



**UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO**

---

**FACULTAD DE DERECHO**

**“LA PROBLEMÁTICA JURÍDICA EN LA  
REGULACIÓN  
DE LOS DELITOS INFORMÁTICOS”**

**TESIS PROFESIONAL  
QUE PARA OBTENER EL TÍTULO DE  
LICENCIADO EN DERECHO**

**PRESENTA**

**ALEJANDRO ARMANDO MONTAÑO ÁLVAREZ**

**LIC. GUILLERMO GONZÁLEZ PICHARDO  
ASESOR DE TESIS**



**CIUDAD UNIVERSITARIA**

**2008**



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## RECONOCIMIENTOS

### A MIS PADRES:

Dr. Alejandro Montaña Salazar.

Maria Magdalena Alvarez Maldonado.

Gracias por que existir, por quien soy y por mostrarme los principios, valores y enseñanzas que necesito para la vida y lograr mis objetivos

### A MIS HERMANOS:

Gustavo Montaña Alvarez.

Natalia Magdalena Montaña Alvarez.

Que con su compañía, cariño y apoyo en cada momento de nuestra vida, ayudaron a forjar al hombre que soy

### A MIS AMIGOS:

Por su confianza y amistad aun hasta en los malos momentos y el apoyo para continuar.

A NUESTRA UNIVERSIDAD  
Y FACULTAD DE DERECHOS:

“Con toda gratitud”

# **“LA PROBLEMÁTICA JURÍDICA EN LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS”**

## **CAPITULADO**

<b>INSTRUCCIÓN</b>	<b>I</b>
<b>CAPÍTULO 1.- Antecedentes sobre la informática, conceptos y sus diversos campos de acción</b>	<b>1</b>
1.1. Antecedentes de la informática	1
1.1.1. Historia de las Computadoras	1
1.2. Conceptos de la electrónica, informática, cibernética y otros	6
1.2.1. La Electrónica	6
1.2.2. La Informática	7
1.2.3. La Cibernética	8
- Orígenes de la Cibernética	9
- Diferencia entre Cibernética y la Informática	9
1.2.4. El Ordenador y sus componentes	10
1.2.5. La Internet	12
- Historia de la Internet en el mundo	12
- Historia de la Internet en México	14
- Servicios en la Internet	18
- Organización de la Internet	21
- Denominación	21
- Dirección de correo electrónico (e-mail)	24
1.3. Campo de acción de la Informática	24
1.3.1. La informática en las Ciencias Naturales	24
- La Informática en la Medicina, en la Biología y en la Genética	25
- La Informática en la Química y Física	27
1.3.2. La Informática en las Ciencias Sociales	27
- La Informática en la Economía y Administración	27
- La Informática en el diseño, ingenierías y manufacturas	28
- La Informática en la Educación	28
- La Informática y la Guerra	32
1.3.3. La Informática en el Derecho	32
- Derecho Informático	33
- Derecho a la Informática y a la información	34
- La Informática Jurídica	36
- La Informática aplicada al Derecho	37

- La Cibernética Jurídica	53
- Derecho de la Informática	55
- Contratación electrónica y comercio electrónico	66
<b>CAPÍTULO 2. Marco jurídico sobre la Informática Jurídica y los delitos informáticos</b>	<b>77</b>
2.1. Constitución Política de los Estados Unidos Mexicanos	80
2.2. Ley Federal del Derecho de Autor	90
2.3. Ley de la Propiedad Industrial	94
2.4. Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental	99
2.5. Código Penal Federal	105
2.6. Código Penal para el Estado de Sinaloa	109
2.7. Otras Legislaciones en México	117
2.7.1. Delitos llevados a cabo mediante medios Informáticos	117
- Delitos patrimoniales	118
- Legislación para el Estado de Aguascalientes	
- Código Penal del Estado de Colima	
- Código Penal del Estado Libre y Soberano de Chiapas	
- Código Penal del Estado de México	
- Código Penal del Estado de Durango	
- Código Penal para el Distrito Federal	
- Código Penal para el Estado de Guerrero	
- Código Penal para el Estado de Nuevo León	
- Código Penal para el Estado de Quintana Roo	
- Código Penal para el Estado de Tamaulipas	
- Delitos en contra de la moral pública	125
- Código Penal del Estado de Colima	
- Código Penal para el Estado de Morelos	
- Código Penal para el Estado de Tamaulipas	
- Código Penal para el Estado de Yucatán	
- Código Penal para el Estado de Zacatecas	
- Delitos ambientales	128
- Código Penal para el Estado de Colima	
- Código Penal para el Distrito Federal	
- Delitos contra las vías de comunicación	129
- Código Penal para el Estado de Tabasco	
- Delito de secuestro	129
- Código Penal para el Estado Libre y Soberano	

de Jalisco

- Delito de revelación de secreto	130
- Código Penal para el Estado de Baja California	
<b>2.7.2. Delitos Informáticos en otras legislaciones</b>	<b>131</b>
- Código Penal para el Estado de Aguascalientes	
- Código Penal para el Estado de Coahuila de Zaragoza	
- Código Penal del Estado Libre y Soberano de Chiapas	
- Código Penal para el Estado de Guanajuato	
- Código Penal para el Estado Libre y Soberano de Jalisco	
- Código Penal para el Estado de Nuevo León	
- Código Penal para el Estado de Tamaulipas	
- Código Penal para el Estado Libre y Soberano de Veracruz – Llave	
<b>CAPÍTULO 3.- PROBLEMÁTICA JURÍDICA DE LOS DELITOS INFORMÁTICOS</b>	<b>139</b>
<b>3.1. Conceptos básicos sobre la Teoría del Delito aplicados a los ilícitos informáticos</b>	<b>139</b>
<b>3.1.1. La Dogmática Jurídico – Penal y la Teoría del Delito</b>	<b>139</b>
<b>3.1.2. El concepto del delito y la definición del delito informático</b>	<b>140</b>
<b>3.2. Clasificación del Delito Informático</b>	<b>147</b>
<b>3.2.1. Clasificación jurídico-penal del delito y su aplicación al delito informático</b>	<b>147</b>
<b>3.2.2. Clasificación conforme a la doctrina jurídico-informática</b>	<b>161</b>
- Como instrumento o medio	
- Como fin u objeto	
<b>3.3. Elementos del delito y su aplicación en el Delito Informático</b>	<b>163</b>
<b>3.3.1. Conducta y ausencia de conducta</b>	<b>163</b>
- Formas de aparición de la conducta	<b>165</b>
La acción	
La omisión	
- La conducta en los Delitos Informáticos	<b>168</b>
- La ausencia de conducta	<b>169</b>
- La ausencia de conducta en los Delitos Informáticos	<b>171</b>
<b>3.3.2. Tipicidad y atipicidad</b>	<b>171</b>
- Concepto de tipicidad	<b>172</b>
- La tipicidad en el Delito Informático.	<b>174</b>
<b>3.3.3. El tipo penal y ausencia de tipo</b>	<b>175</b>
- El tipo penal	<b>175</b>
- Clasificación del tipo penal	<b>176</b>

- Elementos del tipo penal	182
- Elementos del tipo penal informático	184
- La atipicidad y ausencia de tipo penal informático	198
<b>3.3.4. La antijuridicidad y las causas de licitud</b>	198
- Concepto de antijuridicidad	199
- La antijuridicidad en el Delito Informático	201
- Las causas de justificación o de licitud en el Delito Informático	202
<b>3.3.5. La antijuridicidad y las causas de licitud</b>	210
- Concepto de Imputabilidad	210
- La imputabilidad en el Delito Informático.	212
- La inimputabilidad	212
- Las causas de inimputabilidad en el Delito Informático	214
<b>3.3.6. La culpabilidad y la ausencia de culpabilidad</b>	214
- Concepto de culpabilidad	215
- Formas de culpabilidad	217
- La culpabilidad den el Delito Informático	220
- Causas de ausencia de culpabilidad	221
- Causas de ausencia de culpabilidad en el Delito Informático	225
<b>3.3.7. Las condiciones objetivas de punibilidad y su ausencia</b>	226
- Concepto de condiciones objetivas de punibilidad	226
- Las condiciones objetivas de punibilidad en el Delito Informático	227
- La ausencia de condiciones objetivas de punibilidad	227
- Las causas de ausencia de condiciones objetivas de punibilidad en el Delito Informático	228
<b>3.3.8. La punibilidad y las excusas absolutorias</b>	228
- Concepto de punibilidad	228
- La punibilidad en el Delito Informático	229
- Las excusas absolutorias	231
- Las excusas absolutorias en el Delito Informático	232
<b>3.4. Formas de aparición del delito</b>	233
<b>3.4.1. El <i>iter criminis</i>.(la vida del delito)</b>	233
- La Tentativa	236
- La consumación	237
<b>3.4.2. Concurso de delitos y concurso aparente de normas</b>	238
<b>3.4.3. Concurso de personas (autoría y participación).</b>	240
<b>CAPÍTULO 4. LA DELINCUENCIA INFORMÁTICA Y SU REGULACIÓN INTERNACIONAL; EN MÉXICO Y SUS TENDENCIAS</b>	242
<b>4.1. La delincuencia informática internacional.</b>	242
<b>4.1.1. El delincuente informático</b>	242
- El “Hacker”	242

- El "Cracker"	247
- Otros delincuentes informáticos	248
4.1.2. Conductas delictivas y nocivas en medios informáticos	249
- Conductas nocivas en Internet	255
- El virus Informático	257
- Contenido nocivo en Internet	264
- Los mundos virtuales	270
- Conductas delictivas	273
Pornografía infantil	276
Corrupción de menores	280
Redes de narcotráfico	286
4.1.3. El terrorismo cibernético	287
- Ataques en contra del Estado	293
- Ataques a Entidades Financieras	296
- Ataques a Servicios	297
- La seguridad informática	299
4.2. Tratamiento de la delincuencia informática en organismos internacionales	300
4.2.1. En la Organización de las Naciones Unidas	300
4.2.2. En la Comisión de las Comunidades Europeas	303
- El convenio sobre la Ciber-criminalidad	304
- España	312
4.2.3. En la Sociedad de la Información	325
4.3. La Criminalística Informática	327
4.3.1. La Criminalística	327
4.3.2. La Criminalística en la Informática	330
4.3.3. La Política Cibernética	332
- La Unidad de Policía Cibernética de la Policía Federal Preventiva en México	334
- Policías Internacionales	338
Organización Internacional de Policía (INTERPOL)	338
Oficina Europea de Policía (EUROPOL)	339
El Buró Federal de Investigaciones (FBI)	343
4.3.4. Política en la Criminalística Informática	349
4.4. La procuración de justicia en México en relación a los Delitos Informáticos	352
<b>Conclusiones</b>	355
<b>Propuestas</b>	361
<b>Fuentes de Consulta</b>	363

<b>Bibliografía</b>	363
<b>Diccionarios</b>	365
<b>Resoluciones Judiciales</b>	365
<b>Legislaciones</b>	365
<b>Medios electrónicos</b>	367
<b>Hemerografía</b>	370

**Septiembre 2008**

## INTRODUCCIÓN.

En el mundo y concretamente en México, han surgido problemas que deben afrontarse con adecuadas leyes, tal es el caso de la delincuencia organizada, en la cual para poder hacer frente a ella se creó la Ley Federal Contra la Delincuencia Organizada; una de las tales vertientes lo es la constante práctica de “lavar el dinero” producto de actos delictivos, motivo por lo que se perfecciona el delito de operaciones con recursos de procedencia ilícita descrito en el artículo 400 bis del Código Penal Federal. Las crisis económicas que han azotado a nuestro país en las últimas décadas, para lo cual el legislador reformó las leyes financieras sobre todo en lo concerniente a los delitos, ampliando a los sujetos activos, regulando mejor los términos de la prescripción, la necesidad de incluirlos como delitos graves entre otras medidas más, el medio ambiente que se ha deteriorado por la constante industrialización, creándose así los delitos ambientales, las diversas formas en la obtención de lucros indebidos, creándose fraudes especiales, entre otras situaciones más que son indispensables contemplar en adecuadas leyes que generen también una correcta aplicación de tales figuras, brindando una seguridad jurídica a los gobernados.

De esta forma, en otro gran rubro del desarrollo social, en lo que corresponde a la cibernética e informática, ha tenido grandes avances en beneficio de la sociedad en todos sus aspectos, facilitándonos a través de un ordenador o computadora muchas de nuestras actividades, tales como, el pago de los servicios bancarios, la solicitud de préstamos a instituciones financieras, el pago de boletos del teatro, cine o cualquier otro espectáculo, la consulta de bibliotecas enteras en todo el mundo, el guardar información confidencial, el pago de deudas, la celebración de contratos informáticos, el uso de diversos medios de comunicación como la telefonía inalámbrica y celular, o simplemente lo práctico que resulta usar la computadora como un mero procesador de palabras. El mundo entero se encuentra invadido del uso de la Internet con el que se puede “navegar” a todos sus rincones realizando las anteriores operaciones descritas y más.

Sin embargo, la delincuencia también ha hecho uso de todos los medios informáticos para alcanzar sus fines ilícitos, constituyéndose los que muchos han llamado la “delincuencia informática”, que también es parte de la gran delincuencia organizada que pretende abatir el Estado Mexicano, utilizando computadoras para cometer fraudes, robos, abusos de confianza, fraudes financieros, extorsiones, falsificaciones, amenazas, y un gran número de delitos previstos en los códigos penales tanto a nivel federal como local, así como en leyes especiales.

Ese nuevo fenómeno informático se ha convertido en otra más de las grandes preocupaciones de los legisladores para establecer patrones de comportamiento dentro de nuestra sociedad en diversos campos del Derecho, ya que también lo podemos encontrar en ramas como la Civil, Mercantil, Laboral, Administrativa, Fiscal y Penal, entre otras, surgiendo en ésta última los conocidos “ilícitos informáticos”.

Sin embargo, con la denominación de “delitos informáticos” se han encontrado muchas críticas a las que inclusive tiene que enfrentar el legislador para su adecuada tipificación, ya que bajo las diversas situaciones antes planteadas podemos encontrar delitos como los antes señalados cometidos por medios informáticos, o bien, los ilícitos que se cometieran de una manera directa en contra de lo que implica todo el mundo del sistema cibernético como sería los hardware, los software, etc.. y que posiblemente estaríamos en presencia de una regulación que se encuentra ya establecida como es la del Derecho de Autor, así como la violación a la confidencialidad de la información contenida en medios informáticos, o bien atentar contra éstos últimos.

Dentro de la presente investigación se procederá al estudio de los delitos informáticos analizando en primero lugar a través de un método histórico y documental los antecedentes de la Informática, que implica desde el surgimiento de las computadoras e inclusive de los diversos medios que se han utilizado para auxiliar al hombre en sus diversas operaciones, además de contemplar los conceptos más importantes al respecto tales como la Electrónica, la Informática, la Cibernética y de la maravilla de la Internet y los propósitos que ha tenido este sistema en el mundo y en México, lo cual se analizará en el Capítulo Primero, contemplando además la influencia de la Informática en las diversas actividades del ser humano desde las ciencias naturales tales como la Medicina, la Biología, la Genética, la Química y la Física entre otras, así como su importancia en las ciencias sociales como lo es el Derecho, surgiendo en su relación con ésta última novedosas ramas de la Ciencia Jurídica como lo es el Derecho Informático, la Informática Jurídica, el Derecho a la Información la Cibernética Jurídica y otras que son necesarias su comprensión a efecto de poder realizar estructuras jurídicas al respecto en la diversas ramas tradicionales del Derecho como la Civil, la Mercantil y sobre todo en la Penal siendo el plano que interesa al presente trabajo encontrando a los Delitos Informáticos.

En el Capítulo Segundo se pretende llevar a cabo una descripción de la naturaleza de los ilícitos informáticos y del marco jurídico que se encuentra interrelacionado con nuestras figuras delictivas, en donde se parte de la Constitución Política de los Estados Unidos Mexicanos y legislaciones secundarias como la Ley Federal del Derecho de Autor, la Ley la Propiedad Industrial, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como el Código Penal Federal y el Código Penal del Estado de Sinaloa, legislaciones últimas que servirán de modelo

para analizar detalladamente en ésta investigación a los delitos informáticos y que inclusive pudieran tener algunas contrariedades legales con las anteriores legislaciones, ya que además de pretenderse proteger a la información contenida en medios informáticos encontramos que se protege a los propios sistemas informáticos, así como la comisión de delitos a través de medios informáticos, situación que se pretende acreditar en este apartado. Asimismo se hará referencia a otras legislaciones que prevén a los delitos informáticos en la República Mexicana.

Es menester para el estudio de cualquier figura delictiva, y los informáticos no son la excepción, llevar a cabo un análisis Dogmático Jurídico-Penal a través de la Teoría del Delito contemplando tanto a los elementos positivos como negativos, ya que a través de ello se puede comprender jurídicamente éstas novedosas figuras penales, consultándose para tal efecto a prestigiados penalistas, de los cuales plasmaré sus teorías encuadrándolas a los delitos informáticos de las legislaciones penales Federal y del Estado de Sinaloa dentro del Capítulo Tercero.

Por último, en el Capítulo Cuarto se destacarán algunos puntos importantes así como reflexiones acerca de la Delincuencia Informática tanto a nivel internacional como en nuestro país, en virtud de que esta problemática afecta a todos los países del mundo, siendo importante tratar los diversos tipos de personajes expertos en la Informática que son utilizados en esta clase de delincuencia, así como la gran diversidad de conductas ilícitas que pueden realizarse a través de la Informática hasta llegar al llamado "Terrorismo Cibernético", las cuales han recibido diversos tratamientos por múltiples organismos internacionales sirviéndose de las ciencias auxiliares del Derecho Penal como lo es la Criminalística y de las políticas existentes al respecto, requiriéndose así de una Policía que se regule a través de principios científicos y que para el combate de ese tipo de delincuencia ha surgido en diversos países como en México la "Policía Cibernética".

No cabe duda que lo novedoso y cada vez más avanzado de los ilícitos Informáticos requiere de también innovaciones para su tratamiento en todos los sentidos tanto desde el aspecto técnico como el jurídico, siendo éste último campo el que se concentra esta investigación, sin dejar a un lado el primero, ya que todo ello es indispensable para estructurar la base de todo sistema legal y que es el tener adecuadas figuras penales que puedan aplicarse también adecuadamente a los casos concretos, pretendiendo aquí llevar a cabo un estudio jurídico, crítico y propositivo del tema de los Delitos Informáticos.

## **EL SUSTENTANTE**

**Septiembre 2008**

## **CAPÍTULO 1.- Antecedentes sobre la Informática, conceptos y sus diversos campos de acción.**

### **1.1. Antecedentes de la Informática.**

En el presente apartado se analizarán los antecedentes y diversas definiciones en el mundo y en México de conceptos importantes tales como de la informática, la electrónica, la cibernética, la 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 buscado formas para facilitar y simplificar su existencia 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 diversas culturas. El código de Hammurabi da a conocer referencias del uso de este ingenioso 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 Japones 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 máquina calculadora que mantenía una relación de 10:1 en cada una de sus ruedas registradoras de 13 dígitos.

A pesar de este ingenioso invento, aún persistían problemas en la realización de ciertas operaciones, por lo que Jhon Napier (Edimburgo, 1550 - 4 de abril de 1617) crea la Tabla de Logaritmos con lo que permitió realizar multiplicaciones y divisiones de manera sencilla y rápida pero aún con sus problemas por lo que fue inventada la Regla de Cálculo, aparato más sencillo y rápido 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, convirtiéndose en una calculadora de bolsillo, extremadamente versátil.

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.

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 apoyo del gobierno Inglés ideó una máquina denominada “Maquina Diferencial” capaz de realizar 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.

Años después Charles Babbage ideó su Máquina Analítica, con lo que se podía idear operaciones más complejas de manera rápida además de almacenar 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 concretarse.

Los primeros y verdaderos inicios en lo que hoy conocemos como computadoras se debe a Herman Hollerith, miembro del censo de los Estados Unidos de Norte América que 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 (International Business Machines) 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 cableado eléctrico, la cual empleaba señales electromagnéticas para mover las partes mecánicas, su programación dependía de la idea inicial de las máquinas analíticas mediante una cinta perforada, esta máquina podía realizar cualquier tipo de operaciones aunque de una manera relativamente lenta debido a la complejidad de la maquinaria interna<sup>1</sup>.

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 m<sup>2</sup>, llenaba un cuarto de 6 metros x 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 nacimiento de una nueva era abarcando periodos determinados basados en las características del sistema físico o lógico conocidas como Generaciones, dividiéndose en las siguientes:

**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 vacío, lo que permitió su fácil funcionamiento y eran capaz de realizar mil operaciones por segundo y almacenar hasta 20,000 posiciones.

---

<sup>1</sup> LA HISTORIA QUE LLEVO A CONSTRUIR LA PRIMERA COMPUTADORA, [.com/trabajos14/histcomput/histcomput2.shtml](http://www.com/trabajos14/histcomput/histcomput2.shtml)

**La Segunda Generación:** Construidas entre 1960 y 1965 su principal característica consistía en la introducción de elementos electrónicos básicos como el transistor el cual determinaba el paso de corriente entre dos puntos, este tipo de tecnología marcó una gran pauta en la creación de computadoras revolucionando la industria con el ahorro de energía y espacio además de la veracidad y velocidad 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 m<sup>2</sup>, lo que permitía que ésta pudieran abarcar menos espacio a comparación de sus predecesoras.

**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 mm<sup>2</sup>, 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 crear 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 diferencia 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”.<sup>2</sup> 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 vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos”.<sup>3</sup>

Para poder entender de una manera sencilla en su funcionamiento dentro de un aparato electrónico se tiene que tomar en cuenta que el flujo de estos electrones genera corriente eléctrica y ésta a su vez usada en dispositivos cambian la energía eléctrica 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 y es conocida como Electrónica.

---

<sup>2</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA.** Editorial. Planeta. México 1990. Tomo. 3 Pág. 461.

<sup>3</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA.** Editorial Real Academia Española. Vigésima segunda edición. España 2001. Tomo 4. Pág. 590.

### 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 nacimiento 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 modesto programas de aplicación) operación y uso de las computadoras”<sup>4</sup>.

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

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

Esto puede ser entendido como la interpretación y procesamiento lógico de los impulsos eléctricos de manera ordenada, por ejemplo, los audio cassettes, éstos poseen

---

<sup>4</sup> **DICCIONARIO DE INFORMÁTICA Y TELECOMUNICACIONES.** Inglés-Español. Editorial Ariel S.A. Barcelona España 2001. Pág. 131.

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 caso de un audio cassettes estaban acomodados según las vibraciones generadas por el sonido pero en el caso de dispositivos informáticos como lo son los disquetes o discos flexibles está relación ordenada de cargas son entendidos como “ceros y unos”, el lenguaje binario; están procesadas y entendidas lógicamente y matemáticamente mediante una computadora permitiendo reproducir o almacenar información.

### **1.2.3. La Cibernética.**

Cibernética: “del griego *κυβερνητική*: Piloto o el arte de pilotear un navío”.<sup>5</sup> Aunque Platón la utilizó en La República con el significado de "arte de dirigir a los hombres" o "arte de gobernar".

Las investigaciones con fines militares a partir de la segunda guerra mundial propiciaron la creación del concepto moderno de la Cibernética moderna: como una ciencia de la comunicación y el control.

Otra forma de entender a la Cibernética moderna es como: “Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las

---

<sup>5</sup> Mateos Muñoz, Agustín. **COMPENDIO DE ETIMOLOGÍAS GRECO-LATINAS DEL ESPAÑOL**. Editorial Esfinge. Cuadragésima sexta edición. México 2007. Pág. 299.

máquinas y en particular, el de las aplicaciones de los mecanismos de regulación biológicas a las tecnológicas”.<sup>6</sup>

#### **- 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 máquinas” (Cybernetics, or control and communication in the animal and machina) publicada en 1948, el cual empleó el término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina.

#### **- 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 iguales, pero aunque guardan una relación entre sí las partes que lo componen no son iguales.

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.

---

<sup>6</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA**, Op. Cit. Tomo 3. Pág. 370.

#### 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 máquina que podía realizar cálculos.

La Computadora es: “una máquina electrónica analógica y digital, dotado de una memoria de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas.”<sup>7</sup>

Entendido de otra manera una computadora es un “dispositivo electrónico complejo que puede ser programado para recibir, almacenar, procesar, transmitir y presentar”<sup>8</sup>.

Ésta 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

---

<sup>7</sup> Ibidem. Pág. 412.

<sup>8</sup> **DICCIONARIO DE INFORMATICA Y TELECOMUNICACIONES.** Op. Cit. Pág. 130.

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:

- 1) Unidades de Entrada.
- 2) Unidades de Salida.
- 3) Unidades de Procesamiento, Almacenamiento o Memoria.

La Unidad de Entrada. Está constituida de todos aquellos dispositivos con los cuales se permite ingresar datos e información además del manejo de programas informáticos, éstos 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, éstos son pantallas, bocinas, impresoras de papel y 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), discos Flexibles (Floppy Disk Drive de 8, 5 ¼, 3 ½ pulgadas), procesadores (micro procesadores), unidades de almacenamiento (tarjetas de memoria, memorias USB flash).

Dentro de la capacidad de almacenamiento existen dos tipos de memoria la primera llamada RAM (Random Accesses Memory) 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) consta en memoria semiconductora de lectura utilizada para almacenar datos que nunca necesitan modificarse.

### **1.2.5. La Internet.**

Para poder entender los delitos informáticos es necesario poder entender lo que es la 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.

#### **- 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 independiente de las otras, con lo que nació la idea de ARPANET<sup>9</sup> (Advanced Research Projects Agency Network), con lo cual para el funcionamiento de esta red fue necesario la creación de procesadores especiales denominados Procesadores de Mensaje de Interfaz (IMP en sus siglas en inglés), el cual el primer procesador de este tipo entró en funcionamiento el 1 de Agosto de 1969 en la Universidad de California de los Ángeles E.U.A, con una computadora Honeywell 516 con una memoria de 12 MB de memoria<sup>10</sup>, extendiéndose a otras Universidades del país dando origen a ARPANET. Para 1972 se habían instalado 37 Procesadores de Mensaje de Interfaz. ARPANET fusionaba con un programa denominado Network Control Protocol (NPC)<sup>11</sup>, 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.

---

<sup>9</sup> Rojas Amandi, Víctor Manuel. **EL USO DE LA INTERNET EN EL DERECHO**, Segunda Edición. Editorial Oxford, México 2001. Pág. 2.

<sup>10</sup> Idem.

<sup>11</sup> <http://es.wikipedia.org/wiki/Internet#Historia>

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 intentó crear una política de uso científico y no comercial para la Internet lo cual no fue aplicado debido a la privatización de la Internet extendiendo su uso a niveles comerciales.<sup>12</sup>

### **- 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 logró 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.<sup>13</sup>

---

<sup>12</sup> Rojas Amandi, Víctor Manuel. Op. Cit. Pág. 3.

<sup>13</sup> Gutiérrez Cortés Fernando e Islas Carmona Octavio. **APUNTES ACADÉMICOS PARA UNA HISTORIA DE INTERNET EN MÉXICO** .[www.mexicanadecomunicacion.com.mx/tables/FMB/foromex/apuntes.html](http://www.mexicanadecomunicacion.com.mx/tables/FMB/foromex/apuntes.html).

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 el Centro Nacional de Investigación Atmosférica (NCAR) 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:

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, fueron la Universidad de las Américas en Cholula Puebla; el 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 ITEM fueron el Colegio de Postgraduados 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 Guanajuato pudo conectarse a través de la UNAM.

b) Los segundos fueron aquellas universidades que pudieron establecer una conexión a Internet mediante una Institución académica 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.

A inicio de los 90's fue creado el organismo RED-MEX constituido por diferentes instituciones académicas que se dedicaba a discutir políticas, estatutos y procedimientos con el fin de regular el desarrollo de la 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 Americas ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad de Veracruz, Instituto de Ecología, Universidad Iberoamericana e Instituto de Mexicali, se crea MEX-net<sup>14</sup> el cual se encargaría de decodificar, propiciar y contribuir en el desarrollo de Internet en México.

Durante 1983 y 1993 el uso de la Internet era exclusivamente con fines académicos y de investigación a través de las principales instituciones de educación

---

<sup>14</sup> Internet Society. **HISTORIA DE LA INTERNET EN MÉXICO**. <http://www.isocmex.org.mx/historia.html>

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 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, consiguieron 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 creación 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.mx) 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 varias instituciones educativas y las primeras empresas mexicanas interesadas en Internet.

En 1995 el número de servidores (WWW) creció 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 creación del Centro de Información de Redes de

México (NIC-México) la cual era la responsable de administrar y coordinar los recursos de la Internet en México<sup>15</sup>.

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 contribuyen en establecer los fundamentos de una cultura en la 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 cooperación 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 responsabilidad es asegurar la alta disponibilidad de la red y el rápido reconocimiento de fallas y degradación del servicio<sup>16</sup>.

#### **- Servicios en la Internet.**

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

---

<sup>15</sup> NIC-México, **HISTORIA DE NIC-MÉXICO**, <http://www.nic.mx/es/NicMexico.Historia>

<sup>16</sup> Téllez Valdés, Julio. **DERECHO INFORMÁTICO**. Tercera Edición. Editorial Mc Graw Hill, México 2003. Pág. 85.

**Como medio de comunicación,** la red entre computadores permite la comunicación entre sí y entre los usuarios realizada mediante cable telefónico o conexión por línea de alta 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 acceso a la espina dorsal del mismo Internet (backbone). Los medios de comunicación más populares en la Internet se encuentran en el Correo Electrónico (e-mail), la comunicación mediante 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 mediante 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 consiste en que éste necesita contacto directo 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 defecto mecanografiado y corregirlo, el correo electrónico por otro lado los datos e información transmitida puede ser modificada a través de un procesador de palabras (Word, TXT).

**Como comunicación mediante foros de discusión,** se lleva a cabo mediante páginas especializadas en el que se mantiene 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 conversación con personas desconocidas.

**Como medio de información**, la Internet se considera como una gran biblioteca por su amplio contenido de documentos considerado como el más grande y completo del mundo en el cual cualquier persona tiene acceso desde cualquier terminal y desde cualquier parte 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 propicia el crecimiento del contenido de la información disponible, pero el principal problema radica en la veracidad de 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 ésta deberá seguir con lo cual es imposible poner cuotas a su uso por la información consultada, por tal razón el costo del uso de la Internet se dividen entre todos los usuarios, de tal forma sólo son impuestas cuotas mínimas a los usuarios a través de los servidores de acceso a Internet.

### **- Organización de la Internet.**

Consta básicamente de una organización no jerarquizada y que todas las computadoras y sistemas de redes con capacidad de acceso a la información así como de los servicios disponibles en Internet, toda esta información y servicio no se encuentran depositados en una computadora central o red determinada sino son transmitidas entre varias computadoras. Tampoco es posible perder la información debido a que siempre es posible encontrar otra ruta para obtener la información perdida.

Una de las características importantes de la Internet es la autorregulación, consta de un programa denominado TCP/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 teléfono, pero donde la comunicación es directa entre las partes.

### **- Denominación.**

Cada servicio de información cuenta con sus propias direcciones con el fin de acceder de manera fácil y rápida mediante 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).

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

1. (URL), Localizador Uniforme de Recursos, que especifica cómo a cada página de información se asocia a una dirección 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 Hipertexto un método para codificar la información de los documentos y sus enlaces

Puede referirse a una (web) como una página, sitio o conjunto de sitios que proveen información por los medios descritos, o a la (web), que es la enorme e interconectada red disponible prácticamente en todos los sitios de la Internet, ejemplo:

Servicio:// nombre del sistema . dominio . nivel más elevado . código o país / ruta  
 /archivo; Facultad de Derecho UNAM: <http://www.Derecho.unam.mx>

Una dirección de Internet puede tener más de una sola sección, un ejemplo es la dirección de la enciclopedia Wikipedia: WIKIPEDIA Enciclopedia libre:  
<http://es.wikipedia.org/wiki/Portada>

El nivel de dominio más elevado es pieza importante en una dirección debido a que indica el tipo de organización a la que pertenece el dominio, ejemplo de las más comunes:

1. .com organización comerciales.
2. .edu universidades y otras instituciones de enseñanza.
3. .gov organizaciones estatales.
4. .net sistema de la red y administración de Internet.
5. .org otras organizaciones

Otra parte de la dirección en especial para los portales fuera de los Estados Unidos es la utilización 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	Turquia
.cz	Republica checa	.ie	Irlanda	.no	Noruega	.us	E.U.A
.de	Alemania	.il	Israel	.nz	Nueva Zelanda	.uk	Gran Bretaña

### **- Dirección de Correo Electrónico (e-mail).**

Incluye el nombre del usuario seleccionado por el mismo usuario o el prestador del servicio de correo, luego se agrega el símbolo @ (arroba) que en inglés significa “en”, a continuación el nombre del servidor, el dominio y el nivel más elevado si es que éste lo tuviera, ejemplo: Usuario @ servidor . Nivel más elevado . código del país

### **1.3. Campos de acción de la Informática.**

La Informática ha sido utilizada 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.

## - 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”<sup>17</sup>. Actualmente tiene un enfoque sistemático y los beneficios de las nuevas tecnologías han sido enormes y difícil 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.

**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

---

<sup>17</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA.** Op. Cit. Tomo 2. Pág. 216.

Laboratory)<sup>18</sup> 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 Nüsslein-Vollhard y Erich Wieschaus lo cual les concedieron el premio Nóbel de Medicina em ese mismo año.

