Derecho Penal*, Vigésima edición, Editorial Porrúa, México 2003.
84. RADBRUCH Gustav, *Teoría General del Derecho*, 1990.
85. REALE, Miguel, *La Teoría Tridimensional del Derecho. (Una división integral del Derecho)*, Traducción e introducción de Ángeles Mateos, Licenciada en Filosofía y Doctora en Derecho, Editorial Tecnos, España 1997.
86. RESA Nestares, CARLOS, *Crimen Organizado Transnacional: Definición, Causas Y Consecuencias*, Editorial Astrea, 2005.

87. REYNA Alfaro, Luis Miguel, *Fundamentos Para La Protección Penal De La Información Como Valor Económico De La Empresa"*, Publicación hecha en internet en URL: http//www.dercho.org.pe.
88. REYNOSO DÁVILA, Roberto, *Teoría General Del Delito*, Sexta edición, Editorial Porrúa, México 2006.
89. RIVERA Llano, Abelardo, *Dimensiones de la Informática en el Derecho*, Ediciones Jurídicas Radar, Bogotá Colombia 1995.
90. RODAO, Jesús de Marcelo, *Piratas cibernéticos. cyberwars, seguridad Informática e Internet*, Editorial Ra-ma, España 2005.
91. ROJAS Amandi, Víctor Manuel, *El uso de la Internet en el derecho*, Segunda Edición, Editorial Oxford, México 2001.
92. ROMEO, Casabona, Carlos María, *Delitos Informáticos De Carácter Patrimonial*, Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
93. ROMEO Casabona, Carlos María, *Los Llamados Delitos Informáticos*, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995.
94. ROMEO Casabona, Carlos María, *Poder Informático y Seguridad Jurídica, La Función Tutelar del Derecho Penal ante las Nuevas Tecnologías de la Información*, FUNDESCO, Colección impactos, Madrid, 1987.
95. RUIZ Vadillo, Enrique, *Responsabilidad Penal En Materia De Informática*, Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
96. RUIZ Vadillo, Enrique, *Tratamiento de la Delincuencia Informática como una de las expresiones de Criminalidad Económica*, Poder Judicial número especial IX, 1989.
97. SALT, G. Marcos, *Informática y Delito*, Publicación en Internet, URL: http://www.derecho.org.ar
98. SANTOS, Jaime Eduardo, et al, *Fraude Informático en el Banca,* Editorial Jesma, Bogotá, 1993.
99. SERRANO Gómez, Alfonso, *Derecho Penal. Parte Especial I. Delitos contra las Personas*, Editorial Dykinson, Madrid, 1996.

100. SOLANO Bárcenas, Orlando, *Manual de Informática Jurídica*, Editorial Jurídica Gustavo Ibáñez, Santa Fe de Bogotá D.C. Colombia 1997.TÉLLEZ Valdés, Julio, *Derecho Informático*, Tercera Edición, Editorial Mc Graw Hill, México 2003.
101. TELLEZ Valdés, Julio, *Los Delitos informáticos*, Editorial Temis 1999.
102. TELLEZ Valdés, Julio, *Los Delitos Informáticos*, Situación en México Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, pág. 461 474
103. TIEDEMANN, Klauss, *Poder Económico Y Delito*, Barcelona, 1985.
104. TORRES López, Mario Alberto, *Las Leyes Penales*, editorial Porrúa, quinta Edición, México 2005.
105. TORTRAS Y BOSCH, Carlos, *El Delito Informático*, número 17 monográfico de ICADE, Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. TREJO García, Elma del Carmen, *Regulación Jurídica de Internet, servicio de Investigación y Análisis*, subdirección de Política Exterior, Cámara de Diputados.
106. VELÚ, Jacques, *Convención Europea de Derechos Humanos: El respeto a la Intimidad en el hogar y las comunicaciones*, Publicación hecha en Internet: www.google.com.
107. VILLALOBOS, Ignacio, *Derecho Penal Mexicano,* quinta edición, editorial Porrúa. México 1990.
108. VILLANUEVA Romero, Sandra, *La Organización Internacional ante el Derecho y la Regulación del Ciberespacio. Inserción de México en la Internet*, Facultad de Ciencias Políticas y Sociales, UNAM 2001.
109. WILLIAMS, Phil, *Crimen Organizado Y Cibernético, Sinergias, Tendencias Y Respuestas*, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, URL: http://www.pitt.edu/~rcss/toc.html.
110. ZABALA Baquerizo, Jorge, *Delitos contra la Propiedad*, Tomo 2, Editorial Edino, Guayaquil, Ecuador, 1988.
111. ZAFFARONI, Eugenio Raúl, *Manual de Derecho Penal,* segunda edición, editorial Cárdenas, México 2007.
112. ZANONI Leandro, *Los Hackers, la nueva cara de los piratas de Fin de siglo*, Revista de Informática y Derecho, De Palma Buenos Aires Argentina 1998.