Otro segundo centro en surgir con estos mismos propósitos fue el GenBank en los E.U.A. que en 1987 se transformó en el International Nucleotide Sequence Database Collaboration<sup>19</sup>, 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 Gigabites (cien millones de Bites) y se siguen sumando por mes más de 3 millones de secuencias genéticas nuevas.

---

<sup>18</sup> EMBL HEIDELBERG, EUROPEAN MOLECULAR BIOLOGY LABORATORY. <http://www.embl-heidelberg.de/>

<sup>19</sup> INTERNATIONAL NUCLEOTIDE SEQUENCE DATABASE COLLABORATION <http://www.ncbi.nlm.nih.gov/projects/collab/>

### **- 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 imaginada que antes eran tardadas o en muchas ocasiones imposibles de hacer para una 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 la Internet han revolucionado los campos de estudios y uso de a 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:

#### **- La Informática en la Economía y Administración.**

La Informática dentro de la Administración y la Economía ha tenido una gran aceptación causado que en todas sus ramas han generado beneficios en la realización de sus actividades, por ejemplo: el uso de sistemas computacionales 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.

#### **- 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 los diferentes fases de la producción lo que permite la producción en masa y a la vez reducir costos.

#### **- 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 emplee 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 conscientes 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, 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 enfocan 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, que no siempre son útiles para las necesidades educativas y resultan 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 uso de 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 edad 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 el grado y edad de los alumnos con el fin de optimizar el aprendizaje. Otro problema es que 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.

### **- 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 la 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 debe permanecer ajeno a estos adelantos tecnológicos y responder 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 nuevas tecnologías, con lo que se han creado otras ramas o denominaciones para poder dar solución y entendimiento a estos problemas y sin duda a los beneficios como las siguientes:

**- Derecho Informático.**

Se puede hablar de los primeros señalamientos de un 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 ésta relación se da a través de la comunicación.

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.”<sup>20</sup>.

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.

#### **- Derecho a la Informática y a la información.**

Bajo esta idea ha surgido como base a lo que denominaré: “Derecho a la información”, en este campo Carlos M. Correa autor Argentino en su obra Derecho Informático la denomina como: “La Teoría Jurídica de la Información”<sup>21</sup> donde en 1987 y basado en las teorías francesas de esa época en especial de Pierre Catála, donde ya tienen marcado un objeto de estudio, el cual es la Información como una mercancía, donde Pierre Catála sostiene que ésta información “tiene un valor patrimonial y es susceptible de apropiación”<sup>22</sup> 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

---

<sup>20</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA. Op. Cit.** Tomo 6. Pág. 863.

<sup>21</sup> Correa, Carlos M. Carlos, **DERECHO INFORMÁTICO.** Editorial Desalma Buenos Aires Argentina 1999. Pág. 287.

<sup>22</sup> *Ibidem.* Pág. 288.

personales las cuales únicamente conciernen 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.

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.

Herminio Tomás Azpilicueta autor Argentino, 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 delincencial, 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 misma causas. Otras ramas en las que señala son el Derecho de Trabajo, Derecho Fiscal y el Derecho Procesal.

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 puede decir que el Derecho Informático es interdisciplinario, por lo que no puede ser ubicada en una sola rama del Derecho exclusivamente.

Este término ha venido evolucionando junto con las nuevas tecnologías hasta llegar a la definición dada por 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”<sup>23</sup>. 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”.

#### **- 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 por 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, Julio Téllez Valdez la define como: “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los

---

<sup>23</sup> Téllez Valdés, Julio. Op. Cit. Pág. 17.

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”<sup>24</sup>.

### **- 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.

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 se 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 Hermilio Tomás Azpilcueta en su obra<sup>25</sup>, 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

---

<sup>24</sup> Ibidem. Pág. 19.

<sup>25</sup> Azpilcueta Hermilio, Tomas. **DERECHO INFORMATICO**. Editorial Abeledo-Perrot Buenos Aires Argentina 1996. Pág. 55.

cada uno de los principios informáticos a toda actividad jurídica y ésta a su vez la clasificaba en tres grupos:

1.- Informática Registral: Consiste en la rapidez y facilidad de accesibilidad a registros públicos en especial, dando como ventajas del recuperar dichos registros de manera instantánea y llevar a cabo labores estadísticas, así como evitar el monto de papel utilizado y facilitar los trámites.

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

3.- Informática Desicional: Hermilio Tomás Azpicueta 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 Informática 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,

4.- 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.

Otra forma en la que puede ser clasificada la Informática Jurídica es<sup>26</sup>:

**1.- Informática Jurídica Documentaria:** 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.

**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:

**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 judiciales conocido como "Informática Judicial"<sup>27</sup>, 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

---

<sup>26</sup> Téllez Valdés, Julio. Op. Cit. Pág. 28.

<sup>27</sup> Ibidem. Pág. 35.

fases del proceso y el estado del juicio y en un momento en el futuro dejar de asistir a tribunales y ser consultables por vía telemática.

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, redacción, verificación de escritos y funciones 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.

c) Investigación o Informática Jurídica Analítica: Consta de los 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 personales de los delincuentes analizando los antecedentes, medios profesionales, familiares, económicos, etc.

e) Redacción: Consiste en la ayuda y corrección en la redacción de textos en especial legislativos, durante la creación mediante un programa especializado enfocado en la 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. Indexación, 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 completos de forma lógica a través de restrictores de distancia en el cual puede ser organizarlo y consultarlo con mayor facilidad.

b) La formación 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:**

Consistente 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 realizar trabajo creativo en el campo el Derecho

### **- La Internet y el Derecho.**

Con la llegada de la Internet diferentes ramas de la 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 permita 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 electrónico 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 envío 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 a cualquier parte del mundo de manera más segura hasta 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 del correo común, en especial si ésta es realizada en diferentes partes del mundo. Otra ventaja es el ahorro de tiempo y trabajo debido a que el correo electrónico es un envío 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 presenta 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 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 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 correos 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 filtraciones de información, las medidas de seguridad a seguir son básicamente en mantener apagados los dispositivos de comunicación inalámbrica cuando éstos no son utilizados y contar con programas denominados Anti-Virus 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 considera son:

- [Gmail.google.com](mailto:Gmail.google.com)
- [www.hotmail.com](http://www.hotmail.com)
- [www.pordigy.com.mx](http://www.pordigy.com.mx)
- [www.terra.com.mx](http://www.terra.com.mx)
- [mx.yhooo.com](http://mx.yhooo.com)

### **- Foros de Discusión o grupos LISTSERV.**

Este tipo de medio de comunicación por Internet resulta de mayor facilidad y nace de la necesidad de intercambiar información y mensajes entre las personas pertenecientes a la comunidad; los grupos LISTSERV consisten en una lista de correos electrónicos trabajando con una computadora central el cual envía la información o preguntas a cada uno de los correos electrónicos en la lista de miembros; los foros de discusión dependen de una computadora central en el cual queda a disposición de todos los usuarios en el cual se puede dejar información, opiniones etc. las cuales pueden ser vistas por otras personas o los miembros los cuales pueden dejar contestación, o a su vez dejar información comentarios u opiniones, ambos sistemas pueden ser públicos pero la mayoría necesita de un registro para pertenecer el grupo de discusión.

### **- 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 posean 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 conferencia, con lo que representa ahorro de dinero a comparación con el teléfono en especial en llamadas de larga distancia, además, de interactuar a la vez con un mayor número de personas que 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 y accesible del mundo, debido a que desde cualquier parte del mundo puede consultarse cualquier tipo 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 páginas 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 gratuita si así se dispone; la desventaja consiste en que no todo lo publicado en Internet en cierto o actualizado en 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.e-Mexico.gob.mx:80/wb2/eMex/eMex> Diario Oficial de la Federacion

<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://info4.juridicas.unam.mx/ijure/fed/9/>

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

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

**- Leyes Federales:**

<http://info4.juridicas.unam.mx/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=api>

**- 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 ha 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 espacio de oficina; mejor calidad del trabajo, reducción de costos en la gestión de clientes, mejoras en las condiciones de trabajo, permanencia del servicio, velocidad de actuar y calidad de vida.

No sólo en la 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; Julio Tellez Valdes 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”<sup>28</sup> con lo que para la defensa de los ciudadanos y empresas se pretenden establecer diferentes medios para la solución de controversias y su 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

---

<sup>28</sup> Ibidem. Pág.46.

fueron en el año de 1996 en los Estados Unidos de América con la aparición de Virtual Magistrate<sup>29</sup> 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 de usar el mismo sistema u otros disponibles en la red.

Un segundo “Cybertribunal” es el The Online Ombuds Office<sup>30</sup> fue establecido en Junio de 1996 bajo la iniciativa del Center of Information Technology and Sioute Resolution de la Universidad de Massachussets, que consiste en un servicio de mediación para la resolución de decisiones para personas e instituciones surgidas 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 propiedad intelectual.

Otro de los denominados Cibertribunales fue el Cyber-Court un proyecto de corta 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

---

<sup>29</sup> **VIRTUAL MAGISTRATE:** <http://www.vmag.org/>

<sup>30</sup> **THE ONLINE OMBUDS OFFICE:** <http://www.ombuds.org/center/ombuds.html>

Moderador en las mediaciones y prestar asistencia técnica o administrativa. Al término de este fue creado el “Resolution”<sup>31</sup> que continuó con este mismo trabajo.

Por ahora todos los intentos de un Cybertribunal están esencialmente enfocados a un arbitraje entre las partes por conflictos derivados del uso de servicios en Internet, creados por particulares; pero cabe la posibilidad que en un futuro existan Cybertribunales 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 pueda 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 Cybertribunal 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 Cybertribunales 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

---

<sup>31</sup> **ERESOLUTION:** <http://www.udrpinfo.com/eres/>

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 Cybertribunal depende de los conocimientos y honestidad de quien está encargada de la vigilancia y creación de un Cybertribunal o quien hace uso de el, la interacción entre las partes se vería disminuida o eliminada casi en su totalidad. Aunque con la idea de los Cybertribunales no puede ser tomada a la ligera y ser tema de estudio en trabajos posteriores.

#### **- La Cibernética Jurídica.**

Los avances en las 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 procesos de la inteligencia humana”<sup>32</sup>. Aunque en los campos de la Inteligencia Artificial apenas está dando sus primeros pasos la idea de que una computadora pueda tomar decisiones jurídicas por sí mismo sin la

---

<sup>32</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA.** Op. Cit. Tomo 6. Pág. 873.

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 sí, sino que ésta pueda proporcionar auxilio en las tomas de decisiones jurídicas como una herramienta y éstas para un funcionamiento óptimo deben contener como 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 permitan 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 estudiosos 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 los avances en la tecnología siempre trae sorpresas en el futuro.

### **- 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 herramienta 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 comerciales 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 daba 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 esta problemática ha surgido el Derecho de la Informática para poder dar solución a estos conflictos, entendiendo como tal al: “Conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”<sup>33</sup>, 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.
- 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.

---

<sup>33</sup> Téllez Valdés, Julio. Op. Cit. Pág. 21.

- 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 con 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 una 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 usados 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.

Las 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 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 las 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 la 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-Room) 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 comercial 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, cuantas 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 sería 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 comprometedor 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 sin fin 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 1978 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 presenta 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”<sup>34</sup> y su ley orgánica de protección de datos de carácter personal del 13 de diciembre de 1999.

---

<sup>34</sup> **Constitución Española** [http://www.constitucion.es/otras\\_constituciones/espana/index.html](http://www.constitucion.es/otras_constituciones/espana/index.html)

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 lo Datos de Carácter Personal del 28 de Enero de 1981 conocido como el Convenio de Estrasburgo por el consejo Europeo<sup>35</sup> 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 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 Económicos) 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

---

<sup>35</sup> **CONVENIO N° 108 DEL CONSEJO, de 28 de Enero de 1981, DE EUROPA PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL** <http://www.apdcat.net/media/246.pdf>

(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 es 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 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, interceptación de datos, revelación de información confidencial, control y alteración de documentos fuente, extravío de información, tarifas y régimen fiscal, 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 del enero de 1981 donde también se enfocó en el tratamiento de transferencia de datos transfronterizos aplicable a los países miembros.

Otro beneficio 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 empresas 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 informáticos 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 encontrando 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 necesitan 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 transferirla, usarla, explotarla o incluso recibirla, el cual al ser creación del intelecto del autor el 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 objeto: son todos aquellos que tienen la funciones específicas 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 cómputos convencional.

De esto se derivan un sinnfín 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 incompletos 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 puedan ser usados y por lo cual exclusivamente pueden ser descifrados por compañías especializadas o incluso por la misma empresa, lo que trae 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 computadoras 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 cómputo 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.

- **Contratación electrónica y comercio electrónico.**

Con el creciente uso de las 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.
- Consultoría y asesora 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 tipos 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 a el 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, en 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 contratado 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 pueden 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, otro especie de este contrato abarca la consulta de datos, documentación técnica, estudios de mercados, 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 levantó la prohibición de los usos comerciales en la Internet, se ha proliferado esta activada 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, aún 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 páginas 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 sólo 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 ofrecería 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 la 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 es 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](http://www.deremate.com.mx) , [www.amazon.com](http://www.amazon.com).

- Centros Comerciales: [www.liverpool.com.mx](http://www.liverpool.com.mx)  
[www.elpalaciodehierro.com.mx](http://www.elpalaciodehierro.com.mx), [www.sears.com.mx](http://www.sears.com.mx)
- Portal Comercial: [www.todito.com](http://www.todito.com), [www.esmas.com](http://www.esmas.com),  
[www.prodigy.msn.com](http://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 posee 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 almacenadas 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 ha 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 eléctricos 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 mas 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 disk), 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 por 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 escaners y lectores ópticos para capturar textos 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 por que 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 representan 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 2000 existen diversos 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 encuentre en medios electrónicos, ópticos o en cualquier otra tecnología y para poderla valorar se deberá estimar 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. 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 o archivada 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 consulta.

El segundo Ordenamiento en aparecer fue el Código de Comercio en su artículo 1205 en el que se tiene admisible como prueba los "Mensajes de datos" y por último se encuentra el artículo 1298-A donde los mensajes de datos para que puedan ser valorados deberá estimarse la confiabilidad del método utilizado para generar la, archivarla, comunicarla y ser conservada.

Como se ha podido observar la Informática ha aparecido en todas las actividades 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 diversas Ciencias como es el Derecho, sirviendo de consulta para el desarrollo del presente Capítulo.

El apasionante mundo de la Informática ha sido en los últimos cinco años y será una gran herramienta para la Ciencia del Derecho por lo que es de gran importancia darle un marco jurídico adecuados 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 diversificación como se verá en el Capítulo segundo.

## **CAPÍTULO 2.- Marco jurídico sobre la Informática Jurídica y los Delitos Informáticos.**

Dentro de nuestro sistema jurídico se mantiene la supremacía por parte de la Constitución Política de los Estados Unidos Mexicanos, que conforme con la tradicional pirámide de Hans Kelsen se encuentra en la cúspide de todos los demás ordenamientos jurídicos. Por lo tanto, todas las leyes federales y locales, los tratados internacionales, los reglamentos y demás disposiciones jurídicas estarán supeditadas a la Carta Magna.

Han existido diversas posturas sobre la jerarquía en la que deben guardar los tratados internacionales, encontrando quienes sostienen que están por encima de las leyes federales y otros que le asignan el mismo nivel.

Cabe precisar que México se encuentra conformada en una Federación integrada por Estados libres y soberanos en sus tres poderes: Ejecutivo, Legislativo y Judicial; es decir, cada entidad federativa cuenta con un titular del ejecutivo (gobernador), un congreso local , así como un tribunal autónomo, en donde cada uno se encargará de desarrollar sus funciones en sus correspondientes Estados atendiendo a factores muy particulares del mismo denotándose así la existencia de una diversidad de sociedades que Miguel Reale denominara la “Tridimensionalidad del Derecho”<sup>36</sup>.

---

<sup>36</sup> Reale, Miguel. **LA TEORIA 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. Pág. 103.**

Así es como vamos a encontrar en el ámbito legislativo la creación de leyes que deben de atender a la sociedad de cada una de las entidades federativas, respetando sus valores existentes de cada uno de ellos y al marco jurídico de sus atribuciones y las leyes secundarias, las cuales deben estar acordes con la Carta Magna Federal que es el resultado del pacto federal que tienen los estados entre sí.

Por tal motivo, es que en la creación de las figuras ilícitas vamos a encontrar delitos federales y locales, atendiendo a la legislatura federal o común que les ha dado creación y las necesidades que deben atenderse en cada ámbito.

En materia legislativa a efecto de distinguir entre el ámbito federal y local, existe un principio llamado de “exclusión”, que señala: “es local lo que no es federal”, es decir la legislación local podrá crear leyes sobre las materias que no estén reservadas para la Federación, encontrando su fundamento en el Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

De manera similar sucede para la creación de las figuras delictivas encontrado ese principio de exclusión en los artículos 73, fracción XI de la Carta Magna y 50 de la Ley Orgánica del Poder Judicial de la Federación. Situación que se contempló en el Capítulo anterior.

Por lo que no obstante de que aparentemente encontramos delitos regulados simultáneamente en el ámbito federal y en el local, mantienen siempre puntos

diferenciales, sobre todo por que los delitos federales pretenden proteger a la Federación.

Ejemplo de ellos tendríamos un delito de robo (patrimonial) que lo podemos encontrar en el Código Penal Federal (artículo 367) y en Código Penal para el Distrito Federal en el (artículo 220), así como en otras legislaciones estatales; sin embargo, para que sea el robo competencia federal debe darse con alguna de las hipótesis encontradas en el artículo 50 de la Ley Orgánica del Poder Judicial de la Federación tales como; encontrarse en una ley federal, que el objeto materia del robo pertenezca a la Federación por que el sujeto pasivo será ésta, o bien, por que sujeto en ejercicio de sus funciones de índole federal se apodera de un objeto mueble sin derecho, entre otras hipótesis más; en caso de que no se cumpla con estos requisitos previstos por este artículo 50 estaremos en presencia de un robo del fuero común, aplicándose el Código Penal de la entidad federativa correspondiente.

Han sido numerosos los intentos para conformar un Código Penal para todos los estados de la Republica Mexicana con resultados infructuosos en virtud de que se ha requerido mantener la soberanía de cada Estado integrante de la Federación, los valores de sus habitantes, entre otros argumentos más.

El desarrollo de las nuevas tecnologías y la Informática han abierto las puertas a nuevas posibilidades de delincuencia que antes nunca fueron imaginadas, mediante los cuales es posible obtener grandes pérdidas económicas o causar importantes daños materiales o morales.

En el caso de los Delitos Informáticos los hemos encontrado regulados en el ámbito federal en los artículos del 211 bis1 al 211bis 7, del Código Penal Federal, así como en el ámbito común como “Delitos Informáticos” propiamente dicho en el Artículo 217 del Código Penal para el Estado de Sinaloa y en el Artículo 181 del Código Penal para el Estado libre y soberano de Veracruz-Llave.

Esta legislación debe estar siempre respetando las garantías Constitucionales tales como el de legalidad plasmada en los artículos 14 y 16, entre otros preceptos que hacen referencia a la materia penal.

## **2.1 Constitución Política de los Estados Unidos Mexicanos.**

Nuestra Carta Magna precisa los derechos fundamentales del hombre como contienen las garantías que este debe gozar en el territorio nacional y como lo precisa el artículo 1 que dice:

**Artículo 1o.-** En los Estados Unidos Mexicanos todo individuo gozará de las garantías que otorga esta constitución, las cuales no podrán restringirse ni suspenderse, sino en los casos y con las condiciones que ella misma establece.

Existen legislaciones secundarias que son reglamentarias de algunos artículos Constitucionales como el Derecho Laboral (artículo 123), el Derecho Agrario (artículo 27), entre otros. En el caso del Derecho Penal no puede constituirse en un derecho reglamentario de algún precepto jurídico determinado, ya que éste va dirigido a velar por los intereses de toda la sociedad ante la comisión de conductas antisociales que el

legislador ha considerado como delitos, siendo que también podemos encontrar conductas antisociales que no se consideran delitos sino pudieran ser infracciones administrativas, entonces estaríamos en presencia del Derecho Administrativo, contempladas en leyes o reglamentos de tal naturaleza, como serían: los reglamentos administrativos de buen gobierno; la Ley Federal de las Responsabilidades Administrativas de los Servidores Públicos, el Código Fiscal de la Federación, la Ley Aduanera y la Ley Federal del Derecho de Autor en sus respectivos Capítulos de faltas, entre otras legislaciones más.

Cabe precisar por lo que respecta a los delitos, éstos serán federales o locales conforme a lo señalado por la propia Constitución Federal a través del principio conocido como “reserva legal” antes comentado, que es la facultad exclusiva del legislador de definir hipótesis delictivas, al indicar:

**TÍTULO TERCERO**  
**CAPÍTULO II DEL PODER LEGISLATIVO**  
**SECCIÓN III DE LAS FACULTADES DEL CONGRESO**

**Artículo 73.** El Congreso tiene facultad:

XXI. Para establecer los delitos y faltas contra la Federación y fijar los castigos que por ellos deban imponerse.

Las autoridades federales podrán conocer también de los delitos del fuero común, cuando éstos tengan conexidad con delitos federales;

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;

La Constitución Política de los Estados Unidos Mexicanos establecidos en sus diversas disposiciones las garantías que deben de cumplirse en la materia penal mencionando a continuación algunos de ellos:

Las garantías penales se encuentran contempladas en los siguientes artículos Constitucionales, las cuales se deben respetar tanto en el Derecho Penal y en el Derecho Procesal Penal.

## **TÍTULO PRIMERO CAPÍTULO I DE LAS GARANTÍAS INDIVIDUALES**

**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 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.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querrela de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado.

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.

En los casos de delito flagrante, cualquier persona puede detener al indiciado poniéndolo sin demora a disposición de la autoridad inmediata y ésta, con la misma prontitud, a la del Ministerio Público.

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.

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 y que será escrita, 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 una 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. 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, por escrito, 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.

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 prescriptas 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.

**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.

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.

Nadie puede ser aprisionado por deudas de carácter puramente civil.

**Artículo 18.** Sólo por delito que merezca pena corporal habrá lugar a prisión preventiva. El sitio de ésta será distinto del que se destinare para la extinción de las penas y estarán completamente separados.

Los Gobiernos de la Federación y de los Estados organizarán el sistema penal, en sus respectivas jurisdicciones, sobre la base del trabajo, la capacitación para el mismo y la educación como medios para la readaptación social del delincuente. Las mujeres compurgarán sus penas en lugares separados de los destinados a los hombres para tal efecto.

Los Gobernadores de los Estados, sujetándose a lo que establezcan las leyes locales respectivas, podrán celebrar con la Federación convenios de carácter general, para que los reos sentenciados por delitos del orden común extingan su condena en establecimientos dependientes del Ejecutivo Federal.

La Federación y los Gobiernos de los Estados establecerán instituciones especiales para el tratamiento de menores infractores.

Los reos de nacionalidad mexicana que se encuentren compurgando penas en países extranjeros, podrán ser trasladados a la República para que cumplan sus condenas con base en los sistemas de readaptación social previstos en este artículo, y los reos de nacionalidad extranjera sentenciados por delitos del orden federal en toda la República, o del fuero común en el Distrito Federal, podrán ser trasladados al país de su origen o residencia, sujetándose a los Tratados Internacionales que se hayan celebrado para ese efecto. Los gobernadores de los Estados podrán solicitar al Ejecutivo Federal, con apoyo en las leyes locales respectivas, la inclusión de reos del orden común en dichos Tratados. El traslado de los reos sólo podrá efectuarse con su consentimiento expreso.

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 readaptación social.

Artículo 18. Sólo por delito que merezca pena corporal habrá lugar a prisión preventiva. El sitio de ésta será distinto del que se destinare para la extinción de las penas y estarán completamente separados.

Los Gobiernos de la Federación y de los Estados organizarán el sistema penal, en sus respectivas jurisdicciones, sobre la base del trabajo, la capacitación para el mismo y la educación como medios para la readaptación social del delincuente. Las mujeres compurgarán sus penas en lugares separados de los destinados a los hombres para tal efecto.

Los Gobernadores de los Estados, sujetándose a lo que establezcan las leyes locales respectivas, podrán celebrar con la Federación convenios de carácter general, para que los reos sentenciados por delitos del orden común extingan su condena en establecimientos dependientes del Ejecutivo Federal.

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.

La operación del sistema en cada orden de gobierno estará a cargo de instituciones, tribunales y autoridades especializados en la procuración e impartición de justicia para adolescentes. Se podrán aplicar las medidas de orientación, protección y tratamiento que amerite cada caso, atendiendo a la protección integral y el interés superior del adolescente.

Las formas alternativas de justicia deberán observarse en la aplicación de este sistema, siempre que resulte procedente. En todos los procedimientos seguidos a los adolescentes se observará la garantía del debido proceso legal, así como la independencia entre las autoridades que efectúen la remisión y las que impongan las medidas. Éstas deberán ser proporcionales a la conducta realizada y tendrán como fin la reintegración social y familiar del adolescente, así como el pleno desarrollo de su persona y capacidades. 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 reos de nacionalidad mexicana que se encuentren cumpliendo penas en países extranjeros, podrán ser trasladados a la República para que cumplan sus condenas con base en los sistemas de readaptación social previstos en este artículo, y los reos de nacionalidad extranjera sentenciados por delitos del orden federal en toda la República, o del fuero común en el Distrito Federal, podrán ser trasladados al país de su origen o residencia, sujetándose a los Tratados Internacionales que se hayan celebrado para ese efecto. Los gobernadores de los Estados podrán solicitar al Ejecutivo Federal, con apoyo en las leyes locales respectivas, la inclusión de reos del orden común en dichos Tratados. El traslado de los reos sólo podrá efectuarse con su consentimiento expreso.

Los sentenciados, en los casos y condiciones que establezca la ley, podrán cumplir sus penas en los centros penitenciarios más cercanos a su domicilio, a fin de propiciar su reintegración a la comunidad como forma de readaptación social.

**Artículo 19.** Ninguna detención ante autoridad judicial podrá exceder del plazo de setenta y dos horas, a partir de que el indiciado sea puesto a su disposición, sin que se justifique con un auto de formal prisión en el que se expresarán: el delito que se impute al acusado; el lugar, tiempo y circunstancias de ejecución, así como los datos que arroje la averiguación previa, los que deberán ser bastantes para comprobar el cuerpo del delito y hacer probable la responsabilidad del indiciado.

Este plazo podrá prorrogarse únicamente a petición del indiciado, en la forma que señale la ley. La prolongación de la detención en su perjuicio será sancionada por la ley penal. La autoridad responsable del establecimiento en el que se encuentre internado el indiciado, que dentro del plazo antes señalado no reciba copia autorizada del auto de formal prisión o de la solicitud de prórroga, deberá llamar la atención del juez sobre dicho particular en el acto mismo de concluir el plazo y, si no recibe la constancia mencionada dentro de las tres horas siguientes, pondrá al indiciado en libertad.

Todo proceso se seguirá forzosamente por el delito o delitos señalados en el auto de formal prisión o de sujeción a proceso. Si en la secuela de un proceso apareciere que se ha cometido un delito distinto del que se persigue, deberá ser objeto de averiguación separada, sin perjuicio de que después pueda decretarse la acumulación, si fuere conducente.

Todo mal tratamiento en la aprehensión o en las prisiones, toda molestia que se infiera sin motivo legal, toda gabela o contribución, en las cárceles, son abusos que serán corregidos por las leyes y reprimidos por las autoridades.

**Artículo 20.** En todo proceso de orden penal, el inculpado, la víctima o el ofendido, tendrán las siguientes garantías:

A. Del inculpado:

I. Inmediatamente que lo solicite, el juez deberá otorgarle la libertad provisional bajo caución, siempre y cuando no se trate de delitos en que, por su gravedad, la ley expresamente prohíba conceder este beneficio. En caso de delitos no graves, a solicitud del Ministerio Público, el juez podrá negar la libertad provisional, cuando el inculpado haya sido condenado con anterioridad, por algún delito calificado como grave por la ley o, cuando el Ministerio Público aporte elementos al juez para establecer que la libertad del inculpado representa, por su conducta precedente o por las circunstancias y características del delito cometido, un riesgo para el ofendido o para la sociedad.

El monto y la forma de caución que se fije, deberán ser asequibles para el inculpado. En circunstancias que la ley determine, la autoridad judicial podrá modificar el monto de la caución. Para resolver sobre la forma y el monto de la caución, el juez deberá tomar en cuenta la naturaleza, modalidades y circunstancias del delito; las características del inculpado y la posibilidad de cumplimiento de las obligaciones procesales a su cargo; los daños y perjuicios causados al ofendido; así como la sanción pecuniaria que, en su caso, pueda imponerse al inculpado.

La ley determinará los casos graves en los cuales el juez podrá revocar la libertad provisional;

II. No podrá ser obligado a declarar. Queda prohibida y será sancionada por la ley penal, toda incomunicación, intimidación o tortura. La confesión rendida ante cualquier autoridad distinta del Ministerio Público o del juez, o ante éstos sin la asistencia de su defensor carecerá de todo valor probatorio;

III. Se le hará saber en audiencia pública, y dentro de las cuarenta y ocho horas siguientes a su consignación a la justicia, el nombre de su acusador y la naturaleza y causa de la acusación, a fin de que conozca bien el hecho punible que se le atribuye y pueda contestar el cargo, rindiendo en este acto su declaración preparatoria;

IV. Cuando así lo solicite, será careado, en presencia del juez, con quien deponga en su contra, salvo lo dispuesto en la fracción V del Apartado B de este artículo;

V. Se le recibirán los testigos y demás pruebas que ofrezca, concediéndosele el tiempo que la ley estime necesario al efecto y auxiliándosele para obtener la comparecencia de las personas cuyo testimonio solicite, siempre que se encuentren en el lugar del proceso;

VI. Será juzgado en audiencia pública por un juez o jurado de ciudadanos que sepan leer y escribir, vecinos del lugar y partido en que se cometiere el delito, siempre que éste pueda ser castigado con una pena mayor de un año de prisión. En todo caso serán juzgados por un jurado los delitos cometidos por medio de la prensa contra el orden público o la seguridad exterior o interior de la Nación;

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

VIII. 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;

IX. Desde el inicio de su proceso será informado de los derechos que en su favor consigna esta Constitución y tendrá derecho a una defensa adecuada, por sí, por abogado, o por

persona de su confianza. Si no quiere o no puede nombrar defensor, después de haber sido requerido para hacerlo, el juez le designará un defensor de oficio. 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,

X. 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.

Tampoco podrá prolongarse la prisión preventiva por más tiempo del que como máximo fije la ley al delito que motivare el proceso.

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

Las garantías previstas en las fracciones I, V, VII y IX también serán observadas durante la averiguación previa, en los términos y con los requisitos y límites que las leyes establezcan; lo previsto en la fracción II no estará sujeto a condición alguna.

Derogado.

B. 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 averiguación previa como en el proceso, y a que se desahoguen las diligencias correspondientes.

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 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. Cuando la víctima o el ofendido sean menores de edad, no estarán obligados a carearse con el inculpado cuando se trate de los delitos de violación o secuestro. En estos casos, se llevarán a cabo declaraciones en las condiciones que establezca la ley; y

VI. Solicitar las medidas y providencias que prevea la ley para su seguridad y auxilio.

**Artículo 21.** La imposición de las penas es propia y exclusiva de la autoridad judicial. La investigación y persecución de los delitos incumbe al Ministerio Público, el cual se auxiliará con una policía que estará bajo su autoridad y mando inmediato. 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 o arresto hasta por treinta y seis horas; pero si el infractor no pagare la multa que se le hubiese impuesto, se permutará ésta por el arresto correspondiente, que no excederá en ningún caso de treinta y seis horas.

Si el infractor 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 no excederá del equivalente a un día de su ingreso.

Las resoluciones del Ministerio Público sobre el no ejercicio y desistimiento de la acción penal, podrán ser impugnadas por vía jurisdiccional en los términos que establezca 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, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones policiales se regirá por los principios de legalidad, eficiencia, profesionalismo y honradez.

La Federación, el Distrito Federal, los Estados y los Municipios se coordinarán, en los términos que la ley señale, para establecer un sistema nacional de seguridad pública.

**Artículo 22.** Quedan prohibidas las penas de muerte, de mutilación, de infamia, la marca, los azotes, los palos, el tormento de cualquier especie, la multa excesiva, la confiscación de bienes y cualesquiera otras penas inusitadas y trascendentales.

No se considerará confiscación de bienes la aplicación total o parcial de los bienes de una persona hecha por la autoridad judicial, para el pago de la responsabilidad civil resultante de la comisión de un delito, o para el pago de impuestos o multas. Tampoco se considerará confiscación el decomiso que ordene la autoridad judicial, de los bienes, en caso del enriquecimiento ilícito, en los términos del artículo 109; ni el decomiso de los bienes propiedad del sentenciado, por delitos de los previstos como de delincuencia organizada, o el de aquéllos respecto de los cuales éste se conduzca como dueño, si no acredita la legítima procedencia de dichos bienes.