DICCIONARIOS.

1. Diccionario Jurídico Mexicano, Editorial Porrúa, Tomo III, México 1985.

2. Diccionario Planeta de la Lengua Española, Editorial Planeta, México 1990, Tomo 3.

3. Diccionario de la Lengua Española, Editorial Real Academia Española, vigésima segunda edición, España 2001, Tomo 4.

4. Diccionario de Informática y Telecomunicaciones, Inglés-Español, Editorial Ariel S.A. Barcelona España 2001.

LEGISLACIÓN FEDERAL

1. Constitución Política de los Estados Unidos Mexicanos
2. La Ley de Propiedad Industrial.
3. La Ley Federal de Derechos de Autor.
4. Ley de Instituciones de Crédito
5. La Ley Federal de Telecomunicaciones.
6. La Ley Federal de Protección al Consumidor
7. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
8. La Ley de Información y Estadística y Geografía
9. Ley Orgánica del Poder Judicial de la Federación
10. Ley Federal Contra la Delincuencia Organizada.
11. Código Fiscal de la Federación
12. Código de Comercio
13. Código Penal Federal
14. Código Civil Federal
15. Código Federal de Procedimientos Civiles

LEGISLACION ESTATAL

1. Código Penal para el Estado de Aguascalientes
2. Código Penal para el Estado de Baja California
3. Código Penal para el Estado de Baja California Sur
4. Código Penal para el Estado de Campeche
5. Código Penal para el Estado de Coahuila de Zaragoza
6. Código Penal para el Estado de Colima
7. Código Penal para el Estado de Chiapas
8. Código Penal para el Estado de Chihuahua
9. Código Penal para el Distrito Federal
10. Código Penal para el Estado de Durango
11. Código Penal para el Estado de Guanajuato
12. Código Penal para el Estado de Guerrero
13. Código Penal para el Estado de Hidalgo
14. Código Penal para el Estado de Jalisco
15. Código Penal para el Estado de México
16. Código Penal para el Estado de Michoacán
17. Código Penal para el Estado de Morelos
18. Código Penal para el Estado de Nayarit

19. Código Penal para el Estado de Nuevo León
20. Código Penal para el Estado de Oaxaca
21. Código Penal para el Estado de Puebla
22. Código Penal para el Estado de Querétaro
23. Código Penal para el Estado de Quintana Roo
24. Código Penal para el Estado de San Luis Potosí
25. Código Penal para el Estado de Sinaloa
26. Código Penal para el Estado de Sonora
27. Código Penal para el Estado de Tabasco
28. Código Penal para el Estado de Tamaulipas
29. Código Penal para el Estado de Tlaxcala
30. Código Penal para el Estado de Veracruz
31. Código Penal para el Estado de Yucatán
32. Código Penal para el Estado de Zacatecas