No se considerará confiscación la aplicación a favor del Estado de bienes asegurados que causen abandono en los términos de las disposiciones aplicables. La autoridad judicial resolverá que se apliquen en favor del Estado los bienes que hayan sido asegurados con motivo de una investigación o proceso que se sigan por delitos de delincuencia organizada, cuando se ponga fin a dicha investigación o proceso, sin que haya un pronunciamiento sobre los bienes asegurados. La resolución judicial se dictará previo procedimiento en el que se otorgue audiencia a terceros y se acredite plenamente el cuerpo del delito previsto por la ley como de delincuencia organizada, siempre y cuando se trate de bienes respecto de los cuales el inculpado en la investigación o proceso citados haya sido poseedor, propietario o se haya conducido como tales, independientemente de que hubieran sido transferidos a terceros, salvo que éstos acrediten que son poseedores o adquirentes de buena fe.

**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 prohíba 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.

Ahora bien, en el presente estudio de los delitos informáticos encontraremos temas muy relacionados como son el Derecho a la Información y a la propia información que puede corresponder al manejo de otras leyes especiales como la Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental, y la Ley Sobre Delitos de Imprenta, que tienen su fundamento en los artículos 6 y 7 Constitucionales.

**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.

*(Reformado mediante decreto publicado en el Diario Oficial de la Federación el 13 de Noviembre de 2007.)*

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.

*(Adicionado mediante decreto publicado en el Diario Oficial de la Federación el 20 de Julio de 2007.)*

**Artículo 7o.-** Es inviolable la libertad de escribir y publicar escritos sobre cualquier 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 mas 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 pretextos de las denuncias por delitos 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 aquellos.

## **2.2. Ley Federal del Derecho de Autor.**

Esta ley es reglamentaria del Artículo 28 de la Constitución Política de los Estados Unidos Mexicanos, tal como lo precisa en su artículo 1 que señala:

**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.

En los Delitos Informáticos previstos en los artículos del 211 bis1 al 211 bis 7 adicionados el 17 de mayo de 1999 en el Código Penal Federal se contempla que la conducta descrita en la hipótesis delictiva consiste principalmente en el "que sin autorización modifique, destruya o provoque pérdida de **información** contenida en un sistema o equipos de informática protegidos por algún mecanismo de seguridad" y al que "sin autorización conozca o copie **información** contenida en sistemas o equipos de información por algún mecanismo de seguridad" (Artículo 211 bis1).

Este delito en el ámbito federal como se verá en el Capítulo siguiente protege a la **información** que es contenida en un sistema de cómputo, sea particular, del Estado o bien de una entidad financiera como lo indican los subsecuentes artículos. Que a pesar de no hace referencia a lo que es **información** y lo que ésta deberá contener, aquí encontramos lo que es el Derecho a la Información.

Sin embargo el artículo 217 del Código Penal del Estado de Sinaloa tiene dos fracciones de diferente naturaleza que dicen:

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

I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

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

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

La fracción I, va encaminada a la comisión de un fraude o, a la obtención de un lucro a través de un sistema de cómputo.

En la fracción II, encontramos que las conductas descritas en la misma van a la trasgresión de un soporte lógico o programa de cómputo, que se puede dar a través de las conductas de interpretar, interferir, usar, alterar, dañar o destruir; sin embargo estas mismas conductas pueden ser dirigidas a la información contenida en un sistema de cómputo, con lo que en el primer caso estaríamos en presencia de la protección precisamente de los programas de computación y de las bases de datos que se encuentran bajo la tutela de la Ley Federal del Derecho de Autor en sus artículos del 101

al 113, y en el segundo caso se estaría en una hipótesis similar a la federal, es decir, atender contra la propia información.

Sobre la protección de los programas de cómputo y de base de datos la Ley Federal del Derecho de Autor menciona lo siguiente:

**TÍTULO IV DE LA PROTECCIÓN AL DERECHO DE AUTOR**  
**CAPÍTULO IV DE LOS PROGRAMAS DE COMPUTACIÓN Y LAS BASES DE DATOS**

**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 si 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. (DR)IJ

**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.

Al respecto, había que relacionar que si la protección de soportes lógico o programas de cómputo se encuentran regulados en la ley federal como la Ley Federal del Derecho de Autor, éstos pudieran volverse a proteger a nivel local previniéndose hipótesis delictivas como lo hace el artículo 217 del Código Penal para el Estado de Sinaloa.

### **2.3. Ley de la Propiedad Industrial.**

Dentro del termino “información” señalado en los delitos informáticos previstos en los artículos 211bis 1, al 211bis 7, del Código Penal Federal, es un término muy amplio y del cual no se hace referencia qué puede y qué debe contener, con lo que podría contraponerse con la revelación del secreto previsto en el Código Penal Federal y del secreto industrial contemplados en la Ley de la Propiedad Industrial.

La ley que define al secreto industrial es la Ley de la Propiedad Industrial que tiene su fundamento en los artículos 28 y 29 Constitucionales que señalan:

**Artículo 28.** En los estados unidos mexicanos quedan prohibidos los monopolios, las prácticas monopólicas, los estancos y las exenciones de impuestos en los términos y condiciones que fijan las leyes. El mismo tratamiento se dará a las prohibiciones a TÍTULO de protección a la industria.

....

Tampoco constituyen monopolios los privilegios que por determinado tiempo se concedan a los autores y artistas para la producción de sus obras y los que para el uso exclusivo de sus inventos, se otorguen a los inventores y perfeccionadores de alguna mejora.

.....

**Artículo 89.** Las facultades y obligaciones del Presidente son las siguientes:

XV. Conceder privilegios exclusivos por tiempo limitado, con arreglo a la ley respectiva, a los descubridores, inventores o perfeccionadores de algún ramo de la industria.

De igual forma se encuentra una estrecha relación entre los Delitos Informáticos previstos en los artículos del 211 bis1 al 211 bis 7 en el Código Penal Federal y el secreto industrial en la Ley de la Propiedad Industrial, debido a que en los Delitos Informáticos se contempla “que sin autorización modifique, destruya o provoque pérdida de **información** contenida en un sistema o equipos de informática protegidos por algún mecanismo de seguridad” y al que “sin autorización conozca o copie **información** contenida en sistemas o equipos de información por algún mecanismo de seguridad” (Artículo 211 bis1); información que es un término tan empleado que puede incluirse en el secreto industrial que prevé la Ley de Propiedad Industrial en los siguientes preceptos.

### **TÍTULO TERCERO DE LOS SECRETOS INDUSTRIALES CAPÍTULO ÚNICO**

**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 entra al dominio público o que es 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 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.

**Artículo 84.-** La persona que guarde un secreto industrial podrá transmitirlo o autorizar su uso a un tercero. El usuario autorizado tendrá la obligación de no divulgar el secreto industrial por ningún medio.

En los convenios por los que se transmitan conocimientos técnicos, asistencia técnica, provisión de ingeniería básica o de detalle, se podrán establecer cláusulas de confidencialidad para proteger los secretos industriales que contemplen, las cuales deberán precisar los aspectos que comprenden como confidenciales. (DR)IJ

**Artículo 85.-** Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado.

**Artículo 86.-** La persona física o moral que contrate a un trabajador que esté laborando o haya laborado o a un profesionista, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, será responsable del pago de daños y perjuicios que le ocasione a dicha persona.

También será responsable del pago de daños y perjuicios la persona física o moral que por cualquier medio ilícito obtenga información que contemple un secreto industrial.

**Artículo 86 BIS.-** La **información** requerida por las leyes especiales para determinar la seguridad y eficacia de productos farmoquímicos y agroquímicos que utilicen nuevos componentes químicos quedará protegida en los términos de los tratados internacionales de los que México sea parte.

**Artículo 86 BIS 1.-** En cualquier procedimiento judicial o administrativo en que se requiera que alguno de los interesados revele un secreto industrial, la autoridad que conozca deberá adoptar las medidas necesarias para impedir su divulgación a terceros ajenos a la controversia.

Ningún interesado, en ningún caso, podrá revelar o usar el secreto industrial a que se refiere el párrafo anterior.

A continuación mencionaré los delitos especiales previstos en la Ley de la Propiedad Industrial que protegen al secreto industrial.

## **TÍTULO SÉPTIMO DE LA INSPECCIÓN, DE LAS INFRACCIONES Y SANCIONES ADMINISTRATIVAS Y DE LOS DELITOS CAPÍTULO III DE LOS DELITOS**

**Artículo 223.-** Son delitos:

...

...  
...

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;

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

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.

Los delitos previstos en este artículo se perseguirán por querrela de parte ofendida.

**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.

No obstante que la Ley de la Propiedad Industrial contempla el secreto industrial y la revelación de secretos como un delito especial fuera del Código Penal Federal, este mismo contempla la revelación de secreto en sus artículos 210 al 211bis, que es un delito autónomo del mismo secreto que puede contemplarse dentro del término "Información". A continuación se transcriben dichos artículos del Código Penal Federal.

**LIBRO SEGUNDO**  
**TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**  
**CAPÍTULO I. REVELACIÓN DE SECRETOS**

**Artículo 210.** Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que

pueda resultar perjudicado, revele algún **secreto o comunicación reservada** que conoce o ha recibido con motivo de su empleo, cargo o puesto.

**Artículo 211.** La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

**Artículo 211 bis.** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, **información** o imágenes obtenidas en una intervención de comunicación privada, se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

**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.

Qué sucedería si una persona mediante sistemas informáticos irrumpe en una computadora y **conoce** la “**información**” de un “**Secreto**” de otra persona, la cual es usada para su beneficio divulgándolo a una tercera persona. En la hipótesis delictiva principal contemplada en los artículos 211bis 1 del Código Penal Federal donde “Al que sin autorización **conozca** o copie **información** contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad”, aunque el concepto de “**información**” es realmente amplio y puede este contener tanto el **secreto** como el **secreto industrial**, y puede ser llevados tanto a través de medios informáticos considerado como el conocido “espionaje cibernético” en el que el denominado “espía” puede acceder por medios electrónicos ya sea tanto físicamente o por vías redes como la Internet a computadoras donde almacenan la información del secreto industrial, pero éste tipo de delitos pueden ser llevados a través de otros medios no necesariamente informáticos, se tiene que recordar que éstos son delitos específicos previamente contemplados que si bien puede que sus objetos a proteger el secreto pueden entrar en

el termino “**información**” de la hipótesis delictiva del 211bis 1 y pueden ser realizados o no por medios informáticos por lo que no necesariamente entra en la denominación de “Delitos Informáticos” debido a que lo especial tiene preferencia a lo general aunque puede existir confusión.

## **2.4. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.**

Uno de los notorios intentos por los legisladores de modernizar a un México Democratizado es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la cual intenta acoplar otras legislaciones y una realidad de claridad y transparencia a los movimientos efectuados por los diversos niveles de gobierno, la que puede tomarse como referencia para los Delitos Informáticos materia de la presente investigación y en la que también se realiza la protección de la “información” así como algunas connotaciones al respecto tal y como se indica en los siguientes artículos:

### **TÍTULO PRIMERO DISPOSICIONES COMUNES PARA LOS SUJETOS OBLIGADOS CAPÍTULO I 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 3.** Para los efectos de esta Ley se entenderá por:

...

II. **Datos personales:** La **información** concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;

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;

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;

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

**Artículo 4.** Son objetivos de esta Ley:

...

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

### **CAPÍTULO III INFORMACIÓN RESERVADA Y CONFIDENCIAL**

**Artículo 13.** Como **información** reservada podrá clasificarse aquella 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 18.** Como **información** confidencial se considerará:

I. La entrega 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.

#### **CAPÍTULO IV 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.

Esta legislación proporciona otros conceptos sobre la información, así como una legislación para poder acceder a ella y el señalamiento de cual está reservada.

Dentro de la Administración Pública Federal ha cobrado gran importancia el manejo y control de la información gubernamental a tal grado de considerar como información administrativa cuando un servidor público violente su reglamentación encontrándose como falta a *contraio sensu* las disposiciones que a continuación se señalan:

#### **TÍTULO CUARTO RESPONSABILIDADES Y SANCIONES CAPÍTULO ÚNICO**

**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.

Aunque es un intento de acomodar las ideas de transparencia en los movimientos del gobierno ésta ley no otorga una verdadera protección a la información como lo harían otras legislaciones, pero contempla diversos conceptos para los “Delitos Informáticos” como el caso del concepto de “Información”, no obstante estar dirigida a los propósitos de la misma ley gubernamental.

Enfocado en la hipótesis delictiva principal contemplada en los artículos 211bis 1 al 211bis 7 del Código Penal Federal en donde: “Al que sin autorización modifique, destruya o provoque pérdida de **información** contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad” y “Al que sin autorización conozca o copie **información** contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad” en relación con esta Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental la “**información**” a proteger será la contemplada en los Artículos 3 fracción II, III, V, y VI, 13, 14 y 18; en especial a la “información contenida en sistemas o equipos de informática del Estado e Instituciones que integran el sistema financiero” debido a la naturaleza de la misma “**información**”

que protege esta ley debido a que tiene que ser resguardada por las mismas instituciones tanto del Estado como particulares y financieras. Ambas legislaciones pueden aplicarse conjuntamente a un servidor público ante una conducta antisocial de tal naturaleza, toda vez que en el Código Penal Federal se prevén figuras delictivas y en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental contempla infracciones administrativas.

## **2.5. Código Penal Federal.**

Como he venido señalando los Delitos Informáticos materia de la presente investigaron se encuentran previstos en el Código Penal Federal, en los artículos 211 bis1 al 211 bis 7 que se transcriben a continuación y que servirán de base para realizar un análisis dogmático jurídico penal en el Capítulo siguiente.

### **TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA** **CAPÍTULO II. ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**

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

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

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

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

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

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

**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.

Los delitos en contra de los derechos de autor están previstos en los artículos del 424 al 429 del Código Penal Federal que a continuación se transcriben y que tienen por objeto la protección de determinadas obras como los programas de computación como lo precisa el artículo 102, de la Ley Federal de Derecho de Autor:

**LIBRO SEGUNDO**  
**TÍTULO VIGÉSIMO SEXTO.**  
**DE LOS DELITOS EN MATERIA DE DERECHOS DE AUTOR**

**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.

IV. Derogada.

**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. (DR)IJ

**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 por querrela de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio. En el caso de que los derechos de autor hayan entrado al dominio público, la querrela la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

Cabe recordar que en el ámbito federal el Delito Informático persigue la protección de la información contenida en un sistema de cómputo, considerándose que existiría contravención con la Ley Federal del Derecho de Autor, sobre todo cuando en el primer ordenamiento menciona el que sin autorización “conozca o copie la información”, y en el segundo cuando menciona “a quien use en forma dolosa”.

Los anteriores programas de computación protegidos por la Ley del Derecho de Autor y cuyo uso sin autorización es un delito conforme al artículo 424 fracción III, del Código Penal Federal, pudieran estar en contradicción en el artículo 217 del Código Penal para el Estado de Sinaloa que se transcribirá en el apartado siguiente.

Qué sucedería cuando una persona cometa un delito informático previsto en el citado artículo 217 del Código Penal para el Estado de Sinaloa al que “dolosamente y sin derecho use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero o bienes o

información”; o bien “dolosamente y sin derecho 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”, y siendo que estos programas se encuentran protegidos por los artículos 101 y 102 de la Ley Federal del Derecho de Autor y que a su vez nos remite a la hipótesis del Código Penal Federal en su artículo 424, fracción III, ya que también se contempla concretamente “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” (entre ellos están los programas de computadora).

Pudiéramos considerar que la misma hipótesis se encuentra en el delito informático del Código Penal para el Estado de Sinaloa (artículo 217) y la violación del derecho de autor previsto en el Artículo 421 fracción III, sólo restaría analizar si posible invasión de competencia.

Inclusive habría que considerar al artículo 426 del Código Penal Federal, cuando hace referencia a diversas conductas que pudieran atentar por vía satelital al portar un programa.

## **2.6. Código Penal para el Estado de Sinaloa**

El estado de Sinaloa ha sido uno de los primeros Estados que ha contemplado los llamados Delitos Informáticos en su Artículo 217 del cual ya he hecho mención perteneciendo al título de los delitos en contra del patrimonio y cuyo texto dice:

**LIBRO SEGUNDO**  
**PARTE ESPECIAL**  
**SECCIÓN PRIMERA DELITOS CONTRA EL INDIVIDUO**  
**TÍTULO DÉCIMO DELITOS CONTRA EL PATRIMONIO**  
**CAPÍTULO V DELITO INFORMÁTICO**

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

I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

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

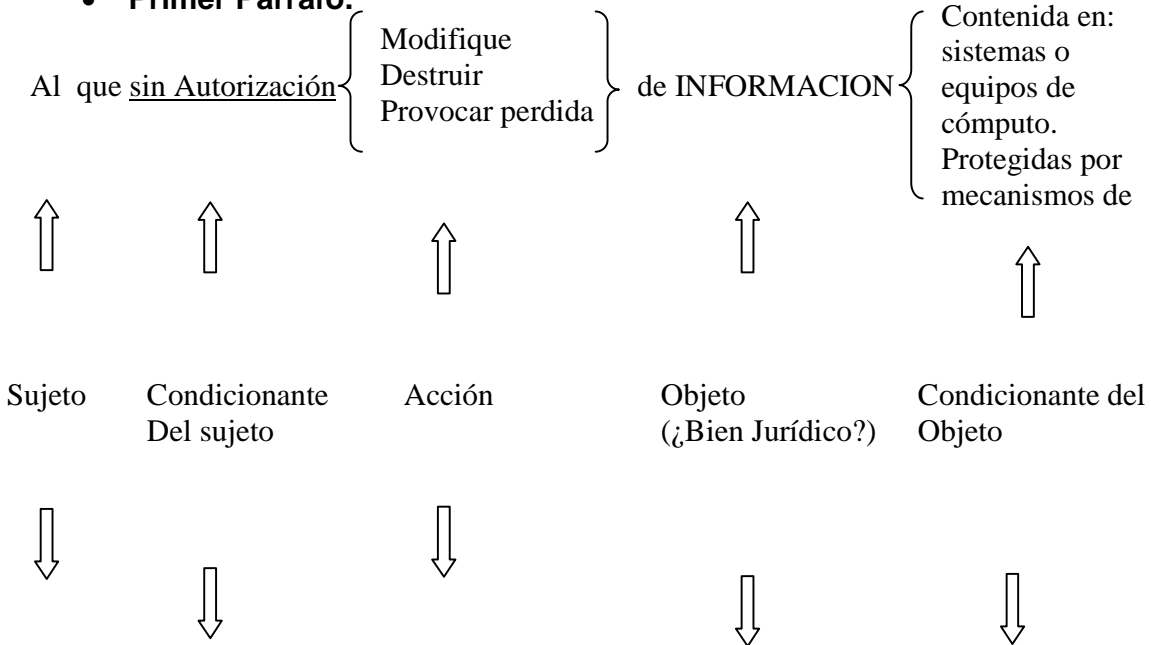
Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

En el presente trabajo independiente de los comentarios que se han realizado sobre este precepto, se realizará un análisis dogmático jurídico penal conjuntamente con el previsto por el Código Penal Federal en el Capítulo siguiente.

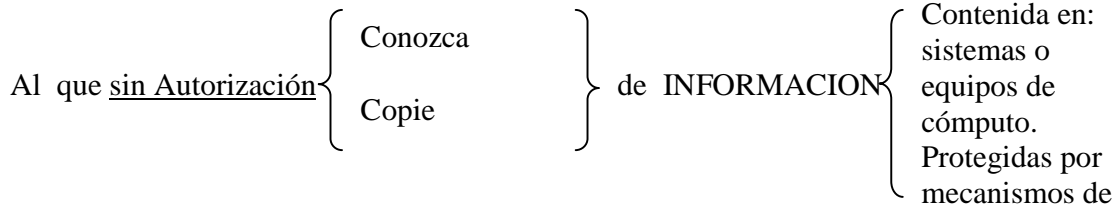
Para efecto de una mejor explicación de la problemática de los Delitos Informáticos previstos en lo artículos 211 bis1 del Código Penal Federal, 217 del Código Penal para el Estado de Sinaloa, y los ilícitos contemplados en los artículos 424 y 424 del citado ordenamiento federal que prevé a los delitos en contra del Derecho de Autor, así como un señalamiento que contempla la Ley Federal del Derecho de Autor de las obras protegidas para esta última legislación, se formulará un cuadro sinóptico de manera comparativa que también servirá para el estudio dogmático que se realizará en el siguiente Capítulo:

**Artículo 211 bis 1, del Código Penal Federal (Elementos del Tipo Penal)**

• **Primer Párrafo.**



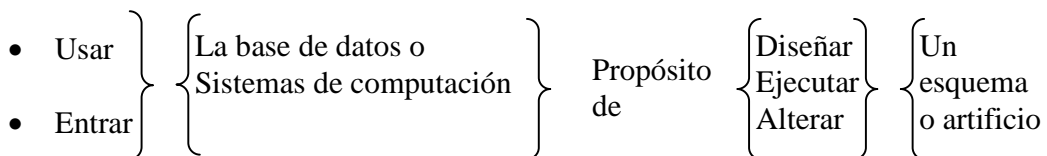
• **Segundo Párrafo.**



**Artículo 217 del Código Penal para el Estado de Sinaloa.**

La persona que dolosamente y sin derecho

**Fracción I.**



**Fin de DEFRAUDAR o de OBTENER UN LUCRO.**

**Fracción II.**

- Inaceptar.
  - Interferir.
  - Recibir.
  - Usar.
  - Alterar.
  - Dañar.
  - Destruir.
- Soporte lógico o
  - Programas de Computadora o
  - Datos contenidos en la base de base sistema o red (**Información**)

Código Penal Federal (delitos contra los derechos de autor artículos 424 y 424 bis.

**Artículo 424.**

I.-

II.-

III.-

Usa ⇒

Dolosamente

- Con Fines de lucro
- Sin autorización

Obras protegidas por la Ley Federal contra el Derecho de Autor

No relaciona, por lo tanto son todas las obras y aquí incluyen los programas de cómputo (Art. 102 LFDA)

**Artículo 424 bis.-**

- I. Producir,  
Reproducir,  
Introducir al País  
Almacenar.  
Transportar.  
Distribuir.  
Vender.  
Arrendar.

- Copias de obras
- Fonogramas.
- Videogramas
- Libros

Protegidos por la Ley Federal del Derecho de Autor

⇒ Dolo

**No menciona sistemas de Cómputo, pero pueden ser parte de uno y ser parte de la Información**

Fin de Especulación comercial sin autorización

Ante la problemática antes expuesta podemos resumir diversas posturas que confirman o niegan la existencia de los Delitos Informáticos tanto en el ámbito federal como del fuero común como es el caso del Estado de Sinaloa conforme a los siguientes puntos:

I.- Por lo que respecta al artículo 211 bis 1, del Código Penal Federal, al protegerse la información contenida en un sistema informático se puede considerar que el Delito Informático pudiera confundirse con los delitos de **robo, abuso de confianza y daño en propiedad ajena** en el bien consistente en la **información**.

II.- En cuanto a los Delitos Informáticos previstos en el artículo 217 del Código Penal para el Estado de Sinaloa, encontramos:

- 1) Por lo que respecta a la fracción I, se llega a negar la existencia de los Delitos Informáticos por considerarlos más bien como **delitos de fraude, abuso de confianza o robo** cometidos a través de sistemas computacionales.
- 2) En cuanto a la fracción II, pudiera negársele el contenido de un Delito Informático ya que ante las hipótesis previstas en tal precepto estaríamos en presencia de delitos tales como: el robo o daño en propiedad ajena al bien de la información o de un programa de cómputo, o bien, ante el delito en contra del derecho de autor previsto en el artículo 424, fracción III, del Código Penal Federal, cuando se use dolosamente con fines de lucro y sin autorización obras protegidas por la Ley

Federal del Derecho de Autor, en donde están incluidos los sistemas de cómputo (artículos 101 y 102).

Desde este momento cabe señalar que en los delitos patrimoniales se ha dado una gran variedad de especies de ilícitos atendiendo a su formulación, como se detalla a continuación:

- a) El delito de fraude encontramos la obtención de un lucro a través de que el sujeto activo realice un engaño al pasivo o aprovechándose del error en que éste se pueda encontrar para obtener ese lucro. Existen diversos tipos de fraude como el genérico que contiene los requisitos generales del engaño y del aprovechamiento del error, dando origen a diversos tipos de fraudes específicos tanto en el Código Penal Federal como en legislaciones especiales que atienden a múltiples modalidades de engaño y aprovechamiento del error, tal es el caso del delito de defraudación fiscal, previsto en el Código Fiscal de la Federación, el delito bancario (fraude a los bancos) contemplado en la Ley de Instituciones de Crédito, entre otros.
- b) En el delito de robo el sujeto activo acude por el objeto material obteniendo un lucro a través de medios como puede ser la violencia, se dan también diversas modalidades del delito de robo que inclusive atenúan o agravan la pena atendiendo precisamente a los medios, tal es el caso de robo en casa habitación, el robo del famélico (que aún contempla algunas legislaciones), como la de robo en despoblado, etc.

Los delitos en contra de los Derechos de Autor se han considerado como una especie del delito de robo de obras protegidas por la ley de la materia.

- c) En el delito de abuso de confianza también se obtiene un lucro indebido por el sujeto activo cuando el objeto material llega a él por la confianza que tiene el pasivo, y el primero se aprovecha quedándose con el bien.
- d) En el delito de daño en propiedad ajena que puede variar atendiendo a los medios comisivos o a determinar circunstancias, tales como: por inundación, por incendio, otro.

Con lo anterior se puede mencionar que los medios comisivos y circunstancias especiales en algunos delitos pueden dar lugar a la creación de otros nuevos que como lo veré en su respectivo apartado de la clasificación del tipo penal, referente a su metodología.

Bajo esa tesitura, los Delitos Informáticos pueden entrar bajo esos conceptos dados anteriormente y aceptar su existencia como otra especie de los delitos patrimoniales.

Como se puede apreciar, el Código Penal Federal no contempló como figura delictiva la comisión de un fraude o la obtención de un lucro a través de los medios informáticos, tal como lo hizo el artículo 217, fracción I, del Código Penal para el Estado de Sinaloa, ya que esta figura penal se encuentra prevista con el tipo de fraude genérico señalada en el artículo 386 que indica:

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

...

I.- ...

II.- ...

III.- ...

Al respecto, cabe precisar que la postura del Código Penal Federal dentro del fraude genérico es contemplar la obtención ilícita de una cosa o de un lucro por cualquier medio y en el caso de los llamados Delitos Informáticos ese medio cibernético entraría dentro de ese cualquier medio, ya que su configuración de un tipo abierto no limita esos medios comisivos; independientemente de la existencia de los fraudes específicos, sin embargo, la legislación Sinaloense en lugar de crear un delito de fraude específico (con el medio comisivo de un sistema informático) consideró crear un delito informático en el artículo 217, fracción I.

En cuanto a esos fraudes específicos previstos en el Código Penal Federal y en leyes especiales no hay que olvidar la postura de algunos tratadistas de que en caso de que fuesen derogados, aún así estarían previstos dentro del fraude genérico ya que manejan los mismos elementos de la obtención de un lucro o cosa a través del engaño o del aprovechamiento del error.

Ahora bien, también es conveniente precisar que los que están a favor de la existencia de los delitos informáticos en esta clase de fraudes, sostienen su postura ya que mencionan que el ilícito de fraude al obtenerse una cosa o un lucro a través del engaño o el aprovechamiento del error radica en que el sujeto pasivo (como aquél en el que recae el daño) es un humano, mientras que si se contemplan esas conductas

obteniéndose los mismos resultados y el engaño o el aprovechamiento del error se infiere también a través de un sistema de cómputo, independientemente de que continúe siempre siendo el sujeto pasivo un humano, estaríamos en presencia de un Delito Informático.

## **2.7. Otras Legislaciones en México.**

En los siguientes incisos se enlistarán las legislaciones en la República Mexicana que contemplan de alguna forma a los delitos realizados a través de medios informáticos de los cuales el legislador ha considerado señalarlos de manera específica, así como a los propiamente conocidos como “Delitos Informáticos” en los que el bien jurídico es la información contenida en medios informáticos, o bien cuando se atenta contra estos últimos.

### **2.7.1. Delitos llevados a cabo mediante medios informáticos.**

En la actualidad algunas legislaciones estatales han adoptado la idea de los Delitos Informáticos como delitos específicos como lo es el Código Penal para el Estado de Sinaloa, sin embargo, en otras legislaciones resaltan algunos delitos existentes contemplados en sus propios ordenamientos jurídicos atendiendo a que sean cometidos por medios electrónicos como lo pueden ser el fraude, secuestro, corrupción de menores e incapaces, pornografía infantil, prostitución de menores e incapaces, contra la moral, entre otros; sin embargo, el hecho de que en otras legislaciones no los han plasmado en sus respectivos códigos no quiere decir que los mismos no puedan cometerse por

diversos medios como lo sería utilizando una computadora, por lo que en el siguiente grupo de legislaciones que se señalarán se prevén ilícitos que no obstante que se les ha considerado como “Delitos Informáticos”, más bien serían delitos cometidos por medios informáticos dentro de los cuales haré mención a algunos de ellos atendiendo a los bienes jurídicos protegidos.

- Delitos patrimoniales.
- Delitos en contra la moral pública.
- Delitos ambientales.
- Contra las vías de comunicación
- Secuestro.
- Revelación de secretos.

- **DELITOS PATRIMONIALES.**

➤ **Legislación Penal para el Estado de Aguascalientes**

**LIBRO PRIMERO DE LAS FIGURAS TÍPICAS  
TÍTULO PRIMERO DE LAS FIGURAS TÍPICAS DOLOSAS  
CAPÍTULO QUINTO TIPOS PENALES PROTECTORES DEL PATRIMONIO**

**Artículo 44.** El robo consiste en:

...

III. El aprovechamiento de energía eléctrica, agua, gas, servicio telefónico, **servicio de Internet** o de imagen televisiva, sin consentimiento de la persona que legalmente pueda disponer de ellos;

**Artículo 45.** El robo será calificado cuando:

...

XI. Se lleve a cabo el apoderamiento mediante el uso de sistemas de informática, sistema de redes de computadoras, base de datos, soporte lógico o programas de cómputo.

En este artículo el legislador contempla al robo de servicio de Internet, aunque, muchos considerarían que dicho servicio podría encuadrarse perfectamente en la transmisión telefónica, no obstante se tiene que recordar que por su especial naturaleza la Internet es un gran medio de transmisión de multimedios que pueden abarcar tanto comunicaciones telefónicas, video, música, etc. que puede ser enviado junto con la señal telefónica, transmisión de radio y vía satelital, con lo que se abarca cualquier medio en el que se puede transmitir para su acceso a Internet.

➤ **Código Penal del Estado de Colima**

**LIBRO SEGUNDO  
TÍTULO SÉPTIMO DELITOS CONTRA EL PATRIMONIO  
CAPÍTULO III FRAUDE**

**Artículo 234.** Se considera fraude y se impondrá pena de uno a nueve años de prisión y multa hasta por 100 unidades, para el caso de las fracciones I y II, y de tres a nueve años de prisión y multa hasta por la misma cantidad en el caso de las fracciones III, IV, V y VI, en los siguientes casos:

V.- **Acceso indebido a los equipos y sistemas de cómputo o electromagnéticos.** 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 cómputo o electromagnéticos de las instituciones emisoras de los mismos, y

VI.- **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.** 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 este facultada para emitir los mismos

Al igual que en otras legislaciones en Colima el legislador contempla como el acceso a bases de datos tanto en medios magnéticos como en digitales, así como el fraude especial, pero se tiene que recordar que para que se presente un fraude debería existir que mediante engaño o error se caiga en una situación de la que el otros puedan tomar ventaja, pero para un sistema informático no posee voluntad, capacidad racional ni de discernir entre usuarios para que pueda ser engañados, siempre que se ingrese a un sistema informático con otra información de otra persona dichos sistemas nos reconocerán como autorizado o no, a pesar de que no sea su verdadero usuario.

➤ Código Penal del Estado libre y soberano de Chiapas

**LIBRO SEGUNDO  
TÍTULO SÉPTIMO DELITOS EN CONTRA DE LAS PERSONAS EN SU PATRIMONIO  
CAPÍTULO V. FRAUDE**

**Artículo 200.-** Se aplicaran las mismas sanciones previstas en el artículo anterior:

XXVII.- Al que para obtener algún beneficio para si 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.

Una vez mas podemos ver que el legislador convierte al acceso y alteración de datos para el propio beneficio o el de otros como fraude especial, pero aún recordando que las computadoras no poseen capacidad para ser engañadas, siempre reconocen a quien introduzca la información como autorizado o no, ni tampoco como autentica, tenemos que recordar quien puede ser engañado somos los seres humanos para constituir como fraude.

➤ Código Penal del Estado de México.

**TÍTULO PRIMERO DELITOS CONTRA EL ESTADO  
SUBTÍTULO CUARTO DELITOS CONTRA LA FE PÚBLICA  
CAPÍTULO IV FALSIFICACIÓN Y UTILIZACION INDEBIDA DE TÍTULOS AL PORTADOR,  
DOCUMENTOS DE CRÉDITO PÚBLICO Y DOCUMENTOS RELATIVOS AL CRÉDITO**

**Artículo 174.-** Se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que:

**IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios; y**

**V. Acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.**

Apropiadamente el legislador en el Estado de México con este artículo desea proteger la veracidad en la información necesaria para realizar operaciones económicas.

➤ Código Penal del Estado de Durango

**LIBRO PRIMERO DISPOSICIONES GENERALES  
TÍTULO CUARTO DELITOS CONTRA EL PATRIMONIO  
CAPÍTULO PRIMERO**

**Artículo 418.** Se equipara al robo y se castigara como tal:

**IV. El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.**

**LIBRO PRIMERO DISPOSICIONES GENERALES  
TÍTULO CUARTO DELITOS CONTRA EL PATRIMONIO  
CAPÍTULO CUARTO FRAUDE Y EXACCIÓN FRAUDULENTA**

**Artículo 426.** Igualmente comete el delito de fraude:

**XXIII. Quien para obtener algún lucro para si 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 en perjuicio de persona alguna, independientemente de que los recursos no salgan de la institución;**

Acertadamente en este precepto se prevé la hipótesis de proteger cualquier tipo de información contemplada en computadoras, aunque de manera muy vaga.

➤ **Código Penal para el Distrito Federal**

**TÍTULO DÉCIMO QUINTO DELITOS CONTRA EL PATRIMONIO  
CAPÍTULO III FRAUDE**

**Artículo 231.** Se impondrán las penas previstas en el artículo anterior, a quien:

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

**CAPÍTULO IV EXPLOTACIÓN LABORAL DE MENORES O PERSONAS CON  
DISCAPACIDAD FÍSICA O MENTAL  
TÍTULO VIGÉSIMO CUARTO DELITOS CONTRA LA FE PÚBLICA  
CAPÍTULO I PRODUCCIÓN, IMPRESIÓN, ENAJENACIÓN, DISTRIBUCIÓN, ALTERACIÓN  
O FALSIFICACIÓN DE TÍTULOS AL PORTADOR, DOCUMENTOS DE CRÉDITO  
PÚBLICOS O VALES DE CANJE.**

**Artículo 336.** Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien este facultado para ello:

IV. **Altere los medios de identificación electrónica** de tarjetas, títulos o documentos para el pago de bienes y servicios;

V. **Acceda a los equipos electromagnéticos** de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo;

VI. **Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas**, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma; o

Una vez más este Delito Informático es contemplado como fraude, se cataloga como delito especial del fraude radicando esencialmente en el engaño que se presenta ante las personas, ya que recordando una computadora no tiene capacidad para discernir entre lo correcto y lo incorrecto, ya que todo lo programado, alterado, o accesado será

reconocido como verdadero, e incluso el propio artículo 336 de éste mismo Ordenamiento sustantivo, plantea la hipótesis delictiva con la finalidad de proteger la validez en la que se presentan la información referencial a los documentos de crédito y tarjetas de créditos.

➤ **Código Penal del Estado de Guerrero.**

**LIBRO SEGUNDO PARTE ESPECIAL  
TÍTULO X DELITOS EN CONTRA DE LAS PERSONAS EN SU PATRIMONIO  
CAPÍTULO I. ROBO**

Artículo 165. Se impondrán las mismas penas previstas en el artículo 163 a quien:

I. Se apodere de una cosa propia, si esta se halla por cualquier TÍTULO legítimo en poder de otro, y

II. Aprovechando energía eléctrica, algún fluido, **programas computarizados**, señales televisivas o de **Internet**, sin consentimiento de la persona que legalmente pueda disponer de aquellas.

Acertadamente una vez más podemos encontrar al Delito Informático como robo de información e incluso de señal de Internet se encuentra bajo el rubro de robo, protegiendo programas de cómputo, que al final seguirá siendo información, contraponiéndose con la protección a los derechos de autor como se ha visto.

➤ **Código Penal para el Estado de Nuevo León.**

**LIBRO SEGUNDO  
PARTE ESPECIAL  
TÍTULO DÉCIMO NOVENO DELITOS EN RELACIÓN CON EL PATRIMONIO  
CAPÍTULO I. ROBO**

**Artículo 365.-** Se equipara al robo, y se castigara como tal:

IV.- El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Podemos encontrar que la sustracción de información e incluso su uso indebido constituye delito de robo, aunque presenta confusión entre documentos y datos de computadora, siendo que cualquier documento en una computadora está constituida por datos pero no todos los datos necesariamente no son documentos propiamente dichos, recuerde una fotografía digital video o música en su computadora personal.

- Código Penal del Estado de Quintana Roo.

## LIBRO SEGUNDO

### SECCIÓN TERCERA DELITOS CONTRA LA SOCIEDAD

#### TÍTULO TERCERO DELITOS CONTRA LA FE PUBLICA

##### CAPÍTULO II FALSIFICACION DE DOCUMENTOS Y USO DE DOCUMENTOS FALSOS

**Artículo 189 bis.** Se impondrá hasta una mitad más de las penas previstas en el artículo anterior, al que:

III. **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.

IV. **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 o servicios o para disposición de efectivo.

En este precepto podemos encontrar que la alteración de identificaciones electrónicas documentos de pago o a disposición de efectivo, así como el uso o acceso de información de instituciones dedicadas a transacciones económicas, dejando en total desprotección a las demás persona quienes posean datos de importancia en sus casas.

- Código Penal para el estado de Tamaulipas.

## TÍTULO DÉCIMO NOVENO DELITOS CONTRA EL PATRIMONIO DE LAS PERSONAS

**Artículo 400.** Se sancionara con la pena del robo:

IV. **El apoderamiento material 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.

También aparece aquí la sustracción de la información contenida como documentos dentro de un sistema informático, contemplado como un delito patrimonial.

- **DELITOS EN CONTRA DE LA MORAL PÚBLICA.**

- **Código Penal del Estado de Colima**

**LIBRO PRIMERO  
TÍTULO SEGUNDO DELITO Y DELINCUENTE  
CAPÍTULO I CONDUCTA O HECHO**

**Artículo 10.** Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los siguientes delitos previstos por este código: ... prevista por el artículo 157 bis, segundo párrafo, tratándose de la realización de acto de exhibicionismo corporal lascivo o sexual, con el objeto de video grabarlo, fotografiarlo o exhibirlo mediante anuncio impreso o electrónico...

**LIBRO SEGUNDO  
TÍTULO QUINTO DELITOS CONTRA LA MORAL PÚBLICA  
CAPÍTULO II CORRUPCION DE MENORES**

**Artículo 157-bis.** Al que explote a un menor o a quien no tenga capacidad para comprender el significado del hecho, con fines de lucro o para conseguir una satisfacción de cualquier naturaleza, se le impondrá de dos años seis meses a ocho años de prisión y multa hasta por quinientas unidades.

Para los efectos de este artículo, se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir, u obligar al sujeto pasivo, a la práctica de la mendicidad, o a realizar acto de exhibicionismo corporal libidinoso o de naturaleza sexual, con el objeto de video grabarlo, o fotografiarlo, o exhibirlo mediante cualquier tipo de impreso o medio electrónico.

- **Código Penal para el Estado de Morelos.**

**LIBRO SEGUNDO  
PARTE ESPECIAL DELITOS CONTRA EL INDIVIDUO  
TÍTULO DÉCIMO SEGUNDO DELITOS CONTRA LA MORAL PÚBLICA**

## **CAPÍTULO I ULTRAJES A LA MORAL PÚBLICA**

**Artículo 213.** Se aplicara prisión de seis meses a tres años y de trescientos a quinientos días-multa:

II. Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por otro;

## **CAPÍTULO III CORRUPCIÓN DE MENORES E INCAPACES**

**Artículo 213 Quater.** Al que induzca, procure u obligue a un menor de edad o a quien no tenga la capacidad para comprender el significado del hecho, a realizar actos de exhibicionismo corporal, lascivos o sexuales, de prostitución, de consumo de narcóticos, a tener practicas sexuales, a la practica de la ebriedad o a cometer hechos delictuosos, se le aplicara de cinco a diez años de prisión y de cien a quinientos días-multa. Se duplicara la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

Si además del delito citado resultase cometido otro, se aplicaran las reglas de acumulación.

Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de video grabarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet, se le impondrá de seis a quince años de prisión y de cien a quinientos días-multa...

### ➤ **Código Penal para el Estado de Tamaulipas.**

#### **LIBRO SEGUNDO PARTE ESPECIAL TÍTULO QUINTO DELITOS CONTRA LA MORAL PÚBLICA CAPÍTULO II CORRUPCION DE MENORES E INCAPACES, PORNOGRAFÍA INFANTIL Y PROSTITUCIÓN SEXUAL DE MENORES E INCAPACES**

**Artículo 194-bis.** Comete el delito de pornografía infantil:

I. El que obligue o induzca a uno o mas menores de dieciséis años a realizar actos de exhibicionismo corporal, lascivos, sexuales o pornográficos con la finalidad de video gravarlos, firmarlos, fotografiarlos o exhibirlos mediante anuncios impresos, electromagnéticos, electrónicos, o por vía Internet, de telefonía o cualquiera otra similar;

II. Toda persona que procure, permita o facilite por cualquier medio el que uno o más menores de dieciséis años con su consentimiento o sin el, realice cualquiera de los actos señalados en la fracción anterior con los mismos fines;

III. Al que fije, grave, procese, elabore o imprima actos de exhibicionismo corporal, lascivos, sexuales o pornográficos en que participen uno o mas menores de dieciséis años;

### • **Código Penal para el Estado de Yucatán.**

**LIBRO SEGUNDO DE LOS DELITOS EN PARTICULAR  
TÍTULO SÉPTIMO DELITOS CONTRA LA MORAL PÚBLICA  
CAPÍTULO II CORRUPCION DE MENORES E INCAPACES, TRATA DE MENORES Y  
PORNOGRAFÍA INFANTIL**

**Artículo 211.** Al que procure o facilite por cualquier medio que uno o más menores de dieciséis años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de video grabarlos, 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 cuatrocientos a quinientos días multa.

- **Código Penal para el Estado de Zacatecas**

**LIBRO SEGUNDO. DE LOS DELITOS EN PARTICULAR.  
TÍTULO SEXTO. DELITOS CONTRA LA MORAL PÚBLICA.  
CAPÍTULO II. CORRUPCION DE MENORES.**

**Artículo 183 bis.** También cometen el delito de corrupción de menores y se harán acreedores a las sanciones previstas:

II. Quienes propicien o permitan que menores de dieciocho años presencien, por medio de aparatos electrónicos, la exhibición de las cintas de video a que se refiere la fracción anterior

Como podemos contemplar con las legislaciones antes señaladas en donde se considera el bien jurídico a proteger en términos generales a la moral pública, relativa a la pornografía infantil, al exhibicionismo corporal lascivo o sexual, la explotación y corrupción de menores, ultraje, y otros actos más considerados como inmorales, y que la delincuencia ha encontrado a los sistemas informáticos como medios para realizar esas conductas antisociales, por lo que se pretende dar regulación no a los propios delitos informáticos, sino contra la moral que se asisten de medios informáticos.

- **DELITOS AMBIENTALES.**

➤ **Código Penal del Estado de Colima**

**LIBRO SEGUNDO  
TÍTULO ÚNICO  
CAPÍTULO ÚNICO DELITOS AMBIENTALES**

**Artículo 244.** Se impondrá de tres meses a seis años de prisión y multa de 100 a 15 mil unidades, a quien ilícitamente:

III.- Altere equipo o programas de cómputo utilizados para la verificación de automotores;

- **Código Penal para el Distrito Federal.**

**CAPÍTULO IV EXPLOTACIÓN LABORAL DE MENORES O PERSONAS CON  
DISCAPACIDAD FÍSICA O MENTAL  
TÍTULO VIGÉSIMO QUINTO DELITOS CONTRA EL AMBIENTE Y LA GESTIÓN  
AMBIENTAL  
CAPÍTULO I DELITOS CONTRA EL AMBIENTE**

**Artículo 346.** Se le impondrán de 2 a 6 años de prisión y de 1,000 a 5,000 días multa, a quien ilícitamente:

IV. Opere o altere en forma indebida equipos o programas de cómputo utilizados para la verificación vehicular.

Las legislaciones anteriores han señalado hipótesis delictivas no para contemplar a los delitos informáticos propiamente, sino principalmente se dirigen a proteger a la biódiversidad o medio ambiente a través del manejo de equipos o programas de cómputo.

- **CONTRA LAS VIAS DE COMUNICACIÓN.**

➤ **Código Penal del Estado de Tabasco.**

**LIBRO SEGUNDO PARTE ESPECIAL.  
TÍTULO DÉCIMOPRIMERO DELITOS CONTRA LA SEGURIDAD DE LA COMUNICACIÓN  
CAPÍTULO I INTERRUPCION O DIFICULTAMIENTO DEL SERVICIO PÚBLICO DE  
COMUNICACION**

**Artículo 309.** Al que por cualquier medio dañe, altere o interrumpa la comunicación telegráfica o telefónica, **o la producción o transmisión de energía, voces o imágenes**, que se presten como servicio publico local, se le aplicara prisión de seis meses a dos años

**LIBRO SEGUNDO PARTE ESPECIAL.  
TÍTULO DÉCIMOPRIMERO DELITOS CONTRA LA SEGURIDAD DE LA COMUNICACIÓN  
CAPÍTULO I INTERRUPCION O DIFICULTAMIENTO DEL SERVICIO PÚBLICO DE  
COMUNICACIÓN**

**Artículo 312.** Al que para la realización de actividades delictivas utilice instalaciones o **medios de comunicación** o de transporte públicos que sean de su propiedad o que tenga bajo su cuidado, se le aplicaran de dos a cuatro años de prisión.

**Artículo 316.** Al que intervenga la **comunicación privada de terceras personas**, a través de medios eléctricos o electrónicos, se le aplicara prisión de uno a cinco años.

El Estado de Tabasco ha considerado como una especie más en la comisión del delito de ataques contra las vías de comunicación el que utilice instalaciones o medios de comunicación para la realización de actividades delictivas, así como el que se intervenga la comunicación privada de terceras personas.

- **DELITO DE SECUESTRO**

➤ **Código Penal para el Estado Libre y Soberano de Jalisco**

**LIBRO SEGUNDO DE LOS DELITOS EN PARTICULAR  
TÍTULO DÉCIMO CUARTO DELITOS CONTRA LA PAZ, LIBERTAD Y SEGURIDAD DE  
LAS PERSONAS  
CAPÍTULO VII SECUESTRO**

**Artículo 194.** Comete el delito de secuestro quien prive ilegalmente de la libertad a otro con la finalidad de obtener rescate o de causar daño o perjuicio. Por rescate se entiende todo aquello que entrañe un provecho indebido y a cuya realización se condiciona la libertad del plagiado. al responsable de este delito se le impondrá una pena de dieciocho a treinta y cinco años de prisión y multa por el importe de mil a dos mil días de salario mínimo.

- I. Al responsable de secuestro se le sancionara con una pena de veinticinco a cuarenta años de prisión y multa por el importe de mil a tres mil días de salario mínimo, y en su caso destitución, e inhabilitación del servidor publico para desempeñar otro empleo, comisión o cargo publico, cuando:

k) **Para lograr sus propósitos, se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología**, que impliquen marcada ventaja en el logro de su fin;

El delito de secuestro que tanto afecta a la sociedad y en la que se han utilizado diversos mecanismos para ese fin delictivo es contemplado en la legislación de Jalisco como una agravante para aquellos que se valgan de redes o sistemas informáticos, por lo que aquí sólo se regula al secuestro a través de medios informáticos.

- **DELITO DE REVELACIÓN DE SECRETOS**
- **Código Penal para el Estado de Baja California.**

**LIBRO SEGUNDO PARTE ESPECIAL  
TÍTULO TERCERO DELITOS CONTRA LA INVOLABILIDAD DEL SECRETO  
CAPÍTULO ÚNICO REVELACION DEL SECRETO**

**Artículo 175.-** Tipo y punibilidad.- Al 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** o se le haya confiado, y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentara hasta una mitad mas. Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de prisión y hasta cien días multa.

Revelación del secreto: se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se genero, que sea transmitida a otra persona física o moral ajena a la fuente.

Querrela: el delito de revelación de secreto se perseguirá por querrela de la persona afectada o de su representante legal.

Considerado como delito de revelación de secretos aparece en la legislación de Baja California cuando se revele un secreto a través de medios informáticos, por lo que también puede considerarse como una agravante de esta clase de ilícitos cuando se asista de estos medios computacionales.

### **2.7.2. Delitos Informáticos en otras legislaciones.**

En los últimos años diversos estados de la República Mexicana se han preocupado por regular la protección de la “información” contenida en medios informáticos, objetivo principal de los “Delitos informáticos”, no obstante de que no le dan esa denominación salvo el Código Penal para el Estado de Libre y Soberano de Veracruz, creando para ello capítulos especiales en sus ordenamientos penales de los cuales nos percatamos que algunas de ellas son réplicas de otras, como las que a continuación se mencionan:

➤ **Código Penal para el Estado de Aguascalientes.**

**Artículo 23.-** Los delitos que se perseguirán por querrela o a petición de parte legítimamente ofendida, son los siguientes:

**XXVI.-** Acceso sin Autorización y Daño Informático, previstos en los artículos 223, 224, 225 y 226.

**TÍTULO VIGÉSIMO PRIMERO  
DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS Y MAGNÉTICOS  
CAPÍTULO PRIMERO ACCESO SIN AUTORIZACIÓN**

**Artículo 223.-** 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.

Al responsable de Acceso sin Autorización se le sancionará con penas de 1 a 5 años de prisión y de 100 a 400 días multa.

Cuando el Acceso sin Autorización tengan por objeto causar daño u obtener beneficio, se sancionará al responsable con penas de 2 a 7 años de prisión y de 150 a 500 días de multa.

También se aplicarán las sanciones a que se refiere el párrafo anterior cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos accedidos sin autorización o excediendo la que se tenga.

**TÍTULO VIGÉSIMO PRIMERO**  
**DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS Y MAGNÉTICOS**  
**CAPÍTULO SEGUNDO DAÑO INFORMÁTICO**

**Artículo 224.-** 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.

Al responsable de Daño Informático se le sancionará de 1 a 5 años de prisión y de 100 a 400 días de multa.

Se le aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos dañados.

**Artículo 225.-** Cuando el Acceso sin Autorización o el Daño Informático se cometan culposamente se sancionarán con penas de 1 mes a 3 años de prisión y de 50 a 250 días multa.

**Artículo 226.-** 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.

Al responsable del delito de Falsificación Informática se le aplicarán de 1 a 5 años de prisión y de 100 a 400 días multa.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma bienes informáticos falsificados con conocimiento de esta circunstancia.

Se aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos falsificados.

➤ **Código Penal para el Estado de Coahuila de Zaragoza.**

**LIBRO SEGUNDO PARTE ESPECIAL**  
**TÍTULO SEGUNDO DELITOS CONTRA LA SEGURIDAD PÚBLICA**  
**CAPÍTULO TERCERO DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS**  
**INFORMÁTICOS**

**Artículo 281 bis.** Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Se aplicara prisión de tres meses a tres años y multa a quien:

I. 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.

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 los contenidos.

Si la conducta que 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 cuatro meses a cuatro años de prisión y multa.

**Artículo 281 bis 1.** Circunstancias agravantes de los delitos anteriores. Las penas previstas en el artículo anterior, se incrementaran en una mitad más:

I. Si el agente actuó con fines de lucro.

II. 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.

**Artículo 281 bis 2.** Sanciones y figuras típica de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública. Se aplicara prisión de seis meses a seis años y multa a quien:

I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad publica de las mencionadas en el párrafo segundo del Artículo 194, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.

II. Con autorización para acceder al sistema informático de una entidad publica de las mencionadas en el párrafo segundo del Artículo 194, indebidamente copie, transmita, imprima, obtenga sustraiga, utilice divulgue o se apropie de datos o 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 publica, la sanción será de uno a ocho años de prisión y multa.

Si el sujeto activo del delito es servidor publico, se le sancionara, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.

**Artículo 281 bis 3.** Circunstancias agravantes en los delitos anteriores. Las penas previstas en el artículo anterior se incrementaran en una mitad mas:

I. Si el agente obro valiéndose de alguna de las circunstancias agravantes previstas en el artículo 290 bis 1.

II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades publicas que se mencionan en el artículo 194, o por funcionarios o empleados que estén a su servicio.

III. Si la conducta afecto un sistema o dato referente a la salud o seguridad publica o a la prestación de cualquier otro servicio publico.

**Artículo 281 bis 4.** Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos. A los fines del presente CAPÍTULO, se entiende por:

I. Sistema informático: 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.

II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

➤ **Código Penal del Estado libre y soberano de Chiapas**

**LIBRO SEGUNDO**  
**TÍTULO DÉCIMO QUINTO DELITOS DE REVELACION DE SECRETOS Y DE ACCESO**  
**ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**  
**CAPÍTULO II ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA**

**Artículo 284 Ter.-** Al que sin autorización modifique destruya, o provoque perdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o que no tenga derecho de acceso a el, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, indebidamente destruya, modifique, o provoque perdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentara en una mitad.

**Artículo 284 Quatre (sic).-** 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 sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días multa.

**Artículo 284 Quinter.-** Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia publica, protegida por algún sistema o mecanismo de seguridad se le impondrá pena de dos a cinco años de prisión y de cien a trescientos días multa.

**Artículo 284 Sexter.-** Al que, estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifiquen, destruya o provoque

perdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

**Artículo 284 Septer.-** 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 de uno a cuatro años de prisión y de cien a trescientos días multa.

**Artículo 284 Octer.-** Los delitos previstos en este TÍTULO serán sancionados por querrela de parte ofendida.

➤ **Código Penal para el Estado de Guanajuato.**

**LIBRO SEGUNDO PARTE ESPECIAL  
TÍTULO TERCERO DE LOS DELITOS CONTRA LAS VÍAS DE COMUNICACIÓN DE USO  
PÚBLICO Y VIOLACIÓN DE CORRESPONDENCIA  
CAPÍTULO II VIOLACIÓN DE CORRESPONDENCIA**

**Artículo 231.-** Se aplicará de diez días a dos años de prisión y de diez a cuarenta días multa, a quien indebidamente:

I.- Abra, intercepte o retenga una comunicación que no le este 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 querrela de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

➤ **Código Penal para el Estado libre y soberano de Jalisco**

**LIBRO SEGUNDO DE LOS DELITOS EN PARTICULAR  
TÍTULO NOVENO FALSEDAD  
CAPÍTULO VIII FALSIFICACIÓN DE MEDIOS ELECTRÓNICOS O MAGNÉTICOS**

**Artículo 170 bis.** Se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente en la época y área geográfica en que se cometa el delito, al que, sin consentimiento de quien este 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 de este Artículo, y los destine a alguno de los supuestos que contempla el presente Artículo; y

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 del artículo.

Las mismas penas se impondrán a quien utilice o revele indebidamente información confidencial o reservada de la persona física o jurídica que legalmente este facultada para emitir los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este Artículo, 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. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentaran en una mitad.

➤ **Código Penal para el Estado de Nuevo León.**

**LIBRO SEGUNDO  
PARTE ESPECIAL**

**TÍTULO VIGÉSIMO SEGUNDO DE LOS DELITOS POR MEDIOS ELECTRÓNICOS**

**Artículo 427.-** A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos, se le impondrá de 2 meses a 2 años de prisión y multa de 200 a 1000 cuotas.

**Artículo 428.-** 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 de 2 a 8 años de prisión y multa de 300 a 1500 cuotas.

**Artículo 429.-** A quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos, se les impondrá de 2 a 8 años de prisión y multa de 350 a 2000 cuotas.

➤ Código Penal para el Estado de Tamaulipas.

**LIBRO SEGUNDO PARTE ESPECIAL**  
**TÍTULO OCTAVO DELITOS COMETIDOS POR SERVIDORES PÚBLICOS**  
**CAPÍTULO II ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**

**Artículo 207 Bis.** 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 el, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.

**Artículo 207-Ter.** 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 se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

**Artículo 207-Quater.** Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario

**Artículo 207-Quinques.** 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 se impondrá una sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

**Artículo 207-Sexies.** 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 de uno a cuatro años de prisión y multa de cien a trescientos días salario.

Los delitos previstos en este TÍTULO serán sancionados por querrela de la parte ofendida.

**Artículo 208.** 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.

- **Código Penal para el Estado libre y soberano de Veracruz-Llave.**

**LIBRO SEGUNDO**  
**TÍTULO IV DELITOS CONTRA LA INTIMIDAD PERSONAL Y LA INVOLABILIDAD DEL**  
**SECRETO**  
**CAPÍTULO III 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.

## **CAPÍTULO 3. PROBLEMÁTICA JURÍDICA DE LOS DELITOS INFORMÁTICOS.**

### **3.1. Conceptos básicos sobre la Teoría del Delito aplicados a los ilícitos informáticos.**

En el presente Capítulo se analizarán a los delitos informáticos contemplados en el Código Penal Federal y en el Código Penal para el Estado de Sinaloa a través de la Dogmática Jurídico Penal en todos y cada uno de los elementos que integran a esas figuras ilícitas.

#### **3.1.1. La Dogmática Jurídico-Penal y la Teoría del Delito.**

La Ciencia del Derecho Penal como un conjunto de conocimientos sistematizados encaminados al objetivo de desentrañar la esencia del delito, de las penas y de las medidas de seguridad a través de la historia el fundamento de esas ideas penales y que inclusive algunos tratadistas la consideran como sinónimo con la Dogmática Jurídico-Penal,<sup>37</sup> que maneja esos conocimiento o principios enfocados al estudio del delito.

Uno de los mejores sistemas que se han dado para el análisis de un delito desde el punto de vista jurídico es la utilización de la Teoría del Delito que contempla precisamente su estudio a través de un sistema analítico de sus elementos que lo

---

<sup>37</sup> Torres López, Mario Alberto. **LAS LEYES PENALES**. Quinta edición. Editorial Porrúa. México 2005. Pág. I.

integran (no obstante haber posturas de quienes sostienen que el delito es un bloque monolítico bajo una concepción totalizadora o unitaria).

Así, el delito puede desintegrarse de una manera didáctica en sus elementos que lo conforman (positivos), o bien, desintegrarse por causas que corresponden a cada uno de tales elementos (negativos), sin que con ello neguemos el carácter unitario del mismo ilícito.

Por tal motivo, es que el análisis de los delitos informáticos materia de la presente investigación se desarrollará principalmente bajo los principios fundamentales de dicha Teoría del Delito, llevándose a cabo también la crítica necesaria al tratar a cada uno de tales elementos tanto en su aspecto jurídico, como social, económico y político.

### **3.1.2. El concepto del delito y la definición del Delito Informático.**

Sobre el delito han existido diversos conceptos, definiciones y clasificaciones, atendiendo a la tendencia del autor, ya sea clásica, positivista, causalista, finalista, neofinalista, basada en el *iusnaturalismo* o en el *iuspositivismo*, o bien en la legal de acuerdo al artículo 7 del Código Penal Federal, por lo que en este apartado haré mención de aquellas que considero importantes, estructurando una que pueda aplicarse al ámbito informático.

El concepto del delito ha sido tratado por connotados penalistas, adoptándose algunos de ellos por ordenamientos penales en toda la República Mexicana, encontrando los siguientes:

Etimológicamente la palabra delito deriva del latín “*delinquere*”, abandonar, descuidar, apartarse del buen camino, alejarse del sendero señalado por la ley. El Diccionario Jurídico Mexicano, del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México precisa al delito como la: “...acción u omisión ilícita bajo la amenaza de una pena o sanción criminal”.<sup>38</sup>

También puede ser definido como el acto típicamente antijurídico, culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal. A nuestro juicio, en suma, las características del delito serían éstas: actividad; adecuación típica; antijuricidad; imputabilidad; culpabilidad; penalidad y, en ciertos casos, condición objetiva de punibilidad.<sup>39</sup>

Otra definición del delito es la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso.<sup>40</sup>

Para el Doctor Rafael Garófalo, de la Escuela Positivista del Derecho Penal citado por Don Celestino Porte Petit en su obra “Apuntamientos de la Parte General de Derecho Penal” precisa al delito como: “la violación de los sentimientos altruistas fundamentales de benevolencia o piedad y probidad o justicia en la medida media en

---

<sup>38</sup> **DICCIONARIO JURÍDICO MEXICANO**. Editorial Porrúa. México 1985. Tomo III, Letra “D”, Op. Cit. Pág. 62.

<sup>39</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Decimaprimer edición. Editorial Sudamericana. Buenos Aires Argentina. Mayo 1980. Pág. 207.

<sup>40</sup> Castellanos Tena, Fernando. **LINEAMIENTOS ELEMENTALES DE DERECHO PENAL. (Parte General)**. Cuadragésima séptima edición actualizada por Horacio Sánchez Sodi, primera reimpresión. Editorial Porrúa. México 2007. Págs. 125 y 126.

que se encuentran en la sociedad civil, por medio de acciones nocivas para la colectividad”.<sup>41</sup>

El Dr. Fernando Castellanos Tena hace referencia a que en la definición del delito no se deben incluir como elementos esenciales a la imputabilidad, a la punibilidad y por ende a las condiciones objetivas de punibilidad.<sup>42</sup>

Así, el artículo 7 del Código Penal Federal precisa:

“**Artículo 7.-** Delito es el acto u omisión que sancionan las leyes penales”.<sup>43</sup>

De manera idéntica al ámbito federal, se define al delito en el Código Penal para el Distrito Federal también en su artículo 7.

En el Código Penal para el Estado de Sinaloa no aparece definición sobre el delito.

Así, el delito lo podemos conceptuar como una conducta antisocial que el legislador prevé en una ley de naturaleza penal y que se encuentra sancionada principalmente por la pena de prisión.

---

<sup>41</sup> Porte Petit Candaudap, Celestino. **APUNTAMIENTOS DE LA PARTE GENERAL DE DERECHO PENAL**. Decimoséptima edición. Editorial Porrúa. México 1998. Pág. 201.

<sup>42</sup> Castellanos Tena, Fernando; Op. Cit., Pág. 130.

<sup>43</sup> **CÓDIGO PENAL FEDERAL. AGENDA PENAL FEDERAL**. Décima novena edición, Ediciones Fiscales ISEF, S.A., México 2007, Pág. 4-7.

Desde el surgimiento de la problemática de las nuevas tecnologías, a pesar de ser un tema relativamente nuevo se encuentra en un rápido crecimiento, con lo que algunos autores han definido a los delitos informáticos de la siguiente manera:

Como actitudes contrarias a los intereses de las personas en que se tiene las computadoras como instrumento o fin o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin.<sup>44</sup>

Otra definición sería como cualquier delito relacionado con la informática: contra la propiedad intelectual, robo por medios computarizadas y redes de pornografía infantil<sup>45</sup> ésta puede abarcar propiedad intelectual robo por medio de computadoras y redes, pornografía infantil entre muchas otras.

Para el Lic. Gabriel Andrés Cámpoli en su libro “Derecho Penal Informático en México” realiza la diferencia entre delitos informáticos y delitos electrónicos definiendo a los primeros como: “aquellos realizados por el autor con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o imputabilidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones”,<sup>46</sup> y el Delito Electrónico como: “aquellos que surgen de las nuevas tecnologías aplicadas y tienen como objeto material del delito expresamente a las

---

<sup>44</sup> Téllez Valdés, Julio. Op. Cit. Pág. 163.

<sup>45</sup> Moreno Martín, Arturo. **DICCIONARIO DE INFORMATICO Y TELECOMUNICACIONES INGLES Y ESPAÑOL**. Editorial Ariel Barcelona 2001. Pág. 130.

<sup>46</sup> Cámpoli, Gabriel Andrés. **DERECHO PENAL INFORMATICO EN MÉXICO**. Editorial INACIPE, México 2004. Pág. 17.

mismas, por regla general no poseen definición de tipos posibles de ser aplicables por estar referidos a bienes y conceptos inexistentes a la sanción de las leyes penales”<sup>47</sup>. Al respecto, y como se ha mencionado con anterioridad la electrónica no es lo mismo que la informática debido a que todo aparato informático es electrónico pero no todo aparato electrónico es necesariamente informático, una licuadora contra su computadora, aún que hay que mencionar que con los avances en las tecnologías incluso un refrigerador cuenta con avanzadas computadoras con acceso a Internet e incluso un poco más inteligentes. Pero también hay que tomar en cuenta que no hay que seguir inventando figuras penales debido a que estos “Delitos Electrónicos” sólo usan el medio electrónico como medio para cometer delitos contra los mismos aparatos electrónicos (daño en propiedad ajena) o contra otros bienes que aunque no estén contempladas en preceptos legales siguen siendo los mismos, un ejemplo fácil para entender esto sería: no es lo mismo sacar el dinero de un cajero automático con una cierra eléctrica o incluso golpeándolo con una video casetera en la que se termina por destruir el cajero con el fin de sustraer el dinero (robo y daño en propiedad ajena), que usando una computadora o un virus informático con conocimiento en informática alterando la información del mismo cajero que al final éste permita entregar el dinero de manera pacífica (robo usando la informática), pero aunque las mencionadas herramientas en este ejemplo son aparatos electrónicos la computadora es un aparato que procesa información y su uso para cometer delitos requiere de personas con conocimientos especializados.

En la obra “Delitos Informáticos en la legislación Mexicana” del citado autor, define a los “Delitos Informáticos” como: “aquellos en los cuales el tipo penal protege la

---

<sup>47</sup> Idem.

integridad física o lógica de los equipos informáticos o páginas Web, es decir, aquellas acciones en las cuales los equipos informáticos o páginas Web resultan objeto del delito”,<sup>48</sup> y hace la diferencia con los “Delitos Telemáticos” como: “aquellos que sin afectar expresamente a un equipo informático en particular disminuyen o anulan su capacidad de transmisión o procesamiento de datos a distancia, ya sea actuando en forma indirecta sobre el equipo, sobre su capacidad de recepción o envío de datos sobre sus parámetros lógicos o sobre las vías de comunicación necesarias para la función normales del mismo a distancia.”<sup>49</sup> Atendiendo a esta definición en sí dentro de los delitos informáticos queda explícitamente contemplado la existencia de ataques a distancia con el uso de la Internet y el uso generalizado de las telecomunicaciones, por lo que dentro de los mismos “Delitos Informáticos” se encuentran los “Delitos Telemáticos” debido a que aunque acceder a una computadora de manera física o a distancia continúan siendo “Delitos Informáticos”.