FUENTES DE INFORMACIÓN ELECTRÓNICAS

1. Congreso del Estado de Aguascalientes http://congresoags.gob.mx/home/.
2. Congreso del Estado de Baja California, http://www.congresobc.gob.mx/.
3. Congreso del Estado de Baja California Sur, http://www.cbcs.gob.mx/.
4. Congreso del Estado de Campeche, http://www.congresocam.gob.mx/.
5. Congreso del Estado de Coahuila, http://www.congresocoahuila.gob.mx/.
6. Congreso del Estado de Colima, http://www.congresocol.gob.mx/.
7. Congreso del Estado de Chiapas, http://www.congresochiapas.gob.mx/.
8. Congreso del Estado de Chihuahua, http://congresochihuahua.gob.mx/.
9. Asamblea Legislativa del Distrito Federal, http://www.asambleadf.gob.mx/.
10. Congreso del Estado de Durango, http://www.congresodurango.gob.mx/.
11. Congreso del Estado de Guanajuato, http://www.congresogto.gob.mx/.
12. Congreso del Estado de Guerrero, http://www.congresogro.gob.mx/.
13. Congreso del Estado de Hidalgo, http://www.congreso-hidalgo.gob.mx/.
14. Congreso del estado de Jalisco, http://www.congresojal.gob.mx/.
15. Poder Ejecutivo del Estado de México, http://www.edomex.gob.mx/portal/page/portal/edomex.
16. Congreso del Estado de Michoacán, http://www.congresomich.gob.mx/.
17. Congreso del Estado de Morelos, http://www.congresomorelos.gob.mx/.
18. Congreso del Estado de Nayarit, http://www.congreso-nayarit.gob.mx/.
19. Congreso del Estado de Nuevo León, http://www.congreso-nl.gob.mx/.
20. Congreso del Estado de Oaxaca, http://www.congresooaxaca.gob.mx/.
21. Poder Ejecutivo del Estado de Puebla, http://www.puebla.gob.mx/.

22. Congreso del Estado de Querétaro, http://www.legislaturaqro.gob.mx/.
23. Congreso del Estado de Quintana Roo, http://www.congresoqroo.gob.mx/.
24. Congreso del Estado de San Luis Potosí, http://148.235.65.21/LIX/.
25. Congreso del Estado de Sinaloa, http://www.congresosinaloa.gob.mx/.
26. Congreso del Estado de Sonora, http://www.congresoson.gob.mx/.
27. Congreso del Estado de Tabasco, http://www.congresotabasco.gob.mx/legislaturaLX/index.php?option=com_content&view=category&id=17&Itemid=84.
28. Congreso del Estado de Tamaulipas, http://www.congresotamaulipas.gob.mx/.
29. Congreso del Estado de Tlaxcala, http://www.congresotlaxcala.gob.mx/.
30. Congreso del Estado de Veracruz, http://www.legisver.gob.mx/index.php.
31. Congreso del Estado de Yucatán, http://www.congresoyucatan.gob.mx/
32. Congreso del Estado de Zacatecas, http://www.congresozac.gob.mx/
33. "La Historia de la Computación", h*ttp://www.cad.com.mx/historia_de_la_computacion.htm.*
34. "El Rincón Universitario", *http://www.emas.co.cl/categorias/informatica/historiacomp.htm.*
35. "La Historia que llevo a construir la Primera Computadora", *http://www.monografias.com/trabajos14/histcomput/histcomput2.shtml#G*
36. "El Rincón Universitario", *http://www.emas.co.cl/categorias/informatica/historiacomp.htm*
37. "Norbert Wiener y el Origen de la Cibernética", *http://www.infoamerica.org/documentos_pdf/wiener2.pdf.*
38. "La Historia de Arpanet", *http://es.wikipedia.org/w/index.php?title=Internet&oldid=67768692.*
39. Gutiérrez Cortés, Fernando y López, Carlos Enrique "Una Década de Internet en México", Revista Mexicana de Comunicación, núm. 56, Octubre-Diciembre 1998, *http://www.cem.itesm/dacs/buendia/rmc56/internet.html.*