La Organización para la Cooperación Económica y el Desarrollo define al delito informático (*Computer Crime*) como: “cualquier conducta ilegal, no ética, no autorizada que involucra el procesamiento automático de datos y/o la transferencia de datos.”<sup>50</sup>

Para poder definir a un “Delito Informático” hay que tomar en cuenta que no hay que definir una sola conducta como el caso de otros delitos convencionales que pueden ser generalizados, sino debido a la complejidad de las nuevas tecnologías y el mundial

---

<sup>48</sup> Ibidem. Pág. 66.

<sup>49</sup> Ibidem. Pág. 67.

<sup>50</sup> OECD, **COMPUTER RELATED CRIMINALITY: ANALYSIS OF LEGAL POLICY IN THE OECD AREA**. ICCP, 84:22, 1984. Pág. 40.

campo de acción para ser llevados hacen que definir el delito informático incluya diversas conductas en una sola definición.

Conforme a la definición legal del delito que precisa el Código Penal Federal en su artículo 7, puedo estructurar el siguiente concepto de un delito informático como: **“el acto u omisión que sancionan las leyes penales que protegen la información en un sistema informático o equipos de informática ya sea modificando la información o dañándolos, o bien obteniendo a través de ellos alguna cosa o lucro indebido”**,

Con lo anterior, también puedo conformar una definición del delito informático para quedar como sigue:

***“Al que sin autorización obtenga, conozca, altere o destruya información confidencial en un sistema informático”***

Con la anterior definición solamente se está considerando al Delito Informático como aquél en que se obtiene información a través de medios electrónicos y no de los diversos ilícitos que pueden cometerse a través de éstos medios, ya que se ha precisado son de variada naturaleza y que sólo utilizan para su comisión de un medio especial.

Con lo que se crea el problema de definir el complejo término de “Información” para el presente trabajo, el que se analizará en apartados posteriores.

Como marco de referencia en el Capítulo anterior fueron transcritos los artículos 217 del Código Penal para el Estado de Sinaloa, y 211 bis 1, del Código Penal Federal, que contemplan expresamente a los llamados “Delitos Informáticos” y sobre de los cuales versará un breve análisis dogmático.

Por lo que respecta a los artículos 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7 del Código Penal Federal se refieren a los Delitos Informáticos cometidos en contra del Estado y de las Instituciones Financieras, también fueron transcritos para tener un mejor marco jurídico de estos delitos.

### **3.2. Clasificación del delito informático.**

A continuación analizaré las diversas clasificaciones que se han tratado en el ámbito jurídico-penal sobre el delito en general aplicando estos conceptos al Delito Informático, así como la que se ha formulado en materia informática aplicada a estos ilícitos:

#### **3.2.1. Clasificación jurídico-penal del delito y su aplicación en el Delito Informático.**

En la doctrina Penal se han manejado diversas clasificaciones del delito, sin embargo la mayoría ha coincidido en diversos puntos, encontrando la descrita por autores como el *Dr. Eduardo López Betancourt*,<sup>51</sup> a la que para efecto de la presente

---

<sup>51</sup> López Betancourt, Eduardo. **TEORÍA DEL DELITO**. Décima cuarta edición. Editorial Porrúa, México 2007, Págs. 280 a 286.

obra he optado por darle seguimiento, en virtud de resultar con un fondo didáctico, además de resumir la mayor parte de la doctrina aplicable en nuestro país, aprovechando cada uno de esos puntos para dar una explicación al Delito Informático materia de esta investigación, exponiéndola de la siguiente manera:

***En función de su gravedad:***

***1.- Bipartita. Delitos y faltas;*** *son delitos los sancionados por la autoridad judicial y las faltas, son sancionadas por la autoridad administrativa.*

***2.- Tripartita. Delitos, faltas y crímenes;*** *esta clasificación no funciona en nuestro sistema penal. (sobre el cual se considera que sólo se utiliza en el argot periodístico al hacer referencia a los crímenes).*

La legislación mexicana acepta la clasificación entre delitos y faltas, atendiendo a la gravedad de las conductas antisociales, los crímenes como delitos de sangre para otro tipo de legislaciones extranjeras.

Los ilícitos informáticos pertenecen a la clasificación de los llamados delitos, ya que dentro de sus textos sinaloense y federal se desprende que en primer lugar se prevé una sanción privativa de la libertad, en donde para su conocimiento interviene el Ministerio Público como autoridad investigadora y persecutora, además de la autoridad judicial que es la encargada de realizar la etapa procesal y de aplicar las sanciones correspondientes.

Dentro de los delitos existen también diversos grados de gravedad que han originado otra subclasificación, atendiendo a que si el sujeto activo pueda obtener su libertad provisional o no, llamándoseles a los primeros “Delitos No Graves” y a los segundos “Delitos Graves”.

Para efectos de determinar si un delito es grave a nivel federal, los mismos se encuentran dentro del artículo 194 del Código Federal de Procedimientos Penales, precepto que no contempla a los delitos informáticos de los artículos 211 bis 1 al 211 bis 7, del Código Penal Federal, por lo tanto sus infractores pueden obtener su libertad provisional.

Posiblemente en fechas no muy lejanas los delitos informáticos contemplados en los artículos 211 bis 2 al 211 bis 5, sean incluidos en los delitos graves ya que su comisión por ser los sujetos pasivos el Estado o alguna entidad del servicio financiero sean considerados de gran relevancia para el Estado al grado que a sus transgresores no les permitan obtener esa libertad provisional; ampliándose así el artículo 194 del Código Penal Federal.

Los delitos informáticos del artículo 217 del Código Penal Federal para el Estado Sinaloa son definitivamente considerados como delitos por encontrarse en un ordenamiento de naturaleza penal.

**Según la conducta del agente:**

**1.- Acción.** Son aquellos en que se requiere el movimiento del sujeto para cometer el ilícito, por ejemplo, para jalar el gatillo de la pistola, para clavar un puñal, entre otros.

**2.- Omisión.** Son aquellos que requieren la inactividad del sujeto, es decir que deje de hacer lo que está obligado.

**a) Omisión simple.** La simple inactividad origina la comisión del delito independientemente del resultado; se viola una ley preceptiva.

**b) Comisión por omisión.** Necesariamente, como consecuencia debe haber un resultado, por ejemplo, el guardavías, no realiza el cambio de vías del tren, por tal razón chocan los trenes, entonces se castigará esa omisión, se viola una ley prohibitiva.

Atendiendo a esta clasificación los delitos informáticos del artículo 217 del Código Penal para el Estado de Sinaloa su forma de conducta de acuerdo a sus verbos rectores son de acción consistente en:

**Artículo 217.**

**Fracción I.-** Usar, entrar, diseñar, ejecutar, alterar o realizar un artificio.

**Fracción II.-** Interceptar, interferir, recibir, usar, alterar, dañar y destruir

Respecto a las hipótesis de “dañar” y “destruir”, cabe desde este momento resaltar la falta de técnica legislativa del tipo penal, ya que la segunda hipótesis (destruir) puede ser considerada como “dañar” siendo definido éste último conforme al artículo 2108 del Código Civil Federal como: “Se entiende por daño la pérdida o menoscabo sufrido en el patrimonio por la falta de cumplimiento de una obligación”.

Por lo que se refiere al Código Penal Federal la forma de conducta del delito informático es también de acción bajo los siguientes verbos:

Artículo 211 bis 1. (Párrafo primero).- Modificar, destruir o provocar pérdida.

(Párrafo segundo).- Conocer o copiar.

***Por el resultado:***

***1.- Formales.*** Aquellos que para configurarse no requieren de ningún resultado, esto es, de ninguna materialización, por ejemplo, el abandono de un niño. Sólo se transgrede a la ley.

***2.- Materiales.*** Requieren de un resultado, de un hecho cierto, por ejemplo, el homicidio. Se da un cambio en el mundo exterior.

En cuanto al resultado de los delitos informáticos se encontró la siguiente clasificación:

En el Código Penal para el Estado de Sinaloa en su artículo 217, encontré un **resultado material** como un cambio en el mundo exterior en su fracción I, ya que se requiere de la finalidad de defraudar, de obtener dinero o bienes o información.

También aquí cabe hacer notar otra falta de técnica legislativa cuando se refiere a defraudar, siendo un término genérico que abarca por su propia descripción a que en el fraude se obtiene por error o engaño indebidamente de alguna “cosa o lucro”; en donde se puede incluir lo referente al “dinero, bienes o información”.

El artículo 217, fracción II, del citado Código Sinaloense refleja un **resultado material** en las formas de conducta de interceptar, interferir, recibir y usar, alterar, dañar o destruir, conocer o copiar la información contenida en un sistema o equipo de información ya que las mismas reflejan la producción de un cambio en el mundo exterior.

En cuanto al artículo 211 bis 1, del Código Penal Federal, su clasificación en torno al resultado en su fracción I, es **material** ya que bajo las hipótesis de modificar, destruir o provocar pérdida de la información o de equipos de informática existe una mutación en el mundo exterior.

En conclusión, los delitos informáticos producen un resultado material.

***Por el daño que causan:***

***1.- De lesión.*** Causan una disminución del bien jurídico tutelado, como ejemplo, la muerte, el robo, entre otros.

**2.- De peligro.** Sólo ponen en riesgo el bien jurídicamente tutelado, por ejemplo, las lesiones que no causan la muerte, sino que se recupera el afectado (sic); o bien la portación de arma, toda vez que puede poner en peligro la vida o la integridad corporal.

Aquí es indispensable precisar el bien jurídico que se pretende proteger en los delitos informáticos en los tipos penales contemplados en los artículos en comento; para lo cual se considera que en el artículo 211 bis 1, es la **confidencialidad y protección de la información que se almacena en sistemas informáticos**, tan es así que el legislador lo ubica en un capítulo denominado “**Acceso ilícito a sistemas y equipo de informático**”, por lo que su transgresión estaría acorde con esa protección y al resultado obtenido. El mismo bien jurídico aparece en el artículo 217 del Código Penal para el Estado de Sinaloa no obstante de que en la fracción I, lleva implícito un resultado encaminado a la obtención de un fin de defraudar, o de obtener dinero, o bienes o información.

En cuanto a la presente clasificación del daño que se ocasionan en los delitos informáticos, se puede observar que éste se encuentra muy relacionado con la clasificación anterior, ya que los delitos de resultado formal el daño que se genera es de peligro y cuando el resultado es material, se está ante la aparición de la clasificación de daño o de lesión.

**Por su duración:**

**1.- Instantáneos.** *Cuando se consuman en un sólo movimiento y en ese momento se perfeccionan, por ejemplo el homicidio.*

**2.- Permanentes (Continuos).** *Cuando su efecto negativo se prolonga al través del tiempo, por ejemplo; el secuestro.*

**3.- Continuados.** *Cuando siendo acciones dañosas diversas producen una sola lesión jurídica; varios actos y una sola lesión.*

Los llamados delitos informáticos en los ordenamientos del estado de Sinaloa y en el Federal que he venido analizando y conforme a su naturaleza patrimonial pueden realizarse de manera instantánea, es decir, en un sólo momento perfeccionarse todos sus elementos con la obtención del resultado deseado.

También puede darse de manera continuada ya que es una característica de los delitos patrimoniales reuniéndose los requisitos que precisa el artículo 7, fracción III, del Código Penal Federal, es decir, que exista unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, violándose el mismo precepto legal. Ejemplo de ello en el Estado de Sinaloa, encontramos cuando alguna persona quiere obtener \$100,000.00 a través de entrar a una base de datos de una empresa y lo hace en 10 ocasiones por \$10,000.00 cada una. Esto es conocido en la Informática Jurídica como la "Técnica del Samali".

Similar situación puede darse en el Código Penal para el Estado de Sinaloa conforme al artículo 13 que contempla esta clasificación.

***Por el elemento interno o culpabilidad:***

**1.- Culposos.** *Cuando el agente no tiene la intención de delinquir, pero actúa con imprudencia, negligencia, descuido o torpeza, por ejemplo, el que atropella a una persona por imprudencia.*

**2.- Doloso.** *Cuando existe la plena y absoluta intención del agente para cometer su delito.*

**3.- Preterintencionales.** *El resultado va más allá de la intención del sujeto. Eliminados del Código Penal Federal en la reforma del 10 de enero de 1994.*

Esta clasificación aún se encuentra en el Código Penal para el Estado de Sinaloa en el artículo 14, párrafo tercero, que indica:

**Artículo 14.-...**

...

...

Obra preterintencionalmente el que causa un resultado típico más grave al querido, habiendo dolo directo respecto del daño deseado y culpa con relación al daño causado.

**Artículo 15.- ...**

La punibilidad del delito preterintencional, sólo es admisible, en los casos en que lo sea la del

delito culposo.

Conforme a la lectura de los artículos 217 del Código Penal para el Estado de Sinaloa los delitos informativos previstos en sus dos fracciones son definitivamente dolosos, ya que inclusive en el proemio de su artículo se aprecia un elemento eminentemente subjetivo al hacer mención que: “Comete delito informático, la persona que **dolosamente** y sin derecho”.

En el ordenamiento federal, artículo 211 bis 1, todas las formas de comisión de los delitos informáticos previstos para su consumación deben de realizarse como lo prevén sus dos párrafos, sin autorización de la persona que pueda disponer de la información o de los equipos de informática, pudiendo darse en su párrafo segundo en lo referente a “conozca o copie información”, solamente de manera dolosa, sin embargo, en su párrafo primero las conductas de “modificar, destruir o provocar pérdida de información”, puede darse de manera culposa.

No obstante de que se encuentren varias computadoras en red el que un usuario conozca o copie la información contenida en sistemas o equipos de informática, debe de ser sin autorización, ya que el usuario que pueda disponer de ella al “subirla” a la red, ya con ello está dando autorización de que otra persona la conozca.

***Por su estructura:***

**1.- *Simples.*** Cuando sólo causan una lesión jurídica, por ejemplo, el robo.

**2.- Complejos.** *Cuando causan dos o más lesiones jurídicas, por ejemplo el robo en casa habitación.*

Los tipos penales informáticos de acuerdo a esta clasificación pueden ser simples ya que se conforman a través de una sola lesión jurídica cuando se refiere al bien jurídico de la confidencialidad de la información que se almacena en los sistemas informáticos. (Artículos 211 bis 1, párrafo segundo del Código Penal Federal y 217, fracción II, del Código Penal para el Estado de Sinaloa).

Serían complejos los artículos 211 bis 1, párrafo primero del Código Penal Federal y 217, fracción I, del Código Penal para el Estado de Sinaloa, ya que además de afectarse la confidencialidad de la información, se puede incluir un robo, o un fraude como bienes jurídicos patrimoniales.

***Por el número de actos:***

**1.- Unisubsistentes.** *Cuando es suficiente un sólo acto para cometer el delito.*

**2.- Plurisubsistentes,** necesariamente requieren la concurrencia de dos o más actos en la realización del ilícito

Conforme la redacción dada por el legislador los delitos informáticos del artículo 217 de la legislación de Sinaloa y del artículo 211 bis 1, del Código Penal Federal, se aprecia la existencia de diversos actos para la concreción del delito.

**Por el número de sujetos:**

**1.- Unisubjetivos.** *Cuando el tipo se colma con la participación de un sólo sujeto.*

**2.- Plurisubjetivo.** *Cuando el tipo penal requiere de dos o más sujetos. Por ejemplo, el adulterio requiere necesariamente de dos personas (anteriormente).*

En esta clasificación se debe de atender al número de sujetos que el legislador ha incluido en la redacción del tipo penal y no confundir con el tema referente al concurso de personas sobre la autoría y participación.

Así, tanto los artículos 217 del Código Penal para el Estado de Sinaloa, como el artículo 211 bis 1, del Código Penal Federal en virtud de no señalar una exigencia en el número de sujetos activos, se puede concluir que son Unisubjetivos.

**Por su forma de persecución:**

**1.- De oficio.** *Son los delitos en los que no es necesaria la denuncia del agraviado, sino que cualquier persona la puede realizar, y el Ministerio Público, tiene la obligación de perseguir el delito, por ejemplo el homicidio.*

**2.- De querrela.** *También conocidos como a petición de parte ofendida; se piensa que es una reminiscencia de la 'venganza privada', en la que la gente se hacía justicia por su propia mano. (Como lo ha venido precisando el Doctor López Betancourt).*

Existe un principio jurídico denominado “De exclusión” que se puede aplicar para detectar en la mayoría de los ordenamientos jurídicos si los delitos son de oficio o de querrela, que señala: “Son delitos de querrela los que no son de oficio”, es decir, cuando en los códigos penales señalan que ciertos delitos son perseguibles por querrela o bien algún otro similar; los que no indique su forma de persecución son de oficio.

En los delitos informáticos del Código Penal Federal (Título Noveno) precisados en los artículos 211 bis 1 al 211 bis 7, no se indica su forma de persecución, por lo tanto son de oficio.

En el artículo 217 del Código Penal del Estado de Sinaloa, se precisa que los Delitos Informáticos son de querrela, al mencionar que:

**Artículo 237.** Los delitos de robo, robo bancario, abigeato, encubrimiento por receptación y extorsión se perseguirán de oficio, excepto cuando sean cometidos por un ascendiente, descendiente, hermano, cónyuge, concubina o concubinario, adoptante o adoptado, pariente por afinidad y por los terceros que hubieren intervenido en su ejecución con aquellos, **casos en que sólo se perseguirán por querrela de parte, al igual que los demás delitos previstos en este Título, incluyendo el robo de uso.**

Se aprecia una complejidad en la persecución de los Delitos Informáticos al ser de oficio en materia federal y por querrela en materia común en el Estado de Sinaloa.

***En función de su materia:***

**1.- Comunes.** *Son los delitos que se aplican en una determinada circunscripción territorial, en un Estado de la República Mexicana, por ejemplo. (Durango).*

**2.- Federales.** *Son los delitos que tienen validez en toda la República Mexicana y de los cuales conocerán únicamente los jueces federales.*

**3.- Militares.** *En esta división nos referimos al fuero militar, el cual es sólo aplicable en los órganos militares, es decir a todos sus miembros, pero nunca a un civil.*

Aquí hace su aparición nuevamente el “Principio de exclusión” para determinar si un delito es federal o común, es decir, es delito local el que no es federal, encontrando su fundamento en el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos que precisa la competencia de la legislatura, ya que lo legislado por la autoridad federal e indicado en ese artículo son las facultades de la Federación, todo lo que no se encuentre en ese precepto puede legislarse en el ámbito local.

De igual forma encontramos la existencia del artículo 50 de la Ley Orgánica del Poder Judicial de la Federación que precisa a los delitos federales, por lo que los que no se encuentren en ese precepto podrán ser materia de legislar en la competencia común.

Por lo tanto, en cuanto al artículo 217 del Código Penal del Estado de Sinaloa es de competencia del fuero común por ser un ordenamiento estatal, mientras que los señalados en los artículos 211 bis 1 al 211, bis 7, del Código Penal Federal, obvio resta decir que son de competencia federal ya que se encuentran en una ley de tal naturaleza.

### **Clasificación legal (Código Penal Federal):**

De acuerdo al autor en cita esta clasificación y que también es tratada por el Dr. Fernando Castellanos Tena en su obra “Lineamientos Elementales de Derecho Penal”, la misma se encuentra de acuerdo a la clasificación de los diversos apartados que realizan los códigos penales.

Así en los delitos informáticos del estado de Sinaloa aparecen dentro de los **“Delitos en contra del patrimonio”**, mientras que en los de competencia federal se encuentran en el Título Noveno denominado **“Revelación de Secretos y Acceso a Sistemas y Equipos de Información”** en su Capítulo II, **“Acceso Ilícito a Sistemas y Equipos de Información”**.

### **3.2.2. Clasificación conforme a la doctrina jurídico-informática.**

Esta clasificación de los Delitos Informáticos atendiendo a su naturaleza precisamente informática con matices jurídicos, dando como resultado el siguiente orden<sup>52</sup>:

#### **- Como instrumento o medio**

Son todas aquellas conductas en las que se tiene a las computadoras como un método, medio o símbolo en la comisión de los delitos, encontrando los siguientes:

---

<sup>52</sup> Téllez Valdez, Julio. Op. Cit, Pág. 165 y 166.

- 1.- Falsificación de documentos mediante una computadora.
- 2.- Variación de los asuntos contables de una empresa.
- 3.- Planeación o simulación de delitos convencionales.
- 4.- Robo de tiempo de computadora.
- 5.- Modificación de datos.
- 6.- Lectura, modificación, y sustracción de información confidencial.
- 7.- El aprovechamiento indebido, o alteración de códigos con el fin de penetrar un sistema para el cambio de instrucciones inapropiadas (caballo de trola).
- 8.- Variación de envío de pequeñas cantidades de dinero hacia cuentas bancarias apócrifas (técnica del salami).
- 9.- Uso no autorizado de programas de cómputo.
- 10.- Introducir instrucciones o programas que provoquen interrupción en el procesamiento lógico de otros programas de cómputo.
- 11.- Alteración en el funcionamiento de los sistemas.
- 12.- Obtención de información residual impresa en papel o cintas magnéticas luego de la ejecución de trabajos.
- 13.- Acceso a áreas informatizadas sin autorización.
- 14.- Intervención de las líneas de comunicación de datos o teleproceso.

**- Como fin u objeto.**

Son todas aquellas conductas que van dirigidas en contra de las computadoras, accesorios y programas en su integridad física; ejemplo daño en propiedad ajena, robo derechos de autor y propiedad industrial, encentrando los siguientes:

1. Programación de instrucciones que producen un bloqueo total al sistema.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.
4. Atentado físico contra la máquina o sus accesorios.
5. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
6. Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje pago de rescate etc.

### **3.3. Elementos del delito y su aplicación en el Delito Informático.**

Conforme a los elementos del delito en su aspecto positivo y negativo visualizado en la Doctrina Penal se aplicarán éstos a los delitos informáticos que he venido estudiando en el Código Penal Federal y en el Código Penal para el Estado de Sinaloa.

#### **3.3.1. Conducta y ausencia de conducta.**

Considerado el primer elemento esencial del delito o bien denominado como elemento objetivo es importante su tratamiento en cualquiera de las Teorías del Delito.

Los autores en el Derecho Penal han dado diversas definiciones sobre éste elemento objetivo.

La conducta como hecho es todo acaecimiento de la vida y lo mismo puede proceder de la mano del hombre que del mundo de la naturaleza. En cambio, acto supone la existencia de un ser dotado de voluntad que lo ejecuta.”<sup>53</sup>

Otra definición de conducta consiste en un hacer voluntario o en un no hacer voluntario o no voluntario (culpa), dirigidos a la producción de un resultado material típico o extratípico. La conducta debe entenderse como el ejercicio de un comportamiento que tiende a un fin. Por tanto, la voluntad del objetivo es claramente la base de la teoría finalista de la acción,<sup>54</sup> o como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito”.<sup>55</sup>

Para Raúl Carrancá Trujillo y Raúl Carrancá Rivas menciona sobre este elemento que: “Lo primero para que el delito exista es que se produzca una conducta humana. La conducta es, así, el elemento básico del delito. Consiste en el hecho material, exterior, positivo o negativo, producido por el hombre. Si es positivo consistirá en un movimiento corporal productor de un resultado como efecto, siendo ese resultado un cambio o un peligro de cambio en el mundo exterior, físico o psíquico. Y si es negativo, consistirá en la ausencia voluntaria del movimiento corporal esperado, lo que también causará un resultado”.<sup>56</sup>

---

<sup>53</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 210.

<sup>54</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 234.

<sup>55</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 149.

<sup>56</sup> Carrancá y Trujillo, Raúl y Carrancá y Rivas, Raúl. **DERECHO PENAL MEXICANO. (PARTE GENERAL)**. Vigésima tercera edición. Editorial Porrúa. México 2007. Pág. 295.

Una de las características esenciales de la conducta es que sea desplegada por un ser humano, a través de su libre albedrío que puede llevarse a cabo a través de diversas formas como lo veré en el siguiente apartado.

### **- Formas de aparición de la conducta**

En la realización de la conducta se encuentran tres elementos indispensables:

1.- Una manifestación de voluntad.

2.- La producción de un resultado ya sea de naturaleza formal o bien material.

3.- La existencia de una relación causal entre la conducta y el resultado. El Dr. Raúl Carrancá y Trujillo, independientemente de los anteriores conceptos, señala que ésta es “una relación de causa a efecto”.<sup>57</sup>

La conducta puede tener las siguientes formas de realización:

- Acción.

- Omisión, siendo éste el género que a su vez se divide en:

- Omisión simple, y

- Comisión por omisión.

### **- La acción.**

La acción consiste en la actividad o el hacer voluntarios dirigidos, a la producción de un resultado típico o extratípico. Es por ello, que da lugar a un tipo de prohibición.<sup>58</sup>

---

<sup>57</sup> Ibidem. Pág. 297.

<sup>58</sup> Porte Petit Caundaudap, Celestino. Op. Cit. Pág. 235.

También se puede decir que la acción consiste en una conducta exterior voluntaria encaminada a la producción de un resultado.<sup>59</sup>

Por último dentro del Finalismo, La acción humana es ejercicio de la actividad final. La acción es, por eso, acontecer 'final', no solamente 'causal'. 'La finalidad' o el carácter final de la acción se basa en que el hombre, gracias a su saber casual, puede prever, dentro de ciertos límites, las consecuencias posibles de su actividad, ponerse por tanto, fines diversos y dirigir su actividad, conforme a su plan, a la consecución de estos fines. En virtud de su saber casual previo puede dirigir los distintos actos de su actividad de tal modo que oriente el acontecer causal exterior a un fin y así lo sobredetermine finalmente. Actividad final es un obrar orientado conscientemente desde el fin, mientras que el acontecer casual no está dirigido desde el fin, sino que es la resultante casual de los componentes causales existentes en cada caso. Por eso la finalidad es -dicho en forma gráfica- 'vidente', la casualidad es 'ciega'".<sup>60</sup>

#### **- La omisión.**

Consiste en un no hacer o una inactividad, sin embargo existe aquí la obligación de hacer una conducta esperada, violándose por lo tanto una ley de índole dispositivo o

---

<sup>59</sup> Cuello Calón, Eugenio. **DERECHO PENAL, PARTE GENERAL**. Novena edición. Editorial Nacional. México 1948, Pág. 293.

<sup>60</sup> Welzel Hans. **DERECHO PENAL ALEMÁN**. Traducción del alemán por los profesores Juan Bustos - Ramírez y Sergio Yáñez Pérez. Editorial Jurídica de Chile. Chile 1977. Págs. 39 y 40.

imperativo. Apareciendo aquí la posición de garante del sujeto en torno a sus obligaciones.

La Omisión es la inactividad voluntaria cuando la norma penal impone el deber de ejecutar un hecho determinado.<sup>61</sup>

### **- La comisión por omisión.**

El Dr. Celestino Porte Petit citando a Bettiol define este concepto precisando que: Existe un delito de resultado material por omisión, cuando se produce un resultado típico y material por un no hacer voluntario o no voluntario (culpa), violando una norma preceptiva (penal o de otra rama del derecho) y una norma prohibitiva.<sup>62</sup>

Los elementos que precisa el citado autor son:

- 1.- Una voluntad o no voluntad (culpa).
- 2.- Inactividad.
- 3.- Deber de obrar (una acción esperada y exigida) y deber de abstenerse violándose así una norma preceptiva y otra prohibitiva; es decir, no se hace lo que se debe hacer y se hace lo prohibido.
- 4.- Resultado típico y material.

---

<sup>61</sup> Cuello Calón, Eugenio. Tomo I. Op. Cit. Pág. 246.

<sup>62</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 243.

## **- La conducta en los delitos informáticos.**

Una vez definida la conducta como el comportamiento humano voluntario positivo o negativo para llegar a un propósito se puede realizar en los Delitos Informáticos a los que he venido haciendo alusión en los ordenamientos del Estado de Sinaloa como a nivel Federal ya que en ambos su forma de realización será a través de la acción, es decir, siempre aparecerán por un movimiento corporal dirigido a obtener alguno de los resultados precisados.

En el caso del artículo 217, fracción I, del Código Penal para el Estado de Sinaloa el usar o entrar a una base de datos de un sistema computacional con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el propósito de defraudar, obtener dinero o bienes o información, definitivamente que sólo puede realizarse por una acción de un sujeto.

De igual forma sería la fracción II, del citado precepto jurídico ya que no es posible concebir la existencia de una omisión, dejando de hacer lo que se debe de hacer para el caso de quien intercepte, interfiera, reciba o use un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

En el artículo 211 bis 1, del Código Penal Federal los verbos rectores del tipo penal (modificar, destruir, provocar pérdida de información, conocer o copiar) la información o confidencialidad protegida en un sistema computacional nos invita a pensar que siempre se llevará a cabo a través de una acción.

## - La ausencia de conducta.

Dentro de la doctrina de la Teoría del Delito, se ha reconocido a la ausencia de conducta como un elemento negativo de esta última, que va a impedir o neutralizar la concepción y realización de la misma, evitándose así la integración o configuración del delito desde su primer elemento.

Dentro de las diversas corrientes que tratan a la Teoría del Delito se manejan las siguientes causas de ausencia de conducta que son causas que excluyen el delito y que encuentran su fundamento en el artículo 15, fracción I, del Código Penal Federal y en el artículo 26, fracción I, del Código Penal para el Estado de Sinaloa, manejándose por la doctrina las siguientes:

- 1.- Vis absoluta o fuerza física exterior e irresistible.
- 2.- Vis Maior o fuerza mayor.
- 3.- Movimientos reflejos.

1.- La *vis absoluta*. Al respecto se puede definir al decir: Cuando el sujeto realiza un hacer o un no hacer por una violencia física humana e irresistible.<sup>63</sup>

Encontramos aquí cuando una persona es empujada por otro sujeto cometiéndose un resultado aparentemente delictivo.

---

<sup>63</sup> Ibidem. Pág. 322.

2.- La *vis maior* o fuerza mayor. Cuando el sujeto realiza una actividad o una inactividad por una fuerza física irresistible, sub-humana.<sup>64</sup>

De forma similar a la anterior se da un movimiento o inamovilidad corporal producido por la naturaleza o de un animal, es decir, subhumana.

3.- Los movimientos reflejos o movimientos mecánicos. Aquí encontramos movimientos de un sujeto ocasionado por un acto impulsivo natural del ser humano como reflejo a una acción, asistiéndonos aquí a términos médicos.

Existen doctrinas que también consideran a las siguientes causas como integrantes del aspecto negativo de la conducta y otros que la incluyen en las causas de inimputabilidad por generar un estado mental inadecuado producido por causas que afectan a la voluntad del agente:

- El sueño.
- El hipnotismo.
- El sonambulismo.
- El alcoholismo.

Sobre el presente tema cabe hacer la precisión de que, para algunos penalistas son verdaderos aspectos negativos de la conducta; el sueño, el hipnotismo y el sonambulismo, pues en tales fenómenos psíquicos el sujeto realiza la actividad o inactividad sin voluntad, por hallarse en un estado en el cual su conciencia se encuentra suprimida y han desaparecido las fuerzas inhibitorias. Otros especialistas los sitúan entre

---

<sup>64</sup> Ibidem, Pág. 324.

las causas de inimputabilidad.<sup>65</sup> Como se determina en las *actiones liberae in causa* sobre las cuales se referirán en el Capítulo de la inimputabilidad.

#### **- La ausencia de conducta en los delitos informáticos.**

Los delitos informáticos materia de la presente investigación han sido clasificados como delitos de acción por las razones antes expuestas, por lo que como causa de exclusión del delito que va a invalidar jurídicamente el presente elemento objetivo es difícil considerar que se actualice la *vis maior*, la *vis absoluta* y los movimientos reflejos, ni tampoco las *actiones liberae in causa* antes vistas como son: el sueño, el hipnotismo y el sonambulismo. (En caso de considerarse en este apartado).

No es dable considerar que se argumente que una persona cometió un delito informático argumentando que lo haya empujado un ser humano o bien, una fuerza subhumana, llámesele animal o de la naturaleza. También sería difícil darse a través del influjo de bebidas embriagantes o de drogas, en el sueño, por hipnotismo o el sonambulismo, ya que los ilícitos informáticos implican una maquinación técnica que no es posible que se den a través de tales estados adquiridos de manera involuntaria.

#### **3.3.2. Tipicidad y atipicidad.**

El segundo elemento esencial del delito es la Tipicidad, que se ha considerado como el encuadramiento de la conducta a un tipo penal

---

<sup>65</sup> Castellanos Tena, Fernando. Op. Cit. Págs. 165 y 166.

## - Concepto de tipicidad.

Dentro de los autores más destacados que han definido a la tipicidad encontramos a:

La tipicidad es la exigida correspondencia entre el hecho real y la imagen rectora expresada en la ley en cada especie de infracción.<sup>66</sup>

También se puede considerá a la tipicidad como una expresión propia del Derecho Punitivo, equivalente técnico del apotegma político '*nullum crimen sine lege*'; bien con el nombre con que ahora técnicamente se le designa, bien como garantía de libertad consagrada en la parte dogmática de las Constituciones políticas, la tipicidad ha sido, desde el inicio de los regímenes de derecho, el fundamento del hecho punible. Las legislaciones de la casi totalidad de los países modernos proclaman expresamente este principio. Así, por lo que respecta a México, el artículo 14 de la Constitución Federal dispone que: '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'; y el artículo 7 del Código Penal estatuye que: 'Delito es el acto u omisión que sancionan las leyes penales.'<sup>67</sup>

---

<sup>66</sup> Jiménez de Asúa, Luis. **TRATADO DE DERECHO PENAL**. Tomo III, Tercera edición actualizada. Editorial Losada, S.A. Buenos Aires 1965. Pág. 746.

<sup>67</sup> Jiménez Huerta, Mariano. **DERECHO PENAL MEXICANO**. Tomo I. Sexta edición, Editorial Porrúa. México 1989. Op. Cit. Pág. 20.

El Dr. López Betancourt hace referencia a la tipicidad mencionando a Laureano Landaburu, al señalar que la tipicidad consiste en esa cualidad o característica de la conducta punible de ajustarse o adecuarse a la descripción formulada en los tipos de la ley penal.<sup>68</sup>

Otra forma de explicar a la tipicidad con fundamento en el tipo penal es que si el tipo penal es la descripción, en la ley penal, de un comportamiento previsto como acción u omisión dentro de un determinado ámbito situacional, que es lesivo a un bien jurídico protegido penalmente, a la vez que violatorio del mandato o prohibición contenido en la norma que precisamente implica la valoración normativa de la ley, consecuentemente, la tipicidad es la atribuibilidad de una conducta, dentro de su ámbito situacional, a la descripción típica penal, es decir, la conducta prevista por la ley penal, dentro del ámbito situacional en que la misma aparece regulada y que implican la presencia de elementos objetivos, normativos y subjetivos del tipo.<sup>69</sup>

Para el Dr. Raúl Carrancá y Trujillo, la tipicidad es: “La acción antijurídica ha de ser típica para considerarse delictiva...la acción ha de encajar dentro de la figura de delito creada por la norma penal positiva, pues de lo contrario al faltar el signo externo distintivo de la antijuridicidad penal, que lo es la tipicidad penal, dicha acción no constituiría delito. Pero puede existir la tipicidad penal sin que exista acción antijurídica,

---

<sup>68</sup> López Betancourt, Eduardo. Op. Cit. Pág.117.

<sup>69</sup> 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.** Segunda edición. Editorial Porrúa. México 1998. Págs. 321 y 322.

como ocurre con las causas de justificación en las que hay tipicidad y también juridicidad, por lo que el delito no existe.”<sup>70</sup>

Por ultimo la tipicidad se puede explicar como la adecuación o conformidad a lo prescrito por el tipo. <sup>71</sup> (La importancia de la tipicidad consiste en que se establece en una forma clara y patente, que no hay delito sin tipicidad).

Una de la razones importantes sobre la tipicidad es que da origen al principio de legalidad “*nullum crimen, nulla poena sine lege*”, debiendo hacer la distinción entre la tipicidad y el tipo que definitivamente son conceptos diferentes como se verá posteriormente

#### **- La tipicidad en el delito informático.**

Ante lo comentado la tipicidad de un delito informático consiste en el perfecto encuadramiento de alguna conducta desplegada por el sujeto activo y que con todas y cada una de sus características se adecue a algunos de las descripciones legislativas, o tipos penales en sus elementos tanto objetivos, normativos y subjetivos, ya sea del fuero común en el Estado de Sinaloa en el artículo 217 de su Código Penal, o bien en el ámbito federal en alguna de las hipótesis previstas en los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7, del Código Penal Federal.

---

<sup>70</sup> Carrancá y Trujillo Raúl y Carrancá y Rivas Raúl. Op. Cit. Pág. 451.

<sup>71</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 333.

### 3.3.3. El tipo penal y ausencia de tipo.

#### - El tipo penal

Definiciones clásicas y tradicionales pero no menos importantes sobre el tipo penal son las que a continuación señalaré:

El Dr. Celestino Porte Petit dice que: “El tipo constituye un presupuesto general del delito, dando lugar a la fórmula: *nullum crimen sine typo*.”<sup>72</sup>

El tipo penal se define como: el injusto descrito concretamente por la ley en sus diversos artículos y a cuya realización va ligada la sanción penal.<sup>73</sup>

También se puede hacer mención al tipo legal que es la abstracción concreta que ha trazado el legislador, descartando los detalles innecesarios para la definición del hecho que se cataloga en la Ley como delito.<sup>74</sup>

Finalmente el tipo penal se puede definir como la creación legislativa, la descripción que el Estado hace una conducta en los preceptos penales.<sup>75</sup>

El tipo penal encuentra su fundamento en el “principio de legalidad”, concretamente al antes referido principio de “reserva legal”, ya que solamente el

---

<sup>72</sup> Ibidem. Pág. 335.

<sup>73</sup> Mezger, Edmundo. **TRATADO DE DERECHO PENAL**. Tomo I. Traducción de J. Arturo Rodríguez Muñoz. Editorial Revista de Derecho Privado. Madrid España 1955. Pág. 366.

<sup>74</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 235.

<sup>75</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 167.

legislador puede realizar las definiciones de lo que considera como delito, encontrando su fundamento como ya se revisó en el artículo 73, fracción XXI, del Constitución Política de los Estados Unidos Mexicanos.

#### **- Clasificación del tipo penal.**

En este punto aprovecharé la tradicional clasificación que realiza el Dr. Fernando Castellanos Tena<sup>76</sup>, la cual ajustaré los tipos penales informáticos que he venido analizando tanto en el ámbito local (Sinaloa), como en el Federal.

**Por su composición**, pueden ser normales y anormales;

Los tipos son considerados normales cuando de su lectura aparecen elementos fáciles a la comprensión y al entendimiento contemplando aspectos objetivos.

En cuanto a los tipos anormales encontramos aquellos elementos que necesitan de alguna definición sobre todo de naturaleza subjetiva.

Los tipos anormales son aquellos en que la impaciencia del legislador le ha hecho penetrar en el juicio valorativo de la antijuridicidad, incluyendo en la descripción típica elementos normativos o excesivas alusiones a elementos subjetivos de lo injusto.<sup>77</sup>

---

<sup>76</sup> Ibidem Pág. 171.

<sup>77</sup> Jiménez de Asúa, Luís. **LA LEY Y EL DELITO**. Op. Cit. Pág. 255.

En los delitos informáticos plasmados en la legislación sinaloense como en la federal encontramos que su clasificación es anormal, por los diversos y variados elementos normativos y subjetivos que tienen en sus respectivos tipos penales tales como los que se subrayan a continuación:

Artículo 217, del Código Penal para el Estado de Sinaloa:

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

I.- Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, o bienes o información; o

II.- Intercepte, interfiere, 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.

Artículo 211 bis 1, del Código Penal Federal:

**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”.

Como se puede apreciar los tipos penales informáticos son anormales ya que tienen diversos elementos con gran variedad de connotaciones.

**Por su ordenación metodológica,** los tipos penales pueden ser fundamentales o básicos, especiales y complementarios.

Como su nombre lo indica los tipos penales son básicos o fundamentales ya que son los cimientos de la estructura de otros tipos, es decir, que no deriva de tipo penal alguno, y cuya existencia es totalmente independiente de cualquier otro tipo.<sup>78</sup>

En torno a éstos tipos básicos encontramos que se pueden estructurar los especiales y los complementados, en donde en los primeros se conforman con los básicos y una peculiaridad o característica que originan a un tipo diferente y que el nuevo cambia de denominación los que pudieran ser que atenúen o incrementen la pena; ejemplo de ellos fueron los delitos de infanticidio (especial atenuado) y de parricidio (especial agravado).

De forma similar, los complementados se conforman de un tipo fundamental o básico y se les agrega una circunstancia o peculiaridad que origina otro tipo penal sin cambiar de nombre, es decir su nomenclatura se conforma con el básico y dicha peculiaridad que también puede atenuar o agravar la pena. Ejemplo de éstos encontramos el homicidio en riña (complementado atenuado) y el homicidio con ventaja (complementado agravado).

Los tipos complementados se constituyen con uno básico y una circunstancia o peculiaridad distinta (como en el homicidio calificado).<sup>79</sup>

---

<sup>78</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 355.

En los delitos a estudio tanto en el Estado de Sinaloa como en el ámbito Federal los Delitos Informáticos pueden considerarse **especiales**, ya que se conforman con un tipo básico y una peculiaridad que origina otro tipo penal con otra denominación (Delitos Informáticos), sin embargo, en el presente aparatado es en donde cobra vigencia parte del dilema de la controversia jurídica de éstos delitos atendiendo a lo siguiente;

En la legislación sinaloense el artículo 217 del Código Penal tiene su estructura básica en delitos tales como: robo, daño en propiedad ajena que van en contra de los derechos de autor e inclusive de fraude y su denominación según el Capítulo al que pertenecen es de “Delito Informático”, correspondiente al Título denominado: “Delitos contra el patrimonio”. Convirtiéndose en atenuado en comparación con las sanciones de los tipos básicos, por ser menor su sanción.

Por otra parte en el artículo 211 bis 1, del Código Penal Federal, los tipos básicos o fundamentales que dan origen a esos tipos son los de: robo, daño en propiedad ajena, en contra de los derechos de autor y su denominación que también atiende al Capítulo en donde se localizan es el de: “Acceso ilícito a sistemas y equipos de información”, correspondiente al Título noveno denominado “Revelación de secretos y acceso ilícito a sistemas y equipos de informática”. Convirtiéndose en atenuado en comparación con las sanciones de los tipos básicos federales, por ser menor su sanción.

---

<sup>79</sup> Márquez Piñero, Rafael. **DERECHO PENAL. PARTE GENERAL**. Cuarta edición. Primera reimpresión agosto 1999. Editorial Trillas. México 1997. Pág. 231.

En cualquiera de los dos casos el Delito Informático justifica su creación como un tipo especial.

**Por su autonomía.** Pueden ser autónomos o subordinados. Se consideran tipos autónomos los que tienen vida por sí mismos, mientras que son dependientes o subordinados cuando se requiere la existencia de algún otro tipo. Esta clasificación se acopla a la anterior al señalar que son básicos o fundamentales los que son autónomos, y son especiales y complementados, aquéllos que son subordinados, ante lo cual los delitos informáticos son clasificados como subordinados desde su estructura, ya que derivan como se ha precisado de otros tipos como el robo, el daño en propiedad ajena, fraude, entre otros.

**Por su formulación.** Se clasifican en casuísticos y amplios. Son considerados casuísticos aquellos tipos penales que en su redacción aparecen diversas formas de realización para la comisión del delito, mientras son denominados amplios aquellos tipos que en su texto solamente existe una forma de concreción del delito.

El Dr. Porte Petit hace referencia sobre los tipos de formulación casuística que: es aquél en que no se señala casuísticamente el medio para producir del resultado contenido en el típico.<sup>80</sup>

El tipo casuístico puede ser dividido en: alternativo y acumulativo, siendo los primeros cuando de las diversas hipótesis puede colmarse el delito con cualquiera de

---

<sup>80</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 358.

ellas, mientras que son tipos acumulativos cuando se necesita la conjunción de todas las hipótesis para la realización del delito descrito.

De la lectura del tipo penal establecido en el artículo 217 del Código Penal para el Estado de Sinaloa y del artículo 211 bis 1, del Código Penal Federal son de formulación causísticos alternativo, ya que como se desprende de su lectura están conformados de varias hipótesis y no es necesaria la conjunción de todas, es decir, con cualquiera de ellas se actualiza el delito.

**Por su resultado.** Esta clasificación se divide en tipos de daño y tipos de peligro.

Son tipos de daño, cuando existe una destrucción del bien jurídico protegido por la norma penal. Son tipos de peligro, cuando el bien jurídico se encuentra en riesgo. Ejemplo de los primeros es el daño en propiedad ajena, homicidio, lesiones, mientras que de los segundos encontramos al delito de portación de arma de fuego.

Por lo tanto para adecuar esa clasificación a nuestros delitos informáticos debemos recordar que anteriormente se señaló al bien jurídico que se pretende proteger por el legislador es “**la confidencialidad y protección de la información que se almacena en los sistemas informáticos**”, por lo que sus tipos penales en ambas legislaturas a estudio pueden ser clasificadas como tipos de resultado de daño, ya que su trasgresión trae aparejada una disminución o destrucción de ese bien jurídico.

Más aún son de daño los tipos penales cuando precisamente se hace alusión a los conceptos de “dañar”, “destruir”, o “provocar pérdida”, con la reflexión de que tales vocablos son sinónimos vista anteriormente.

### **- Los elementos del tipo penal.**

De gran importancia el presente tema, ya que son estos elementos del tipo penal a los que se debe de ajustar una conducta de manera exacta para que se de lo que se ha llamado la tipicidad.

En la doctrina mexicana seguida por autores prestigiados como los Doctores Celestino Porte Petit y Fernando Castellanos Tena, pilares de nuestro Derecho Penal se han relacionado estos elementos de la siguiente forma:

**a) Elementos objetivos y normativos.-** Como condiciones externas o jurídicas encontradas en el tipo penal de naturaleza objetiva en donde se advierten:

- 1.- Los sujetos activo y pasivo.
- 2.- El objeto o bien del delito, clasificado en:
  - Objeto o bien material, y
  - Objeto o bien jurídico.
- 3.- El elemento normativo que también acepta la siguiente división:
  - Valoración cultural.
  - Valoración jurídica.
- 4.- La acción u omisión considerada en el tipo penal.

5.- Las circunstancias objetivas de agravación o atenuación contenidas en el tipo, las cuales se subclasifican en:

- Referencias temporales.
- Referencias espaciales.
- Medios de ejecución.

Los elementos objetivos son aquellos susceptibles de ser apreciados por el simple conocimiento y cuya función es describir la conducta o el hecho que pueden ser materia de imputación y de responsabilidad penal.<sup>81</sup>

Para el estudioso Edmundo Mezger menciona que los elementos objetivos o descriptivos del tipo son: “estados y procesos externos, susceptibles de ser determinados espacial y temporalmente, perceptibles por los sentidos (objetivos), fijados en la ley por el legislador en forma descriptiva”.<sup>82</sup>

Como se precisó los elementos objetivos son aquellos que son tangibles y fáciles y demostrar en la materia procesal.

Los elementos normativos son aquellos que llevan una interpretación jurídica o cultural.

---

<sup>81</sup> Pavón Vasconcelos, Francisco. **MANUAL DE DERECHO PENAL MEXICANO**. Décima edición debidamente corregida y puesta al día. Editorial Porrúa. México 1991. Pág. 276.

<sup>82</sup> Mezger, Edmundo. Op. Cit. Tomo I. Pág. 372.

**b) Elementos subjetivos.** Son aquellos que reflejan la intención del sujeto, o bien la finalidad que tuvo en la realización de su conducta. Aquí es en donde la Teoría Finalista incluye dentro del tipo penal a la antijuridicidad y la culpabilidad.

**- Elementos del tipo penal informático.**

Basados en la relación antes mencionada de los elementos objetivos y normativos se procederá al análisis de los elementos que se encuentran en los delitos informáticos que aparecen en los Códigos Penales que he venido estudiando:

**- El sujeto activo y el sujeto pasivo.**

El sujeto activo de un delito se ha considerado como aquella persona que lleva a cabo la realización de la conducta considerada como delictiva, es decir, el delincuente. Mientras que el sujeto pasivo es aquella persona a la que le recae el daño, debiendo diferenciar aquí al sujeto ofendido que es aquél que resiente el daño, importante éste último en el Derecho Procesal Penal.

En ocasiones el legislador hace mención señala algunas calidades específicas de los sujetos activo y pasivo en las hipótesis delictivas, de ser así la conducta desplegada del hombre debe tener tales exigencias.

Hay que resaltar que a veces el tipo establece determinada *calidad en el sujeto activo* a la cual queda subordinada, por así decirlo, la punibilidad de la acción bajo un

concreto tipo delictivo. Ello excluye la posibilidad de ejecución de la conducta (acción u omisión) por cualquier sujeto y por tal razón se les ha denominado *delitos propios particulares o exclusivos*, para diferenciarlos de los delitos de *sujeto común o indiferente*.<sup>83</sup>

Nuevamente aquí se debe de atender a lo que el legislador redactó en los tipos penales de los delitos informáticos sin que encontremos una calidad específica para el sujeto activo ni tampoco del pasivo en el artículo 217 del Código Penal para el Estado de Sinaloa, ni en el artículo 211 bis 1, del Código Penal Federal, estudiados en el presente documento; sin embargo, en los tipos penales federales plasmados en los artículos 211 bis 2 al 211 bis 5 aparecen exigencias al respecto como son:

Artículos 211 bis 2 y 211 bis 3.- Aparece una calidad del sujeto pasivo al señalar al Estado.

Artículos 211 bis 4 y 211 bis 5.- Aparece como calidad en el sujeto pasivo a las entidades del sistema financiero.

#### **- El objeto material y el bien jurídico.**

En la doctrina penal mexicana se diferencia entre el objeto material y el objeto jurídico, siendo el primero la cosa, o bien la persona sobre la que recae el daño de un delito, mientras que el objeto jurídico es considerado el bien tutelado por la norma penal.

---

<sup>83</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 276.

Al respecto el Dr. Carrancá y Trujillo hace referencia que el objeto material del delito: es la persona o cosa sobre la que recae el delito. Lo son cualesquiera de los sujetos pasivos o bien las cosas animadas o inanimadas, (distinguiendo del objeto jurídico como),...el bien o el interés jurídico, objeto de la acción incriminable. Por ejemplo; la vida, la integridad corporal, la libertad sexual, la reputación, la propiedad privada, etc...<sup>84</sup>

El objeto jurídico de un delito consiste en la valoración que hace el legislador de lo que pretende proteger con su figura delictiva, encontrando bienes tales como: la vida, la libertad sexual, el patrimonio, entre otros.

Visto así el objeto material en los delitos informáticos se considera que estarían integrados por los datos contenidos en la información cibernética o bien, el sistema informático e inclusive el propio equipo computacional, ya que cabe recordar que se puede incurrir en éste delito cuando se use, altere o se destruyan tales objetos.

Por lo que respecta al bien jurídico tutelado ya se ha precisado que es **“la confidencialidad y protección de la información que se almacena en los sistemas informáticos”**, perteneciendo al género de los delitos patrimoniales, así como el propio patrimonio cuando se atenta en contra de estos sistemas computarizados.

---

<sup>84</sup> Carrancá y Trujillo, Raúl. Op. Cit. Pág. 292.

## **- El elemento normativo en el delito informático.**

Este elemento consiste en la connotación que se le debe dar a ciertas palabras principalmente desde un punto de vista jurídico.

El Dr. Eduardo López Betancourt menciona que: los elementos normativos del tipo se refieren a hechos que únicamente pueden pensarse bajo el presupuesto lógico de una norma.<sup>85</sup>

El citado autor conjuntamente con otros tratadistas mexicanos como Celestino Porte Petit y Fernando Castellanos Tena consideran dividir a estos elementos atendiendo a su valoración en:

- Valoración normativa cuando se atiende a conceptos de naturaleza jurídica.
- Valoración cultural, cuando la interpretación debe ser apoyada en aspectos culturales, pudiéndose consultar diccionarios de tal naturaleza.

En los delitos informáticos que son novedad en el mundo jurídico y que aparecen en la legislación sinaloense y federal encontramos diversos elementos normativos tanto de índole jurídica como cultural tales como:

### **Artículo 217 del Código Penal para el Estado de Sinaloa:**

---

<sup>85</sup> López Betancourt, Eduardo. Op. Cit. Pág. 131.

**Fracción I.-** base de datos - sistema de computadoras – red de computadoras - diseñar – ejecutar – alterar – esquema – artificio – defraudar (eminentemente jurídico) – dinero – bienes de información,

**Fracción II.-** interceptar – interferir – recibir – usar – alterar – dañar –destruir – soporte lógico – programa de computadora – base – sistema – red.

**Artículo 211 bis 1 del Código Penal Federal.**

- modificar – destruir – provocar pérdida – información – sistemas o equipos de informática protegidos – mecanismo de seguridad – conocer o copiar información.

Son de llamar la atención los artículos 211 bis 4 y 211 bis 5, del Código Penal Federal, en donde encontramos otro elemento que cabe resaltar consistente en las instituciones que pertenecen al sistema financiero, entendiéndose como tales de acuerdo al artículo 211 bis 6, las que precisa el artículo 400 bis del propio ordenamiento federal relativo al delito de “Operaciones con recursos de procedencia ilícita” conocido como “Lavado de Dinero” y que es la repetición de lo que señalan las leyes financieras tales como la Ley de Instituciones de Crédito. Véase aquí la valoración jurídica que debe darse a ese elemento.

Dentro de estos conceptos cobra gran relevancia los referentes a “sistemas computacionales” del cual ya se hizo mención en el Capítulo Primero, además del referente a la “información” sobre el que haré algunas reflexiones a continuación: Como ya se ha mencionado con anterioridad el concepto de información se ha convertido en un

término muy amplio que con los avances en las tecnologías en especial con la aparición de la súper carretera de la información, para el Diccionario de la Real Lengua Española información se define como: “1.f. Acción y efecto de informar. 5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada”<sup>86</sup>.

En un sentido actual la información puede entenderse como un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno<sup>87</sup>, como ejemplo podríamos armar una investigación referente a un tema en especial, primero hay que recolectar una serie de datos que al final procesados, sintetizados e incluso una vez aclarados llegan a constituir la información sobre el tema a tratar. Se tiene que tomar en cuenta que la idea de información cubre toda rama del conocimiento humano y por conocer.

Con la llegada de la informática y las nuevas tecnologías, la información se ha generalizado e incluso popularizado, con lo que ha surgido el tratamiento de la información la cual se define como: Aplicación sistemática de uno o varios programas sobre un conjunto de datos para utilizar la información que contienen.<sup>88</sup> Se tiene que recordar que las computadoras actuales procesan datos de manera ordenada y específica para representar información la cual nosotros podremos comprender con nuestros sentidos, ya sea música, imágenes, animación, video o texto, que al ser

---

<sup>86</sup> **DICCIONARIO PLANETA DE LA LENGUA ESPAÑOLA.** Op. Cit. Tomo VI. Pág. 700.

<sup>87</sup> <http://es.wikipedia.org/wiki/Información>

<sup>88</sup> **DICCIONARIO DE LA LENGUA ESPAÑOLA.** Tomo 6. Op. Cit. Pág. 863.

alterados dichos datos puede presentar la información de diferente manera, con los avances en las tecnologías todo se presenta de manera Multimedia la cual puede ser entendida como “Multi” que significa muchos y “medios” que significa “al método utilizado para difundir la información”<sup>89</sup>, que ésta a su vez se convierte en interactiva la cual es una herramienta hoy en día muy eficiente para la educación y negocios.

Con la popularización de la información y el fácil acceso a ésta con las nuevas tecnologías ha llevado a que las personas deseen conocer cada vez más, que incluso con las ideas globales de Democratización se desea conocer los movimientos del gobierno, por lo que ante ésta preocupación en México ha surgido la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en la que podríamos encontrar la definición de Información, lo que puede entenderse y comprender dentro de ella en sus Artículo 3, 13 y 14 vistos en el Capítulo 2 de la presente investigación.

Con lo anterior se puede demostrar que la palabra Información es un término verdaderamente amplio con el que hay que tener mucho cuidado al ser empleado ya que puede comprender tanto imágenes, videos, audio, animaciones, textos como documentos, libros, datos tanto como personales, empresariales y gubernamentales, y que incluso los mismos datos con los que funciona una computadora para ser procesado y obtener nueva información, y gracias a las nuevas tecnologías es posible acceder a ella en cualquier momento y de manera rápido con lo que nos permite tomar decisiones rápidas informadas e incluso usar dicho conocimiento en nuestro beneficio, que como la

---

<sup>89</sup> Haskin, David. **MULTIMEDIA FÁCIL**. (Traducción. Sánchez García Gabriel). Editorial Prentice Hall. México 1995. Pág. 8.

historia lo ha demostrado el control de la misma implica el control de las masas, con lo que en muchas ocasiones podemos considerar a la información como un bien susceptible a ser apoderado y con un valor propio.

En este punto de los elementos normativos del tipo penal cobran vigencia las reglas de interpretación de la Ley Penal en todos y cada uno de los conceptos a definir, debiendo asistirse para ello de la propia legislación penal u otra conforme a la naturaleza de la figura a definir, acudir a la jurisprudencia, a la doctrina y a los diccionarios jurídicos e inclusive académicos.

**- Las circunstancias de agravación o atenuación contenidas en el tipo penal informático.**

Estas circunstancias que tienen la propiedad de agravar o atenuar la pena de un delito atendiendo a la importancia que el legislador le da se actualizan cuando hace exigencias en las hipótesis delictivas de los siguientes puntos:

- a) Las referencias temporales.
- b) Las referencias espaciales.
- c) Los medios de ejecución.

**a) Las referencias temporales.**

Estas aparecen en los tipos penales cuando el legislador considera necesaria alguna situación de tiempo, es decir, determina cierto tiempo para la comisión de un delito. Ejemplo de ello tenemos el ilícito de traición a la patria, cuando hace referencia a tiempos de guerra.

En ocasiones la ley establece determinados medios temporales como exclusivamente típicos, y por tanto, no caerá bajo el tipo, la ejecución en tiempo distinto del que se señala en la ley.<sup>90</sup>

En los delitos informáticos a estudio no se aprecia una referencia o exigencia que deba darse en un determinado tiempo.

#### **b) Las referencias espaciales.**

Las circunstancias espaciales son cuando la ley fija exclusivamente como típicos determinados medios locales de comisión del delito, y que la ejecución del acto en otro lugar no recaerá bajo el tipo.<sup>91</sup>

Al respecto el legislador considera que en la hipótesis delictiva aparezcan exigencias de lugar para llevarse a cabo la comisión de algún delito, ejemplo el delito de robo en casa habitación, el robo en despoblado, entre otros.

---

<sup>90</sup> Mezger, Edmundo. **TRATADO DE DERECHO PENAL**. Tomo I. Op. Cit. Pág. 369.

<sup>91</sup> Ibidem. Pág. 369.

En los tipos en los que plasman los delitos informáticos tanto en el Estado de Sinaloa como en el Federal no aparece ninguna referencia espacial que se convierta en una exigencia.

### **c) Los medios de ejecución.**

Los llamados delitos con medios legalmente determinados o limitados, quiere decir, que para que pueda darse la tipicidad tienen que concurrir los medios que exija el tipo correspondiente. Por delitos con medios legalmente determinados debemos entender aquellos tipos de delitos en los que la tipicidad de la acción se produce, no mediante cualquier realización del resultado último sino sólo cuando éste se ha conseguido en la forma que la ley expresamente determina.<sup>92</sup>

Estas exigencias sobre los medios de ejecución aparecen en determinadas formas de comisión del delito que el legislador anota en los tipos penales, como ejemplo encontramos a la violencia física o moral que se exigen en el delito de violación, el engaño o el error en el delito de fraude, la violencia psicológicas en el delito de violencia intrafamiliar, etc...

Los delitos informáticos a estudio tienen una gran variedad de medios de ejecución tales como:

Artículo 217 del Código Penal para el Estado de Sinaloa:

---

<sup>92</sup> Idem.

– defraudar (eminentemente jurídico que lleva implícito el medio del error o el engaño) – interceptar – interferir – recibir – usar – alterar.

En el artículo 211 bis 1, del Código Penal Federal, no se aprecian medios de ejecución, salvo que se considere como éstos, el que la modificación, destrucción o pérdida de la información sea a través de sistemas o equipos informáticos.

#### **- Los elementos subjetivos en el tipo penal informático.**

Estos elementos son los que reflejan una especial culpabilidad del sujeto activo para la comisión de un delito, es decir, se refieren al ánimo de una persona demostrando su situación interna.

Los elementos subjetivos del injusto son cuando el legislador tipifica conductas que sólo son delictivas si se toma en cuenta la situación anímica del sujeto que actúa, ha de hacer referencia, en forma explícita o implícita, a dichos elementos subjetivos que, desde el momento en que dejan su impronta en la estructura del tipo, se convierten en verdaderos elementos del mismo.<sup>93</sup>

Este aspecto subjetivo de la antijuridicidad liga a ésta con la culpabilidad, estableciendo así un contacto entre ambas características del delito. El legislador, como

---

<sup>93</sup> Jiménez Huerta, Mariano. **DERECHO PENAL MEXICANO**. Tomo I. Op. Cit. Pág. 51.

he dicho, los incluye a menudo en el tipo y son los *elementos típicos subjetivos del injusto*, que han sido valorados de distinto modo”.<sup>94</sup>

En los tipos penales el legislador ha colocado esos elementos subjetivos cuando hace mención a términos tales como: maliciosamente, dolosamente, a sabiendas, el que con conocimiento, el que intencionalmente, entre otras.

En el artículo 217 del Código Penal para el Estado de Sinaloa encontramos un elemento subjetivo cuando menciona en su proemio; “...la persona que **dolosamente** y sin derecho”, así como cuando hace referencia a que la realización del delito informático tenga ciertos fines como el “de defraudar, obtener dinero, o bienes o información” (fracción I). Por lo que si no se demuestra que el sujeto activo haya tenido alguna de esas finalidades no se llevará a cabo el delito.

En el artículo 211 bis 1 del Código Penal Federa, no se aprecia algún elemento subjetivo o que demuestre una situación anímica del activo.

#### **- La atipicidad y ausencia de tipo.**

Si consideramos a la tipicidad como la adecuación de la conducta a un tipo penal o figura o hipótesis delictiva, la atipicidad es la falta de encuadramiento de esa conducta al referido tipo penal a todos y cada uno de sus elementos objetivos, normativos y subjetivos que así se requieran.

---

<sup>94</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág, 255.

La ausencia de tipo presupone la absoluta imposibilidad de dirigir la persecución contra el autor de una conducta no descrita en la ley, incluso a que sea antijurídica. Es consecuencia primera de la famosa máxima *nullum crimen, nulla poena sine lege*, que técnicamente se traduce: ‘no hay delito sin tipicidad’... casos específicos de atipicidad y ausencia total de tipo. Cuando un hecho de la vida diaria presenta ciertos aspectos que parecen hacerle subsumible en un tipo legal y explorado éste resulta que faltan las referencias del sujeto activo, como cuando por ejemplo, el protagonista de un pretendido delito que exige función pública no es funcionario.<sup>95</sup> Sobre este último caso encontramos la atipicidad por no reunirse los elementos del tipo.

Sobre la ausencia de tipo el Dr. Celestino Porte Petit señala: “no existe descripción de la conducta o hecho por la norma penal, y en el segundo caso, la descripción existe pero no hay conformidad o adecuación al tipo”.<sup>96</sup>

Existe ausencia de tipo cuando no existe en el mundo jurídico la descripción de la conducta como delito, descrita por el legislador, siendo importante que sea por el poder legislativo, ya que aquí opera un principio importante de legalidad para el Derecho Penal que es el de “reserva legal” consistente en que únicamente el legislador es el facultado para crear hipótesis delictivas, ningún otro poder lo puede decidir.

En relación a éste punto se debe tener cuidado que en un tipo penal no se le deje su descripción al Poder Ejecutivo su intervención para que lo integre, ya que se

---

<sup>95</sup> Ibidem. Pág. 263.

<sup>96</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 366.

estaría violando el citado principio a tal grado de que se encuentre en riesgo de que se declare inconstitucional la figura delictiva. Tal es el caso de lo acontecido en el año 2004 con el artículo 171, fracción II, del Código Penal Federal, declarado inconstitucional conforme a la tesis de jurisprudencia número 5/2008 de la Primera Sala de la Suprema Corte de Justicia de la Nación que dice: “ATAQUES A LAS VÍAS GENERALES DE COMUNICACIÓN. LA FRACCIÓN II DEL ARTÍCULO 171 DEL CÓDIGO PENAL FEDERAL QUE PREVÉ ESE DELITO, VIOLA LOS PRINCIPIOS DE EXACTA APLICACIÓN Y RESERVA DE LA LEY MATERIA PENAL”,<sup>97</sup>.

La ausencia del tipo debe ser tratada, en cada caso, examinando cuidadosamente el articulado de la parte especial de los códigos -o las leyes especiales y las complementarias- para comprobar si el hecho está o no tipificado.<sup>98</sup> El legislador no considera que una conducta antisocial sea elevada al grado de delito, posiblemente solamente se incluya como infracción administrativa, o definitivamente no la considere como antisocial.

La atipicidad tiene tres consecuencias:

*a) No se integraría al tipo penal.* (Originando la inexistencia del delito).

*b) Existencia de otro delito.* Es decir se da una traslación de un tipo penal a otro tipo penal (originando así una variación del tipo).

---

<sup>97</sup> Tesis de Jurisprudencia número 5/2008 de la Primera Sala de la Suprema Corte de Justicia de la Nación.

<sup>98</sup> Márquez Piñero, Rafael. Op. Cit., Pág. 232

c) *Existencia de un delito imposible*. Cuando falta por ejemplo: el bien jurídico (siendo una tentativa imposible).<sup>99</sup>

#### **- La atipicidad y ausencia de tipo informático.**

Tomando en consideración los elementos objetivos, normativos y subjetivos de los tipos penales que contemplan los delitos informáticos en las legislaturas de Sinaloa y en la Federal, habrá atipicidad cuando la conducta desplegada por un sujeto activo no se adecue a esos elementos que señalan las hipótesis delictivas previstas en los tipos penales de las legislaciones mencionadas.