40. Sociedad Internet de México, "Historia de la Internet En México", *http://www.isocmex.org.mx/historia.html.*

41. Corporativo Nic-México, "Historia de Nic-México", *http://www.nic.mx/es/NicMéxico.Historia.*
42. Pozo, Juan R, "Breve Historia de la World Wide Web", *http://html.conclase.net/articulos/historia.*
43. EMBL Heidelberg**,** "European Molecular Biology Laboratory", *http://www.emblheidelberg.de/*

44. "International Nucleotide Sequence Database Collaboration", *http://www.ncbi.nlm.nih.gov/genbank/collab/country.*

45. Wiener, Norbert, *"The Human Use of Human Beings: Cybernetics and Society"*, *http://biblioteca.universia.net/html_bura/ficha/params/titlethehumanuseofhumanbeingscyberneticsandsocietyn/id/37815461.html*
46. "Virtual Magistrate", *http://www.vmag.org/*
47. "The Online Ombuds Office", *http://www.ombuds.org/center/ombuds.html*

48. "Resolution", *http:/www.udrpinfo.com/eres/*

49. Constitución Española, h*ttp://www.derechoshumanos.net/constitucion/index.htm?gclid=CKX0iq3l7gCFWrl7Aod73YAeQ.*

50. Convenio No 108 del Consejo, de 28 de Enero de 1981, de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, *http://www.apdcat.net/media/246.pdf*

51. "Página de la Secretaría de Seguridad Pública", *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1276161*
52. "Guía Taller contra la Prevención del Delito Cibernético", *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1214152//archivo.*
53. Policía Cibernética, *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/388074//archivo*

54. Sobre el tema puede revisarse las siguientes direcciones electrónicas, *http://www.stop-childpornog.at/, y también http://www.info2000.csic.es/midas-net/pornoinfantil.htm*
55. Trejo García, Elma del Carmen, "*Regulación Jurídica de Internet*", Servicio de Investigación y Análisis, subdirección de Política Exterior, Cámara de Diputados. *http://www.diputados.gob.mx/cedia/sia/spe/SPE-ISS-12-06.pdf*
56. Los informes de GAFI (Grupo de Acción Financiera) sobre el blanqueo de dinero se encuentran visibles en *http://oecd.org/fatf/index.html.*
57. Se puede revisar el texto íntegro de La Ley Orgánica de Protección de Datos de Carácter Personal de España (LOPD), *http://club.telepolis.com/vicenti/ce78/Vicenti/lotc/Vicenti/lloo/lo15_99.htm*
58. Texto completo del Código Penal Alemán en idioma inglés, puede consultarse en: *http://wings.buffalo.edu/law/bclc/germind.htm. Del Centro de Leyes Penales de Búfalo, Estados Unidos de América.*
59. El texto completo del Código Penal Español, puede verse en: *http://www.law.unican.es/incade/lex/cpint.htm, del Instituto Cántabro de Derecho.*
60. El texto completo del Código Penal Francés, puede revisarse en: *http://www.legifrance.gouv.fr/citoyen/code.ow*
61. La Legislación Europea Comunitaria, Documento 399D0276, *http://europa.eu.int/eurlex/es/lif/index.html*
62. Departamento de Cooperación Jurídica de la Organización de los Estados Americanos, http://www.oas.org/juridico/spanish/cybersp_legis.htm.
63. Sociedad de Internet, www.internetsociety.org/es.
64. Plantel de Arquitectura de Internet, www.iabmexico.com/
65. Fuerza Social de Internet, istf.ucf.edu/.
66. Autoridad de Asignación de números de internet, www.iana.org/
67. Business Software Alliance, www.bsa.mx/
68. Asociación Hispanoamericana de centros de investigación y de empresas de telecomunicaciones, www.ahciet.net/
69. Unión Internacional de Telecomunicaciones, www.itu.int/es/about/Pages/default.aspx
70. Comisión de Regulación de Telecomunicaciones, www.regulatel.org/,

71. Ley Modelo de las Naciones Unidas para el Derecho Mercantil, www.uncitral.org
72. Organización que dispone y gestiona los recursos de internet en América Latina y el Caribe, www.lacnic.net
73. Instituto Mexicano de la propiedad intelectual, www.tumarca.com.mx/