No se puede hablar de ausencia del tipo penal del delito informático ya que como se ha indicado ese delito se encuentra perfectamente creado por los legisladores del Estado de Sinaloa en el artículo 217 de su Código Penal, siendo también creado por el legislador federal en los artículos 211 bis 1 al 211 bis 7, del Código Penal Federal, y hasta el momento no se ha declarado alguna causa de inconstitucionalidad por parte del Poder Judicial de la Federación como aconteció con el artículo 171, fracción II, del Código Penal Federal, antes visto.

#### **3.3.4. La antijuridicidad y las causas de licitud.**

Existen diferentes posturas sobre este tema desde considerarla como un elemento que nos señala que es ir en contra del Derecho, hasta aquellos que la

---

<sup>99</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 371.

consideran inexistente ya que si la tipicidad es la adecuación de una conducta a un tipo penal, no es posible que surja algo en contra de la ley, ya que lo que hace el sujeto activo es precisamente adecuarse a la ley (hipótesis delictiva), no ir en su contra.

### **- Concepto de antijuridicidad.**

Hay que analizar desde su raíz etimológica de la antijuridicidad del latín *anti* que significa, lo contrario; y de *juridice*, como Derecho; es decir, es ir en contra del Derecho.

La antijuridicidad a diferencia de la tipicidad, tiene un ámbito de valoraciones es diverso del sentido de la valoración inicial de la norma que nace con esta y frente a su violación genera la antinormatividad propia de la tipicidad, cuando no opera alguna causa de atipicidad.<sup>100</sup>

Se debe diferenciar a la antijuridicidad del injusto, siendo la primera una contradicción a los ordenamientos jurídicos, mientras que la segunda, se enfoca a la conducta antijurídica en sí, originando con ello dos aspectos fundamentales a estudiar como son:

- Los elementos subjetivos del injusto.
- El injusto personal.

Se plasma al injusto penal integrado por la tipicidad y la antijuridicidad dividiendo a esta última de la siguiente manera: (atribuida esta clasificación principalmente a Franz Von Liszt).

---

<sup>100</sup> Malo Camacho, Gustavo. Op. Cit. Pág. 404.

- Antijuridicidad formal.
- Antijuridicidad material.

La antijuridicidad formal o nominal, es el acto formalmente contrario al Derecho, en tanto que es trasgresión de una norma establecida por el Estado, de un mandato o de una prohibición del orden jurídico.<sup>101</sup> Es cuando se atenta contra la ley concretamente.

La antijuridicidad material, será materialmente contrario al Derecho cuando esté en contradicción con los fines del orden jurídico que regula la vida común; esta lesión o riesgo será materialmente legítima, a pesar de ir dirigida contra los intereses jurídicamente protegidos, en el caso y en la medida en que responda a esos fines del orden jurídico, y, por consiguiente, a la misma convivencia humana. Ese contenido material (antisocial) de la infracción es independiente de su exacta apreciación del legislador.<sup>102</sup> Es decir, se atenta contra los intereses reales de la sociedad.

A esta última los finalistas la llamaron “el injusto personal” que es el desvalor de la acción, incluyendo la finalidad de la acción ya sea dolosa o culposa y que va referida a la conducta del sujeto activo.

Dentro de esta Teoría Finalista es importante hacer mención a Welzel que destaca el injusto personal y que refiere a la antijuridicidad es siempre la desaprobación

---

<sup>101</sup> Jimenez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 277.

<sup>102</sup> Ibidem. Pág. 278.

de un hecho referido a un autor determinado. Lo injusto de la acción referida al autor es injusto personal.<sup>103</sup>

#### **- La antijuridicidad en el delito informático.**

Precisamente en ésta época moderna porque el legislador ha considerado importante la protección de la información que se guarda de una manera confidencial a través de diversos medios informáticos o contra éstos es que ha tomado la determinación de realizar un juicio valorativo y llegar a la conclusión de considerar antijurídicas las conductas y que atenten en contra de esa información contenida en medios informáticos y contemplarlas dentro de los códigos penales, así lo valoró el legislador sinaloense al crear el tipo penal previsto en el artículo 217 y el legislador federal al crear las figuras de los artículos 211 bis 1 al 211 bis 7, del Código Penal Federal.

Por lo tanto en un delito informático una conducta típica es antijurídicamente cuando va en contra de los preceptos jurídicos antes mencionados (antijuridicidad formal), lo cual va en contra de los valores que pretende proteger el legislador en una sociedad en la que a través de los medios informáticos ha pretendido proteger su información o proteger a tales medios, haciendo patente mayormente la preocupación del Estado sobre esa protección cuando el sujeto pasivo o persona a la que le recae el daño es el propio Estado o una entidad financiera, por la importancia de la información concentrada en ellos, además hay que recordar que en la historia de México se han

---

<sup>103</sup> Welsel, Hans. Op. Cit. Pág. 74.

dado grandes crisis financieras que han desestabilizado a nuestro país, por lo que es menester resguardar sigilosamente esa información financiera. Tal es el caso de los artículos 211 bis 3 al 21 bis 5, del Código Penal Federal.

#### **- Las causas de licitud o de justificación en el delito informático.**

La antijuridicidad de una conducta típica deja de serlo cuando aparece su aspecto negativo con normas de índole permisivas, llamándose causas de licitud, de justificación, o inclusive de permisión, dentro de las que encontramos:

- La legítima defensa.
- El estado de necesidad.
- Cumplimiento de un deber y ejercicio de un derecho, y
- El consentimiento del titular del bien afectado.

Son causas de justificación las que excluyen la antijuridicidad de una conducta que puede subsumirse en un tipo legal; esto es, aquellos actos u omisiones que revisten aspecto de delito, figura delictiva, pero en los que falta, sin embargo, el carácter de ser antijurídicos, de contrarios al Derecho, que es el elemento más importante del crimen.<sup>104</sup>

Existe una causa de licitud, cuando la conducta o hecho siendo típicos, son permitidos, autorizados o facultados por la ley, a virtud de ausencia de intereses o de la existencia de un interés preponderante, para este autor, la conducta o hecho siendo típicos, son permitidos por la ley, en virtud de ausencia de interés o por existir un interés

---

<sup>104</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Pág. 284.

preponderante, es decir, es aquella especial situación en la que un hecho que normalmente está prohibido por la ley penal, no constituye delito por la existencia de una norma que lo autoriza o lo impide.<sup>105</sup>

Las causas de justificación son aquellas condiciones que tienen el poder de excluir la antijuridicidad de una conducta típica. Representan un aspecto negativo del delito: en presencia de alguna de ellas falta uno de los elementos esenciales del delito, a saber: la antijuridicidad.<sup>106</sup>

#### **- La legítima defensa.**

La legítima defensa es la repulsa de una agresión antijurídica y actual o inminente por el atacado o por terceras personas contra el agresor, sin traspasar la medida necesaria para la protección.<sup>107</sup>

También la legítima defensa es la repulsa de la agresión ilegítima, actual o inminente, por el atacado o tercera persona, contra el agresor, sin traspasar la necesidad de la defensa y dentro de la racional proporción de los medios empleados para impedir la o repelerla.<sup>108</sup>

---

<sup>105</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 386.

<sup>106</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 183.

<sup>107</sup> Ibidem. Págs.191 y 192.

<sup>108</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 289.

Otra forma en la que se puede definir a la legítima defensa es el contraataque (o repulsa) necesario y proporcional a una agresión injusta, actual o inminente, que pone en peligro bienes propios o ajenos, aún cuando haya sido provocada insuficientemente.<sup>109</sup>

La legítima defensa en materia federal encuentra su fundamento en el artículo 15, fracción IV, del Código Penal Federal, mientras que en el Código Penal para el Estado de Sinaloa aparece en el artículo 26, fracción IV, del Código Penal para el Estado de Sinaloa, destacando que los principales elementos de esta figura son:

- La repulsa de una agresión.
- Una agresión real, actual o inminente.
- Que la agresión sea antijurídica.
- Que dicha repulsa a la agresión sea para proteger bienes propios o ajenos.
- Que cuando se realice la repulsa a una agresión, no se base en una provocación por parte del agredido o de la persona a quien se va a defender.

**- El estado de necesidad.**

Otra de las causas de licitud o de justificación o de permisión que impide la integración de la antijuridicidad es el estado de necesidad en la que se ataca a un bien jurídicamente protegido por la norma para salvaguardar otro de igual o de mayor valor.

---

<sup>109</sup> Porte Petit Candaudap, Celestino. Op. Cit. Pág. 394.

Estamos frente al estado de necesidad, cuando para salvar un bien de mayor o igual entidad jurídicamente tutelado o protegido, se lesiona otro bien, igualmente amparado por la ley. Existe el estado necesario, cuando haya la necesidad de salvar un bien de mayor o igual entidad jurídicamente tutelado, de un peligro grave, actual o inminente, lesionando otro bien igualmente amparado por la ley, siempre que no se tenga el deber jurídico de afrontarlo y no sea el peligro ocasionado dolosa o culposamente por el propio agente.<sup>110</sup>

Fernando Castellanos Tena señala que el estado de necesidad en cuanto a sus elementos es una situación de peligro real, actual e inminente; que ese peligro no haya sido ocasionado intencionalmente por el agente; la amenaza recaiga sobre cualquier bien jurídicamente tutelado (propio o ajeno), con un ataque por parte de quien se encuentra en el estado necesario; y que no exista otro medio practicable y menos perjudicial al alcance del agente.<sup>111</sup>

El Código Penal Federal prevé esta causa en el artículo 15, fracción V, mientras que el Código Penal para el Estado de Sinaloa lo contempla en el artículo 26, fracción V, encontrando que los principales elementos de esta figura son:

- La existencia de un peligro real, actual o inminente.
- El peligro no debe de haberse ocasionado por el agente.
- El peligro debe de radicar sobre bienes propios o ajenos,

---

<sup>110</sup> Ibidem. Pág. 431.

<sup>111</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 206.

- La producción de una lesión a otro bien jurídico que puede ser de igual o de menor valor que el que se protege o salva.

- Que el peligro no se pueda evitar por otro medio menos perjudicial.

- Que el agente no tenga el deber o la obligación de afrontar dicho peligro.

El estado de necesidad a diferencia de la legítima defensa es que la primera es un ataque a un bien jurídicamente protegido, mientras que en la segunda es un contraataque.

#### **- El cumplimiento de un deber y ejercicio de un derecho.**

Cuando el sujeto activo actúa bajo el amparo de un ordenamiento jurídico o bien cumpliendo un deber que tiene conferido, no aparecerá la antijuridicidad, encontrando aquí las normas permisivas, ejemplo de ello es el ejercicio del derecho en el deporte de boxeo que tiene un pugilista cuando en el ring lesiona a su contrincante, o cuando un bombero cumpliendo su deber de salvar vidas tiene que romper una puerta, ocasionando daños en propiedad ajena, o el médico en cumplimiento de su deber de salvar una vida lesiona a un sujeto con su bisturí al operarlo de un padecimiento grave.

El Código Penal Federal contempla esta situación en el artículo 15, fracción VI, mientras que el Código Penal para el Estado de Sinaloa lo previene en el artículo 26, fracción VII, refiriendo a los siguientes elementos:

- Que la conducta realizada por el sujeto activo esté en el cumplimiento de un deber o en el ejercicio de un derecho y estos se encuentren permitidos por la ley.

- La existencia de la necesidad racional del medio empleado para cumplir el deber o ejercer el derecho.

- Que el cumplimiento de un deber o ejercicio de un derecho no se realice con el propósito de perjudicar a otro.

#### **- El consentimiento del titular del bien jurídico afectado.**

Aquí debemos estar presente ante un bien jurídico protegido por la ley que pueda disponerse por el sujeto pasivo para poder otorgar ese consentimiento de que alguien disponga de él.

Encuentra su fundamento en artículo 15, fracción III, del Código Penal Federal, y en el artículo 26, fracción II, del Código Penal para el Estado de Sinaloa, destacando también los siguientes elementos:

- La existencia de un bien jurídico que pueda disponerse.

- Que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo.

- La existencia de un consentimiento expreso o tácito y que no exista algún vicio sobre dicho consentimiento.

Algunos autores consideran a la legítima defensa y al estado de necesidad como una causa de cumplimiento de un deber y ejercicio de un derecho, ya que las mismas deben de estar permitidas en la ley.

#### **- Las causas de justificación o de licitud en el delito informático.**

Una conducta será típica del delito informático cuando se ajuste a todos los elementos descritos en las hipótesis jurídicas previstas en el artículo 217 del Código Penal para el Estado de Sinaloa, o bien al artículo 211 bis 1, del Código Penal Federal, conforme a lo que he venido estudiando, o bien, en las hipótesis de los artículos 211 bis 2 al 211 bis 5, del citado ordenamiento federal, sin embargo será antijurídica cuando no opere ninguna de las causas de justificación o de licitud antes vistas.

Por lo que podríamos hablar de las existencias de las siguientes causas de licitud o justificación o de permisión:

Por lo que respecta a la legítima defensa es absurdo pensar que una persona pretenda justificar su conducta de haber violado la información protegida en los sistemas informáticos, o de dañarlos, o de ocasionar un fraude por defenderse de una agresión de esos bienes jurídicos tutelados por el legislador.

En cuando al estado de necesidad sí sería posible pretender justificar la comisión de una conducta típica al delito informático haciendo patente el atacar a un bien jurídico para salvaguardar otro igual o de mayor valor. Pudiéramos mencionar como ejemplo aquella persona que tiene el conocimiento de que en las computadoras de una empresa de energía nuclear se tuviera información confidencial de que se haría explotar una bomba atómica, por lo que se infiltraría a través de algunos de los medios comisivos de los tipos penales para obtener sin autorización esa información con la que salvara a una población de tal estallido atómico.

En esta causa de licitud habría que tener mucho cuidado, ya que como en todos los delitos pudiera anteponerse la violación de cualquier bien jurídico tutelado justificándola con la protección inclusive de una vida humana, para no caer en el absurdo siguiente; cuando un narcotraficante transporta cocaína y pretende justificarse de que con esa actividad obtendría dinero para salvarle la vida a un pariente.

Como en todas las causas de exclusión del delito pudieran invocarse en cualquier conducta típica, lo importante es que sean lógicas y que sean demostrables. En la práctica jurídica existe un apotegma que dice: “el derecho no es de quien lo tiene sino del que lo sabe probar y a su debido tiempo”. Del mismo modo será una obligación práctica por parte del Agente del Ministerio Público ya sea local o federal acreditar los elementos del cuerpo del delito y la probable responsabilidad; debiendo recordar los principios de “presunción de inocencia” y de “el que afirma está obligado a probar”.

Por lo tanto, las causas del cumplimiento de un deber o cumplimiento de un derecho pudieran darse en los delitos informáticos si el sujeto activo demuestra fehacientemente de que tenía el deber de actuar de infiltrarse a obtener información en los medios electrónicos, o bien destruirlos, o de defraudar, o bien que alguna disposición jurídica le permitía hacerlo.

En cuanto al consentimiento del titular del bien jurídico tutelado se puede precisar que una persona que tiene “encriptada” su información en un sistema computacional le dé permiso a otra para que tenga acceso a dicha información, sin

embargo, más bien estaríamos en presencia de una causa de atipicidad ya que la conducta del activo no se estuviera encuadrando a tales tipos penales que requieren dentro de sus elementos que sea “sin autorización”; artículo 211 bis 1, del Código Penal Federal.

### **3.3.5. La imputabilidad y la inimputabilidad.**

El criterio sostenido dentro de la presente investigación se acoge a aceptar que la imputabilidad es un presupuesto de la culpabilidad por las razones que se explicarán en el desarrollo del presente tema.

#### **- Concepto de imputabilidad.**

La mayoría de los autores han coincidido de que la imputabilidad es un presupuesto de la culpabilidad ya que mantienen sincronía con sus respectivos elementos relativos a la voluntad y al conocimiento, existiendo al respecto diversas definiciones tales como las que a continuación se mencionarán.

La imputabilidad es la capacidad de querer y de entender en el campo del Derecho Penal. Querer es estar en condiciones de aceptar o realizar algo voluntariamente, y entender es tener la capacidad mental y la edad biológica para desplegar esa decisión.<sup>112</sup>

---

<sup>112</sup> López Betancourt, Eduardo. Op. Cit. Pág. 180.

Será pues, imputable, todo aquel que posea al tiempo de la acción las condiciones psíquicas exigidas, abstracta e indeterminadamente, por la ley, para poder desarrollar su conducta socialmente; todo el que sea apto e idóneo jurídicamente para observar una conducta que responda a las exigencias de la vida en sociedad humana.<sup>113</sup>

En la imputabilidad se puede hacer mención a los siguientes elementos:

- El elemento intelectual o de conocimiento, reflejado en la capacidad de comprensión de lo injusto.
- Un elemento volitivo para conducirse conforme a esa comprensión.

Lo anterior es resumido en la teoría causalista como:

- Capacidad de querer, y
- Capacidad de entender.

En la legislación mexicana la imputabilidad se ha reducido a dos situaciones a saber:

- Que la persona se encuentre bien de sus facultades mentales tanto de forma permanente como transitoria.
- Que el sujeto activo sea mayor de edad. En donde ha prevalecido el criterio de uniformar la edad penal a los 18 años.

---

<sup>113</sup> Carrancá y Trujillo, Raúl. Op. Cit. Pág. 463.

En el Código Penal Federal como en la legislación punitiva sinaloense un sujeto es imputable a los 18 años de edad.

#### **- La imputabilidad en el delito informático.**

Por lo tanto para que un sujeto fuere imputable respecto a algún Delito Informático a nivel federal y en el Estado de Sinaloa, es necesario que se encuentre bien de sus facultades mentales y que tenga una mayoría de edad penal.

#### **- La inimputabilidad.**

Son causas de inimputabilidad la falta de desarrollo y salud de la mente, así como los trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la facultad de conocer el deber.<sup>114</sup>

Si la imputabilidad, según el criterio más generalizado, es la capacidad del sujeto para conocer el carácter ilícito del hecho y determinarse espontáneamente conforme a esa comprensión, la *inimputabilidad* supone, consecuentemente, la ausencia de dicha capacidad y por ello *incapacidad* para conocer la ilicitud del hecho o bien para determinarse en forma espontánea conforme a esa comprensión.<sup>115</sup>

---

<sup>114</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 339.

<sup>115</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 375.

Así, se considerarían inimputables aquellos que en el momento de la realización de su conducta estuvieran mal de sus facultades mentales o bien fueren menores de edad.

En relación a la parte final del citado artículo 15, fracción VII, del Código Penal Federal algunos autores han incluido a las “*acciones liberae in causa*” vistas en Capítulos anteriores. Hipótesis que se encuentra en el artículo 26, fracción VII, del Código Penal para el Estado de Sinaloa.

La inimputabilidad se convierte así en la ausencia de la capacidad de querer y de entender frente al Derecho Penal, traducida a contrario *sensu* respecto a las causas de imputabilidad como aquellas personas que en el momento de su conducta típica y antijurídica se encuentren trastornadas mentalmente de manera permanente o transitoria y sean menores de la edad penal, como lo indicia el Código Penal Federal en su artículo 15, fracción VII, cuando “al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible”, siendo similar su tratamiento en el artículo 26, fracción IX, del Código Penal para el Estado de Sinaloa.

### **- Las causas de inimputabilidad en el delito informático.**

Por lo anterior podré concluir que una persona que fuere menor de la edad penal o se encontrare en una situación mental como las señaladas y llevara a cabo alguna de las conductas que establecen los artículos relacionados a los delitos informáticos ya sea en la legislación del Estado de Sinaloa o en la Federal, estaría respaldada por una causa de exclusión del delito considerada como inimputabilidad, estando fuera del Derecho Penal y su efecto sería su valoración jurídica a través de los sistemas especiales de tratamiento de menores a los que se les ha llamado infractores y a las nuevas disposiciones sobre justicia para adolescentes, o de las medidas de seguridad que se regulan para los trastornados mentales.

Las causas de inimputabilidad operarían en cualquier conducta típica antijurídica en el Derecho Penal.

### **3.3.6. La culpabilidad y la ausencia de culpabilidad.**

Dentro de la Teoría Causalista la culpabilidad ocupa el cuarto y último elemento esencial del delito, mientras que los finalistas tratan a este elemento dentro del tipo penal al hacer referencia a los elementos subjetivos del tipo.

- **Concepto de culpabilidad.**

Diversas definiciones se han dado sobre la culpabilidad derivado de diversas corrientes como la Causalista y la Finalista, tales como:

Para Eugenio Zaffaroni, la culpabilidad es la reprochabilidad del injusto al autor.<sup>116</sup> (la que sólo es posible cuando revela que el autor ha obrado con una disposición interna a la norma violada, disposición que es fundamento de la culpabilidad)

Según Jiménez de Asúa las especies de la culpabilidad - el dolo y la culpa, con las correspondientes subespecies- no son características de aquella, como Mezger ha creído ni formas de presentación. Constituyen auténticas especies en las que encarna conceptualmente el género abstracto *culpabilidad*.....(dicho tratadista define al dolo de la siguiente manera:)...existe cuando se produce un resultado típicamente antijurídico, con consciencia de que se quebranta el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la relación de causalidad existente entre la manifestación humana y el cambio en el mundo exterior, con voluntad de realizar la acción y con representación del resultado que se quiere o ratifica...(señalando como culpa),...en su sentido más clásico y general no es más que la ejecución de un acto que pudo y debió ser previsto, y que por falta de previsión en el agente, produce un efecto dañoso.<sup>117</sup>

---

<sup>116</sup> Zaffaroni Eugenio, Raúl. **MANUAL DE DERECHO PENAL**. Quinta reimpresión. Editorial Cárdenas. Pág. 543.

<sup>117</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Págs. 358, 365 y 371.

También se establece que la culpabilidad es el nexo intelectual y emocional que liga al sujeto con su acto.<sup>118</sup>

La culpabilidad puede ser explicada desde dos puntos de vista:

- Teoría Psicológica.
- Teoría Normativa.

En la Teoría Psicológica se explica la existencia de un nexo principalmente subjetivo entre el sujeto y su conducta o el resultado ocasionado, dependiendo si es un simple delito de conducta o bien, de resultado.

En el sistema causalista se observa al dolo como una relación psíquica entre el autor y el resultado, añadiéndole a dicha relación el reproche; mientras que en el finalismo, el dolo es ubicado en el tipo penal en donde aparece esa relación psicológica, dejando para la culpabilidad el reproche como juicio valorativo.

Así, la culpabilidad para los finalistas tiene tres elementos:

- a) La imputabilidad o capacidad de culpabilidad.
- b) El conocimiento de la antijuridicidad del hecho cometido, y
- c) La exigibilidad de un comportamiento distinto.

---

<sup>118</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 234.

## - Formas de culpabilidad.

Las formas de aparición de la culpabilidad es a través de dos:

- Dolo, y
- Culpa.

Las mismas encuentran su fundamento en el artículo 9 del Código Penal Federal que dice:

“**Artículo 9.-** Obra dolosamente el que, conociendo los elementos del tipo penal, o previniendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley, y

Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales”.

El dolo es el actuar, consciente y voluntario, dirigido a la producción de un resultado típico y antijurídico,<sup>119</sup> y tiene varias acepciones en el ámbito del derecho. Aquí se entiende como conciencia y voluntad de realizar el tipo objetivo de un delito.<sup>120</sup>

El dolo tiene dos elementos a saber:

- El elementos de conocimiento o intelectual
- El elemento de intención o también llamado volitivo.

---

<sup>119</sup> Ibidem. Pág. 239

<sup>120</sup> Muñoz Conde, Francisco. **TEORÍA GENERAL DEL DELITO**. Segunda edición. Editorial Toblandú. 1991. Pág. 60.

En cuanto al índole volitivo de su conducta, encontramos que el agente tiene el deseo de que con ella se produzca un resultado típico y antijurídico.

En relación a la culpa Luis Jiménez de Asúa señala que en su sentido más clásico y general no es más que la ejecución de un acto que pudo y debió ser previsto, y por falta de previsión en el agente, produce un efecto dañoso.<sup>121</sup>

Ignacio Villalobos dice que una persona tiene culpa cuando obra de tal manera que, por su negligencia, su imprudencia, su falta de atención, de reflexión, de pericia, de precauciones o de cuidados necesarios, se produce una situación antijurídica típica no querida directamente ni consentida por su voluntad, pero que el agente previó o pudo prever y cuya realización era evitable por él mismo.<sup>122</sup>

Existe culpa cuando se realiza la conducta sin encaminar la voluntad a la producción de un resultado típico, pero éste surge a pesar de ser previsible y evitable, por no ponerse en juego, por negligencia o imprudencia, las cautelas o precauciones legalmente exigidas".<sup>123</sup>

Se puede hablar también de la existencia de culpa cuando la actitud del sujeto, enjuiciada a través del imperativo de los deberes impuestos por la ley, es reprochable a virtud de la inobservancia de la prudencia, atención, pericia, reglas, órdenes, disciplinas,

---

<sup>121</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 371.

<sup>122</sup> Villalobos, Ignacio. **DERECHO PENAL MEXICANO**. Quinta edición. Editorial Porrúa. Méxicó 1990. Pág. 307.

<sup>123</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 248.

etc., necesarias para evitar la producción de resultados previstos en la ley como delictuosos.<sup>124</sup>

También en la culpa encontramos elementos como son:

- Que se lleva a cabo a través de una acción o bien de omisión.
- La falta de previsión o de cuidado. En la que radica la posición de garante.
- Se da un resultado ya sea típico y antijurídico.

En la culpa se puede dar las siguientes clasificaciones:

- a) Culpa consciente o con representación. y
- b) Culpa inconsciente o sin representación.

En la culpa con representación o conciente, el sujeto activo realiza una conducta teniendo la esperanza de que el resultado delictivo no se produzca, mientras que en la culpa inconsciente o sin representación la conducta del sujeto activo no se prevé la existencia de algún delito.

El dolo es explicado con gran agilidad por los finalistas ya que es precisamente aquí cuando un sujeto tiene el fin o finalidad de llevará a cabo una conducta ilícita, es decir, tiene la voluntad de llevarla a cabo y el conocimiento de su actuar.

Sin embargo con la culpa los finalistas tuvieron algunos problemas en explicarla ya que aquí no existe la finalidad de producir un resultado (por ello es culpa, no se quiere

---

<sup>124</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 405.

el resultado sin embargo se acepta), por lo que los finalistas manejaron la finalidad de la conducta del sujeto activo no radica en su dirección a ese resultado delictivo, sino dirigirla a realizar una actividad lícita, la cual debe de llevarse a cabo con toda diligencia, es decir, cobra actualidad la posición de garante; sin embargo al no tener cuidado en llevar a cabo esa actividad lícita se realiza un resultado ilícito. Ejemplo, la persona que limpia un arma y se le dispara accidentalmente lesionando a otro, su finalidad con la posición de garante es limpiarla adecuadamente, lo que no realiza con tal atingencia y por falta de cuidado produce un resultado ilícito.

#### **- La culpabilidad en el delito informático.**

Atendiendo a la redacción de los tipos de los delitos informáticos previstos en el Código Penal del Estado de Sinaloa y en el Código Penal Federal, se desprende una realización principalmente dolosa de estos delitos, tal sería el caso del artículo 217 del Código Penal para el Estado de Sinaloa en donde en su proemio refleja un elemento eminentemente subjetivo al precisar que “la persona que dolosamente”. Sin embargo los delitos informáticos de naturaleza federal (artículo 211 bis 1) no hace su aparición este elemento subjetivo y sus formas de comisión puede ser tanto dolosas como culposas, como sería el caso de “la modificación, destrucción o pérdida de la información”, ejemplo: cuando una secretaría sin autorización de su jefe para entrar a su computadora personal quiere ser atingente y buscar algunos datos para quedar bien y por falta de cuidado ocasiona daño a la información protegida en el sistema (culpa), o definitivamente de manera intencional quiere dañar esa información porque su jefe le cae mal (dolo).

## **- Causas de ausencia de culpabilidad.**

La inculpabilidad o causas de inculpabilidad son causas de exclusión del delito que tienen por objeto el evitar que se integre el elemento volitivo y cognoscitivo del delito, por lo tanto invalidar el juicio de reproche.

La inculpabilidad consiste en la falta de nexo causal emocional entre el sujeto y su acto, esto es, la falta del nexo intelectual y emocional que une al sujeto con su acto.<sup>125</sup>

Dentro de las causas de inculpabilidad que la doctrina penal maneja encontramos:

- El error
- La no exigibilidad de otra conducta.
- Eximentes putativas.

El error puede apreciarse de dos formas.

En el error de tipo, se está en presencia de un desconocimiento por parte del sujeto activo sobre alguna circunstancia objetiva del hecho desprendida del tipo penal, que bien puede ser sobre un elemento descriptivo o normativo del tipo.

En cuanto al error de prohibición el sujeto activo se confunde en relación con el conocimiento de su conducta, de decir, tiene una equivocación sobre la antijuridicidad

---

<sup>125</sup> López Betancourt, Eduardo. Op. Cit. Pág. 238.

del hecho con el pleno conocimiento de la realización del tipo. Aquí el sujeto sabe lo que está haciendo pero considera que su conducta se encuentra respaldada lícitamente con independencia de que conozca perfectamente la norma jurídica, ya que cabe recordar la existencia de un principio importante en el Derecho Penal de que “la ignorancia de la ley no exime su cumplimiento.

Se considera que el error es divergencia entre la representación del agente y la realidad. Ignorancia es falta de conocimiento; error es conocimiento equivocado.<sup>126</sup>

Dentro de la corriente causalista el error se ha clasificado de la siguiente manera:

a) Error de derecho, y

b) Error de hecho, subclasificándose a éste en:

- Error de hecho esencial.
- Error de hecho accidental.

Los finalistas que han tenido predominancia en este tema denominan que el error de hecho, ahora es el error de tipo, mientras que el llamado error de derecho es lo que ahora se considera el error de prohibición. “Abandonada mayoritariamente la distinción italiana entre *error de hecho* y *error de derecho* por la notoria dificultad de

---

<sup>126</sup> Reynoso Dávila, Roberto. **TEORÍA GENERAL DEL DELITO**. Segunda edición. Editorial Porrúa. México 1997. Pág. 260.

establecer una clara frontera entre ambos errores, ahora se prefiere hablar de *error de tipo* y *error de prohibición*.<sup>127</sup>

El penalista Roberto Reynoso Dávila haciendo referencia a Alexander Graff Zu Dohna inició la terminología de error sobre el error de tipo y error sobre la prohibición en lugar de error de hecho y de derecho; error de hecho (sobre los caracteres del tipo) y error sobre la prohibición (error de Derecho). El error sobre el tipo, consiste en el desconocimiento o equivocada creencia sobre las circunstancias objetivas pertenecientes al tipo legal. Excluyendo claro está del dolo. Ejemplo: el cazador que dispara contra un objeto negro, creyéndolo una pieza, cuando en realidad se trata de una leñadora. Será punido como autor de un delito culposo. Error de prohibición, que es el que recae sobre la antijuridicidad del hecho en el conocimiento completo de la realización del tipo (por consiguiente, en el absoluto dolo del tipo). El autor sabe lo que hace, pero yerra en cuanto a si es permitido o no. Este error excluye la reprochabilidad; es inculpable. La diferencia entre ambos errores se halla condicionada históricamente por las partes de conceptos *error facti* y *error iuris*.<sup>128</sup>

La legislación Penal Federal contempla a los errores antes vistos en el artículo 15 fracción VIII que dice:

“Artículo 15.-El delito se excluye cuando:

I...

II...

...

VIII.- Se realice la acción o la omisión bajo un error invencible:

---

<sup>127</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 435.

<sup>128</sup> Reynoso Dávila, Roberto. Op. Cit. Págs. 265 y 266.

a) Sobre alguno de los elementos esenciales que integran el tipo penal; o **(ERROR DE TIPO)**.

b) Respecto de la ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma, o porque crea que está justificada su conducta. **(ERROR DE PROHIBICIÓN)**.

Si los errores a que se refieren los incisos anteriores son vencibles, se estará a lo dispuesto por el artículo 66 de este Código”.

En el Código Penal para el Estado de Sinaloa se prevén estos errores en el artículo 26, fracción X.

Por lo que respecta a lo no exigibilidad de otra conducta ésta ha sido criticada ya que refleja una emotividad en el sujeto activo, situación que es de índole subjetivo, y se ha clasificado de la siguiente manera:

1.- El estado de necesidad cuando se sacrifica un bien de igual valor.

2.- Cuando obra el temor fundado e irresistible (*vis compulsiva*). Traduciéndose en una coacción.

Respecto a las eximentes putativas que alteran la psique del sujeto por caer en el mundo de lo imaginario, el maestro Jiménez de Asúa señala que: Cabe lo putativo en el cumplimiento de la ley cuando se cree que ésta autoriza un acto que, en realidad, no se permite; en el estado de necesidad... y, sobre todo, en la defensa.<sup>129</sup>

Por eximentes putativas se entienden las situaciones en las cuales el agente, por un error esencial de hecho insuperable cree, fundadamente, al realizar un hecho típico

---

<sup>129</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit.. Pág. 404.

del Derecho Penal, hallarse amparado por una justificante, o ejecutar una conducta atípica, permitida, lícita, sin serlo.<sup>130</sup>

Estas causas de inculpabilidad se encuentran contempladas en el mundo del error de prohibición visto anteriormente.

#### **- Causas de ausencia de culpabilidad en el delito informático.**

Como se ha visto, las causas de inculpabilidad pretenden influir en la voluntad del sujeto activo sobre todo en concretarse en el mundo de los errores, en donde se actúa considerando que su conducta es la correcta o bien que está justificada por alguna disposición jurídica o considera que el alcance de la ley es el correcto.

Así los delitos informáticos previstos en el Código Penal para el Estado de Sinaloa y en el ámbito Federal, pueden darse tanto el error de tipo como el de prohibición, ya que podemos encontrar a un sujeto que esté en la convicción de que tiene la autorización de alguien para poder acceder a un sistema computacional y obtener una información protegida, o bien, alguna persona cree que puede obtener esa información por la interpretación errónea de la ley o tiene un desconocimiento de ella (situación aún más difícil ya que cabe recordar el principio de que la ignorancia de la ley no exime su cumplimiento"); sin embargo, en este apartado debemos de recordar que éstas causas de exclusión del delito, como las demás, deben de probarse fehacientemente para desvirtuar la integración del presente elemento del delito.

---

<sup>130</sup> Castellanos Tena, Fernando. Op. Cit.. Pág. 267.

### **3.3.7. Las condiciones objetivas de punibilidad y su ausencia.**

Tema discutido en la Teoría del Delito, ya que existen posturas que las consideran como condicionantes objetivas para poder aplicar una pena, y que se encuentran en el tipo penal, con lo cual estaríamos más bien en presencia de los elementos del tipo penal. Otros incluyen en este tema a los requisitos de procedibilidad.

#### **- Concepto de las condiciones objetivas de punibilidad.**

El Doctor Eduardo López Betancourt haciendo mención a Ernest Von Beling dice sobre estos elementos o consecuencia ciertas circunstancias exigidas por la ley penal, para la imposición de la pena, que no pertenecen al tipo del delito y no condicionan la antijuridicidad y tampoco tienen carácter de culpabilidad.<sup>131</sup>

También son aquellas exigencias ocasionalmente establecidas por el legislador para que la pena tenga aplicación”.<sup>132</sup>

Las condiciones objetivas de punibilidad deben diferenciarse de los presupuestos procesales. En las primeras se expresa el grado de menoscabo del orden jurídico protegido, que en cada caso se requiere, mientras que los presupuestos

---

<sup>131</sup> López Betancourt, Eduardo. Op. Cit. Pág. 247.

<sup>132</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 278.

procesales toman en consideración circunstancias opuestas a la verificación de un proceso penal.<sup>133</sup>

#### **- Las condiciones objetivas de punibilidad en el delito informático.**

Si consideramos que las condiciones objetivas de punibilidad son aquéllos elementos objetivos que sirven para aplicar una sanción y que están dentro del tipo penal, como se mencionó, estamos en presencia de los elementos del tipo penal y por lo tanto este tema ya ha sido abordado en su respectivo apartado.

En cuanto a considerar a estas condicionantes como requisitos de procedibilidad (denuncia y querella), igualmente ya se comentó que estos delitos son de oficio en el ámbito federal y por querella en el ámbito común en el Estado de Sinaloa.

#### **- La ausencia de condiciones objetivas de punibilidad.**

El Dr. López Betancourt hace una importante diferencia entre incumplimiento y ausencia de las condiciones objetivas de punibilidad determinando que en caso de incumplimiento el hecho no sería punible, mientras que en la ausencia realmente estamos frente a una hipótesis delictiva que no requiere tal circunstancia, es decir, dicho autor concluye que el incumplimiento de las condiciones de punibilidad, traerá consigo el impedimento de la aplicación de la sanción correspondiente. Cabe mencionar, que el incumplimiento de las condiciones objetivas de punibilidad difiere de la ausencia de

---

<sup>133</sup> López Betancourt, Eduardo. Op. Cit. Págs. 247 y 248.

éstas, en virtud de que en la primera hipótesis no se realizan los requisitos exigidos por la ley, mientras en la segunda...el precepto jurídico no lo establece.<sup>134</sup>

### **- Las causas de ausencia e incumplimiento de las condiciones objetivas de punibilidad en el delito informático.**

El incumplimiento de las condiciones objetivas de punibilidad de los delitos informáticos bajo la primer postura radicaría en que no se cumplan con los elementos objetivos descritos por los correspondientes tipos penales, y ante la segunda postura consistiría en que siendo delito perseguible de oficio en el ámbito federal y por querrela en el Estado de Sinaloa no se dieran éstas situaciones.

### **3.3.8. La punibilidad y las excusas absolutorias.**

#### **- Concepto de punibilidad.**

Existen variadas posturas sobre la definición de la punibilidad tales como:

La amenaza de pena que el Estado asocia a la violación de los deberes consignados en las normas jurídicas, dictadas para garantizar la permanencia del orden social.<sup>135</sup>

---

<sup>134</sup> Ibidem. Págs. 257 y 258.

La punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal.<sup>136</sup>

Las penas que se le asocian a las hipótesis delictivas deben también respetar determinados principios tales como la existencia de un mínimo y máximo de las mismas, deben de ser con un propósito de readaptación, etc...

#### **- La punibilidad en el delito informático.**

Los delitos informáticos como se ha comentado a lo largo del presente trabajo son de reciente creación surgiendo ante la necesidad de proteger la confidencialidad de información protegida a través del sistema informático, o bien evitar su destrucción, por lo que los legisladores consideraron contemplar una pena de prisión mínima, y a la multa, las cuales consideró aumentarlas cuando el sujeto pasivo resultare ser el Estado y las instituciones pertenecientes al sistema financiero por los razonamiento vistos con antelación:

Así, a continuación se transcribirán nuevamente los artículos respectivos anotando con negrillas las sanciones correspondientes:

---

<sup>135</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 453.

<sup>136</sup> López Betancourt, Eduardo. Op. Cit. Pág. 263.

De acuerdo al Código Penal Federal:

## CAPÍTULO II

### Acceso ilícito a sistemas y equipos de informática

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

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

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

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

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

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

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

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

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

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

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

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

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

**De acuerdo al Código Penal para el Estado de Sinaloa la punibilidad es:**

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

I.- Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, o bienes o información; o

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

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

**- Las excusas absolutorias.**

Considerado como elemento negativo de la punibilidad, ésta surge por las políticas criminales que el legislador ha considerado para que no obstante el carácter delictivo de una conducta, ésta no sea castigada, la cual es imprescindible que exista en la ley.

Son causas de impunidad o excusas absolutorias, las que hacen que a un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena alguna, por razones de utilidad pública.<sup>137</sup>

Las excusas absolutorias son aquellas causas que dejando subsistente el carácter delictivo de la conducta, o hecho impiden la aplicación de la pena.<sup>138</sup>

Estas causas de excusas absolutorias se han basado en la Doctrina Penal en:

- a) Excusa en razón de la mínima temibilidad.
- b) Excusa en razón de la maternidad consciente.
- c) Excusa en razón a la no exigibilidad de otra conducta.

#### **- Las excusas absolutorias en el Delito Informático.**

Ni el legislador del Estado de Sinaloa ni el federal han considerado expresamente la existencia de alguna excusa absoluta para que no se aplique la pena a alguna persona que haya cometido el delito informático, sin embargo, atendiendo a las causas antes descritas en la doctrina sí pudiéramos hacer mención a la excusa absoluta en razón a la no exigibilidad de otra conducta, prevista en el artículo 400 del Código Penal Federal, cuando se realice un encubrimiento por parte de un pariente o

---

<sup>137</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 433.

<sup>138</sup> Castellanos Tena, Fernando. Op. Cit. Págs. 278 y 279.

allegado de alguien que cometió el delito informático, sin embargo, cabe recordar que no es que se exculpe al delito informático sino que se está dando una excusa absolutoria al delito de encubrimiento del propio artículo 400, y esto puede darse en todos los delitos, con las salvedades probatorias antes vistas.

### **3.4. Formas de aparición del delito.**

El delito una vez que se ha integrado puede tener diferentes formas de aparición ya sea en su esencia misma en la cual podrá ser concretado en el mundo real o bien quedarse en un intento, estando así en presencia del delito consumado o en la tentativa respectivamente, así como poder llevarse a cabo por diversos sujetos encontrándose en diferentes grados de autoría o participación.

#### **3.4.1. El *Iter criminis* ( la vida del delito).**

El hablar del *iter criminis* es precisamente conocer la trayectoria que puede darse en un delito desde el momento en que surge como una idea en la mente del sujeto activo hasta su realización en el mundo externo, acontece en los delitos dolosos.

El maestro Francisco Pavón Vasconcelos refiere que: “El *iter criminis* comprende el estudio de las diversas fases recorridas por el delito *desde su ideación hasta su agotamiento*. Tradicionalmente distingúense en el *iter criminis* (camino del delito). El delito se encuentra en su *fase interna* cuando aún no ha sido exteriorizado; no ha salido

de la mente del autor; en tal estado se colocan a la *ideación*, a la *deliberación* y a la *resolución* de delinquir”.<sup>139</sup>

El Dr. Raúl Carrancá y Trujillo señala que el *iter criminis*, “es el camino que recorre el delincuente para dar vida al delito, pueden advertirse dos fases: la interna o psíquica y la externa o física. En la vida del delito concurren una actividad mental y una muscular. A la primera pertenece la idea criminosa (motivo, deliberación y resolución); a la segunda, la manifestación de la idea (proposición, conspiración, inducción), la preparación, los actos ejecutivos (tentativa) y los de consumación”.<sup>140</sup>

Así, ese *iter criminis* en la doctrina se ha dividido en:

**1) Fase interna.** La cual aparece en la mente del sujeto activo la cual a su vez se divide en las siguientes fases:

- Ideación.
- Deliberación.
- Resolución

Por lo que hace a la ideación es cuando al sujeto activo le surge la idea de cometer un delito.

En la deliberación el sujeto activo discute mentalmente entre el cometer el delito o no.

---

<sup>139</sup> Pavón Vasconcelos, Francisco. Op. Cit. Pág. 467.

<sup>140</sup> Carrancá y Trujillo, Raúl. Op. Cit. Pág. 693.

En la resolución es cuando el sujeto activo decide mentalmente en cometer el delito ideado.

**2) Fase externa.-** Es cuando el sujeto exterioriza de alguna manera su idea criminosa. Y se divide también en tres etapas:

- Manifestación.
- Preparación.
- Ejecución.

En la manifestación encontramos cuando el sujeto concreta el delito por la simple exteriorización de la idea criminosa, es el clásico ejemplo del delito de amenazas. También encontramos aquí cuando se manifiesta comentando la realización del delito con lo que pudiera involucrar a otras personas, ubicándonos en temas de la autoría y participación, ya que de alguna forma al manifestar la comisión del delito se estaría involucrando a otro.

En la preparación tenemos actos lejanos a la consumación que van enfocados a condicionar de alguna manera el delito. Estos actos por sí solos no pudieran ser constitutivos de delito sino hasta que el ilícito ideado se ejecute (ya sea en grado de tentativa o en consumación); pero una vez concretado el delito los actos preparatorios pudieran tener la cualidad de agravar dicho delito.

Si tales actos son de naturaleza inocente, que igual pueden ser practicados por un individuo que tenga propósitos delictivos, que por aquél que vaya a cometer un acto ilícito (el que compra una escopeta puede ser para realizar un homicidio o para ir a una partida de caza), entonces son preparatorios, y si sólo pueden ser ejecutados por el que tenga ánimo de delinquir, son actos de ejecución. Es muy importante tenerlos en cuenta, pues por medio de ellos se puede averiguar si el delito fue premeditado.<sup>141</sup>

La ejecución es la concreción del delito, ya sea en grado de tentativa o en la consumación.

#### **- La Tentativa.**

Cuando la voluntad criminal se traduce en un caso externo que entra en la esfera de consumación del delito, sin llegar a llenarla, y va dirigido claramente a conseguir la objetividad jurídica del delito, pero sin llegar a lesionarla, el acto se llama ejecutivo y la figura a la que da lugar se denomina tentativa. Esta puede definirse sintéticamente como la ejecución incompleta de un delito.<sup>142</sup>

La tentativa esta constituida de los actos ejecutivos (todos o algunos), encaminados a la realización de un delito, si éste no se consuma por causas ajenas al querer del sujeto.<sup>143</sup>

---

<sup>141</sup> Jiménez de Asúa, Luis. **LA LEY Y EL DELITO**. Op. Cit. Pág. 471.

<sup>142</sup> *Ibidem*. Pág. 474.

<sup>143</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 287.

Aquí tiene que imperar que las causas por las que se interrumpa el delito sean externas al sujeto activo, ya que si estuviéramos en presencia de causas propias estaríamos en el tema del arrepentimiento.

#### **- La consumación.**

Consiste en la concreción o realización de todos los elementos ejecutivos del delito, obteniendo el resultado deseado.

Los delitos informáticos que se han venido analizando y atendiendo a su comisión dolosa pueden recorrer las fases del *iter criminis* desde el momento en que el activo puede gestar en su mente esa idea criminosa (ideación), deliberar entre ella o desistir (deliberación), decidiendo o resolviendo en realizarla (resolución), continuar con ella y posiblemente realizar preparar o acondicionar la comisión del delito (actos preparatorios) como por ejemplo: (comprar una computadora, sin embargo hasta ese momento no se sabrá si la compró para hacer una trabajo o un ilícito) y llevar a cabo actos ejecutivos, los cuales podrán ser interrumpidos por causas ajenas a la voluntad del activo (tentativa) o bien realizaría todos esos actos hasta obtener el resultado deseado de apoderarse ilícitamente de una información confidencial resguardada en medios informáticos o bien destruir éstos últimos (consumación).

### 3.4.2. Concurso de delitos y concurso aparente de normas.

El Dr. Eduardo López Betancourt resumiendo a diversos autores, destaca a Cuello Calón quien dice que: “Hay pluralidad de delitos en el llamado concurso de delitos, cuando el mismo agente ejecuta varios hechos delictuosos, de la misma manera o diversa índole. Se distinguen dos formas de concurso: el llamado concurso formal o ideal y el concurso real”.<sup>144</sup>

Encontramos la siguiente clasificación sobre el concurso de delitos:

- 1.- Concurso ideal o formal, y
- 2.- Concurso real o material.

En el concurso ideal o formal existe unidad de acción y pluralidad de lesiones jurídicas o delitos, es decir, aquí el agente con su conducta viola varios preceptos legales.

En el concurso ideal se advierte una doble o múltiple infracción; es decir, por medio de una sola acción u omisión del agente se llenan dos o más tipos legales y por lo mismo se producen diversas lesiones jurídicas, afectándose, consecuentemente, varios intereses tutelados por el Derecho.<sup>145</sup>

---

<sup>144</sup> López Betancourt. Eduardo. Op. Cit. Pág. 225.

<sup>145</sup> Castellanos Tena. Fernando. Op. Cit. Pág. 307 y 308.

El concurso real o material surge cuando existe una pluralidad de acciones y pluralidad de resultados, es decir, el agente ocasiona diversos delitos como resultado de varias conductas independientes.

Existe otra forma de concurso, que es el que se refiere al concurso aparente de normas y que el penalista Mario Alberto Torres López hace mención que se presenta en los casos en que existe un evento cuya totalidad o sus fracciones encajan en figuras delictivas o tipos previstos en dos o más leyes penales, respecto de lo cual se ha comprobado previamente que no existe ni Concurso Real ni Concurso Ideal. La aplicación de todas las leyes penales que concurren representaría la desarticulación de lo que con antelación se identificó como unidad delictiva, con el resultado de que uno o varios aspectos de ese evento valdría para fundamentar dos o más penas.<sup>146</sup> Situación que no se aprecia en los Delitos Informáticos.

El concurso ideal puede darse en los delitos informáticos analizados, ejemplo de ello sería cuando un activo con una sola acción de obtener o alterar ilícitamente una información contenida en los medios informáticos de un hospital dañando sus computadoras que mantenía vivo a un sujeto en estado de coma y éste muere.

El concurso real puede aparecer en los delitos informáticos materia de la presente investigación como en todos los ilícitos, tal sería el caso de que el activo en día determinado se robe un equipo informático, otro día cometa un delito informático

---

<sup>146</sup> Torres López, Mario Alberto. Op., Cit. Págs. 156 y 157.

apoderándose ilícitamente de una información contenida en medios informáticos y después venda esa información indebidamente.

Estaríamos aquí en presencia de múltiples actos de terrorismo informático.

En este apartado volvemos a encontrar los grandes problemas que se pueden generar a través del mal uso de los sistemas de cómputo de los cuales el hombre se ha convertido en más dependiente en la mayoría de sus actividades por lo que se demuestra aquí lo frágil que es ante los delitos informáticos.

### **3.4.3. Concurso de personas. (autoría y participación).**

Es la voluntaria cooperación de varios individuos en la realización de un delito, sin que el tipo requiera esa pluralidad.<sup>147</sup>

No confundir con la clasificación del tipo penal sobre el número de sujetos activos que requiere el legislador para llevarse a cabo el delito; es decir cuando de la lectura del tipo penal aparece la exigencia de que su comisión sea a través de varias personas (plurisubjetivo), o bien cuando solamente en el tipo penal se requiere la aparición de un sujeto activo (unisubjetivo). Aquí se refiere a que en los hechos cualquier delito pueda ser realizado por varias personas para lo cual entraríamos a los conceptos doctrinales de autoría y participación.

---

<sup>147</sup> Castellanos Tena, Fernando. Op. Cit.. Pág. 293.

El presente tema tiene su fundamento en el artículo 13, del Código Penal Federal, que reflejado en la doctrina encontramos la siguiente clasificación:

**A) Autor.**

**a) Autor material.**

**b) Autoría intelectual.**

**c) Autoría mediata.**

**B) Coautoría.**

**C) Complicidad.**

El encubrimiento es otra forma de que otros sujetos auxilien en un delito solamente que aquí la ayuda es posterior a la comisión del ilícito y los ayudantes no serán partícipes del delito cometido, sino que caerán en un delito autónomo denominado encubrimiento, y si el auxilio es anterior al delito, o posterior previa promesa anterior sí estaríamos en presencia de la autoría y participación que establece el artículo 13, del Código Penal Federal, o del artículo 18 del Código Penal para el Estado de Sinaloa.

También puede darse en los delitos informáticos la colaboración con otras personas posteriormente a la comisión del delito, por lo que tales personas serían responsables de otro ilícito autónomo como lo es el encubrimiento.

## **CAPÍTULO 4. LA DELINCUENCIA INFORMÁTICA Y SU REGULACION INTERNACIONAL; EN MÉXICO Y SUS TENDENCIAS.**

### **4.1. La delincuencia informática internacional.**

En el presente Capítulo se analizarán algunos temas de gran importancia a nivel internacional en torno a los Delitos Informáticos tales como los sujetos que intervienen, las diversas formas de comisión de estos ilícitos y sus medios, los delitos que son cometidos por los medios computacionales, el tratamiento que se le ha dado a esa problemática en el mundo, así como la importancia que cobra la Criminología y la Criminalística en los ilícitos materia de la ésta investigación.

#### **4.1.1. El delincuente informático.**

En este presente apartado se presentarán los sujetos que intervienen en los Delitos Informáticos e ilícitos cometidos por medios informáticos.

##### **- El “Hacker”**

El Hacker puede ser definido como un “Intruso o Pirata informático<sup>148</sup>”, que en muchas ocasiones 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

---

<sup>148</sup> Rodao, Jesús de Marcelo. **PIRATAS CIBERNÉTICOS. CYBERWARS, SEGURIDAD INFORMÁTICA E INTERNET**. Editorial- Ra-ma. España 2001. Pág. 23.

informática y las telecomunicaciones como: programación, software, hardware. No existe una definición exacta de Hacker debido que es un grupo muy amplio y variado de personas con un vasto conocimiento y características que pueden compartir sin ser únicas, de entre las cuales se puede encontrar:

- Su objetivo es adquirir conocimientos para ellos mismos de manera autodidacta.
- Son personas minuciosas con la tecnología, analizándola, descubriéndola hasta dominarla, modificarla y explotarla.
- Se consideran obsesivos y compulsivos por acumular conocimiento y tener lo mejor en la tecnología.
- Poseen un alto nivel de conocimiento informático.
- Con gran fuerza de voluntad y perseverancia en reintentar nuevas técnicas una y otra vez hasta tener éxito.
- Nunca divulgan los conocimientos obtenidos.
- No existe edad entre los Hackers.
- No tienen gustos en especial, no tienen una vestimenta específica y no siguen un estereotipo de película norteamericana.
- En muchos casos se consideran extrovertidos.
- Actúan de manera inadvertida muchas veces consideran a un buen Hacker cuando nunca son atrapados.
- Se preocupan por poner accesible otros conocimientos que generalmente son de interés público, que son publicados en sus propias páginas de Internet.

El Hacking es la acción realizada por los Hackers para introducirse en sistemas y redes privadas o públicas, con lo que se ha convertido en algo muy común con la extensión de la computadora personal y de la Internet alrededor de todo el mundo haciendo que una computadora con información vital conectada a Internet sea inseguro, debido a que no existe demasiada información sobre medidas de seguridad por parte del usuario y el poco nivel de conocimiento acerca de medidas de seguridad de los administradores de sitios y servidores, así como el amplio conocimiento de los Hackers para actuar.

El Hacker utiliza agujeros en la seguridad de los protocolos para poder acceder y navegar en Internet, estos protocolos son conocidos como TCP/IP o protocolo de control de transmisión, que se divide en TCP o control de transición, haciendo que se reciba la información transmitiendo la dirección a donde deberá ser enviada según la solicitud del usuario y de mantener el orden de la información y el IP o protocolo de Internet, este último es una forma de identificación de equipos utilizados para la navegación, similar a un número telefónico que permite enviar y recibir información debido a que al dividir en bloques la información almacena la dirección de IP tanto del remitente como del destinatario.

A su vez éstos protocolos se dividen en otros dos que son: el protocolo encargado de la transmisión de datos de equipo a equipo y el protocolo que controlan la administración que permite ver parte de la información mientras ésta se transmite, de los protocolos útiles para conectarse, transferir datos, visitar páginas Web y de interés para un Hacker resaltan: ARP que es el protocolo de resolución de direcciones que convierte

las direcciones de Internet en direcciones físicas descifrando las direcciones de IP de cada bloque de información y comprobar si ésta posee la dirección de IP del destinatario correcto según la petición hecha por el usuario evitando que llegue información no solicitada; ICMP o protocolo de mensaje de control de Internet encargado de monitorear el estado del mensaje, así como del estado de quien envía y recibe información; INETD este protocolo sirve para administrar los puertos en caso de que se necesiten realizar dos o más actividades al mismo tiempo y el HTTP utilizado para acceder a páginas Web, una vez siendo utilizados presentan espacios en la seguridad debido a errores en la programación de los programas legítimos, el mal uso de los protocolos o la navegación en Internet.

Otra forma que un Hacker pueda conocer estos protocolos es mediante los COOKIES, estos poseen una buena intención debido a que un usuario entra a una página y envía una solicitud para poder acceder a ella y ésta a su vez otorga o no autorización para el acceso y utiliza los Cookies para almacenar la información de los protocolos algo así como una tarjeta de datos para la transmisión de información de ambas partes con el fin de que en un futuro al ingresar de nuevo en la misma página no se tenga que hacer de nuevo todo el proceso de verificación y aceptación<sup>149</sup>. El problema radica que muchos Hackers crean páginas señuelos con interés para el usuario el cual utilizan la excusa de los Cookies para obtener esta información o incluso más información confidencial sin que el usuario pueda darse cuenta con el fin de encontrar víctimas para estudiar y encontrar brechas en la seguridad en los usuarios.

---

<sup>149</sup> Ibidem. Pág. 147.

Una vez obtenida esta información el Hacker ingresa a la computadora investigando el tipo de software al que se enfrenta y el equipo en el que se encuentra, una vez adentro del sistema y conocer el software el Hacker puede entrar como si ya fuera un usuario legítimo o robando las claves de acceso al momento de entrar e intenta obtener los privilegios de un administrador autorizado con el fin de tener acceso a toda la información disponible en el equipo, con el fin de evitar sospechas de existencia de intrusos en el sistema, los Hackers intentan permanecer poco tiempo en ellos al día con lo que un ataque puede llevarse a cabo durante días o sólo tocar los archivos de interés sin acceder un número determinado de archivos que levante sospechas, al terminar para no ser detectado conforme a su dirección de correo electrónico o dirección IP utiliza editores dentro del sistema infiltrado para borrar o cambiar su mismo correo o dirección de IP.

En muchas ocasiones, personas normales se consideran Hackers, pero para entrar a éste selecto grupo de elite informático o como los denomina Jesús de Marcelo Rodao “caballeros del bit”<sup>150</sup> es necesario un nivel mínimo de conocimientos, aunque sí cualquier persona puede actuar como ellos, de los cuales surgen una sub-especie de Hackers bajo las siguientes denominaciones:

**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

---

<sup>150</sup> Ibidem. Pág. 23.

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.

**Wrackers:** Son personas dedicadas a descargar programas nocivos como los 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 encuentran 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.

Al igual que los Hackers, existen diversos tipos de usuarios que sin ser Crackers son considerados de gran peligrosidad usando el nombre de Crakers y sus técnicas para lograr sus objetivos, entre los cuales están los siguientes:

### **Otros delincuentes informáticos.**

**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.

**Script-Kiddies:** 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.

**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.

**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.

De lo anterior se puede apreciar una gran variedad de personas que pueden obtener la calidad de sujetos activos en la comisión de un delito informático que a través de esos grandes conocimientos técnicos se pueden infiltrar en sistemas computacionales e incluso en alguna conducta de la cual el legislador debe estar conciente para proponer y crear legislaciones que vayan adelante de esos delincuentes.

#### 4.1.2. Conductas delictivas y nocivas en medios informáticos.

Durante la creación de la Informática surgieron incidentes inesperados que han cambiado para siempre el rumbo del mundo en esta ciencia, la seguridad y el uso de las computadoras que en muchos casos se utilizaron para bien y en otras se ocuparon para realizar ilícitos y ataques tanto a gobiernos como a particulares. A continuación se enlista algunos de estos hechos que cambiaron la forma de ver a la Informática, incidentes que demuestran el poder del mal uso de la misma.

Año	
70's	<ul style="list-style-type: none"> <li>El centro de investigación de <b>Xerox</b> en Palo Alto, Estados Unidos de América, fue creado <b>WORM</b> por John F. Scoch y John Up, con el fin de reducir el trabajo con una serie de equipos interconectados, con lo que este programa tenía la intención de administrar y supervisar cien equipos en red, inicialmente sólo fue instalado en 6 equipos, al día siguiente todos los equipos se encontraban infectados, con lo que el sistema fue reiniciado y reinstalada la red, pero al ser reencendidos el problema volvió a surgir y se estuvo en la necesidad de lo que sería el primer Anti-Virus del planeta. Se debe tener en claro que WORM no fue creado como un virus propiamente dicho sino que sólo fue un accidente de trabajo.</li> </ul>
1974	<ul style="list-style-type: none"> <li>Aparece <b>RABBIT</b>, creado para autoreplicarse en los sistemas, su funcionamiento era el de copiarse dentro de la lista de</li> </ul>

	instrucciones, pero éste se salió de control ocupando toda la memoria posible.
1976	<ul style="list-style-type: none"> <li>• Surge el término <b>CYBERWAR</b> por Andy Marshall, el cual definía a los ataques llevados a cabo por piratas informáticos tanto particulares como agencias del gobierno.</li> </ul>
80s	<ul style="list-style-type: none"> <li>• La NSA (Agencia Nacional de Seguridad) de los Estados Unidos de América pone en funcionamiento la red <b>ECHELON</b> para espiar llamadas telefónicas e interceptar mensajes codificados.</li> </ul>
1980	<ul style="list-style-type: none"> <li>• Aparece <b>REDUX</b> el cual podía autoreplicarse sin poderse borrar por todo la ARPA-Net, con lo que logró deshabilitar esta red por tres días.</li> </ul>
1981	<ul style="list-style-type: none"> <li>• Aparece <b>ELK CLONER</b> diseñado para las computadoras Apple II mediante disquetes podía copiarse asimismo dejando el poema:  <p style="text-align: center;">Elk Cloner  El programa con personalidad.  Se mete en sus discos.  Se infiltra en sus chips  Si, es un fabricante de clónicos  Se pegará a todo como pegamento.  Modificará la Ram también.  Distribuye al fabricante de clónicos.<sup>151</sup></p> Siendo este el primer programa que podía infectar a otros de manera involuntaria mediante disquetes</li> <li>• Surge el <b>ELECTRONIC HITCHNICKER.</b> o <b>APPLE WORM</b> creado por Jim Hauser y William R. Buckley en la Universidad Politécnica de California cuya función consistía en pegarse y viajar libremente en archivos sin causar daño alguno.</li> <li>• Se da la idea de ataque mediante virus informáticos propiamente dichos por Robert Cerruti y Marco Morocotti mediante el uso de disquetes como medio de infección afectando el sistema operativo con 16 repeticiones que reiniciaban el disco duro.</li> <li>• Se crea al “Chaos Computer Club” en Alemania por Hervert Wau Holland-Mortiz con el fin de hacer conciencia del peligro de los ataques por virus informáticos, seguridad informática y advertirá las empresas de sus fallos en seguridad.</li> </ul>
1983	<ul style="list-style-type: none"> <li>• Surge el término <b>COREWAR</b> en la conferencia dada por Kent Thompsons al ganar el premio A.M.Turning de la Association of Computing Machinery.</li> </ul>
1984	<ul style="list-style-type: none"> <li>• Fred Cohen considerado el padre de la teoría vírica fijó los planos para la base de los modernos virus al intentar crear</li> </ul>

<sup>151</sup> Ibidem. Pág. 7.

	<p>programas capaces de modificar otros programas para introducir copias de sí mismo.</p> <ul style="list-style-type: none"> <li>• Mayo- la revista Scientific American publicó un artículo de A.K.Dewdney describiendo a los <b>COREWARS</b> con gran difusión con el programa denominado "Guerra Nuclear".</li> </ul>
1985	<ul style="list-style-type: none"> <li>• Scientific American publicó los primeros testimonios de usuarios que experimentaron con los <b>COREWARS</b> demostrando el peligro de estos virus.</li> </ul>
1986	<ul style="list-style-type: none"> <li>• Ralf Burger basado en las teorías de Freed Cohen diseña a <b>VIRDEM</b>, el cual borraba los archivos de la computadora destruyéndolos después de grabar de sí mismo en los archivos.</li> </ul>
22 de Octubre de 1987	<ul style="list-style-type: none"> <li>• Se descubre la primer infección masiva en el mundo en la Universidad de Delawer en Newark Estados Unidos de América, infectando cientos de disquetes inutilizándole 1% de cada uno con el mensaje: "bienvenidos a la Mazmorra 1986 Basit &amp; Amjad (pvt) ltda. SERVICIOS INFORMATICOS BRAIN7730 NIZAB BLOCK ALAMA IQBAL TOWN LAHORE-PAKISTAN/TELEFONO 430791, 443248, 280530. cuidado con este virus...póngase en contacto con nosotros para obtener la vacuna...<sup>152</sup>"</li> </ul>
1987	<ul style="list-style-type: none"> <li>• Aparece el <b>VIENNA</b> con la innovación de un contador de cada cuatro infecciones sobrescribía el contenido de cualquier disquete con datos aleatorios, nuevas versiones de este virus destruían el contenido de los disquetes con diez infecciones.</li> <li>• En este mismo año surgen las computadoras personales permitiendo que todo mundo pudiera acceder a una PC desde su casa.</li> <li>• Nace el primer <b>CABALLO DE TROYA</b> con una inofensiva tarjeta electrónica de felicitación navideña, que al ser abierta podía observar un árbol de Navidad pero éste se autorreplicaba saturando las bandejas de entrada de los correos y ser enviado de manera autónoma a los correos almacenados de la víctima, dentro de 6 días miles de computadora fueron infectadas.</li> </ul>
1988	<ul style="list-style-type: none"> <li>• Drew Davidson diseñó un virus para las computadoras Macintosh, el cual su función era de poner en pantalla el planeta tierra con un mensaje de paz. Este virus fue repartido en un club de usuarios, y Marc Canter consultó sin querer su computadora al probar dicho programa, el cual salió de control infectando a más de cinco mil usuarios en el mundo.</li> <li>• En Abril de este mismo año surge el <b>SCORES</b>, este virus infectaba el sistema operativo ocultándose en archivos y tras</li> </ul>

<sup>152</sup> Ibidem. Pág. 9.

	<p>dos días iniciaba la infección en todo el sistema, este virus fue detectado en 24 computadoras en una filial de General Motors en Estados Unidos. Tras minuciosos estudios se descubrió que este virus fue creado por un empleado descontento en dicha compañía.</p> <ul style="list-style-type: none"> <li>• Aparece <b>BRAIN</b> en las oficinas de un periódico, pero este salió de control e infectó más de cuatro millones de computadoras de los Estados Unidos de América.</li> <li>• Tras los ataques de virus informáticos malintencionados y experimentos fallidos sale a la venta el <b>FLU SHOT</b> creado por Ross Greenberg y el <b>VIRUSCAN</b> por John McAfee que fueron los primeros antivirus comerciales a la venta.</li> <li>• Se da a conocer el primer ataque a las computadoras de la NASA mediante un virus tipo gusano, con un mensaje navideño.</li> <li>• Mayo de este mismo año aparece el <b>JERUSALEM o VIERNES 13</b>, infectando miles de computadoras incluyendo computadoras del ejército y de gobierno.</li> <li>• Aparece el <b>MICHELANGELO</b> infectando un mayor número que sus predecesores, provocando pánico mundial, incrementando las ventas de los antivirus comerciales.</li> </ul>
1990	<ul style="list-style-type: none"> <li>• Se dan los primeros rumores de CYBERWAR durante la guerra del Golfo, en la que los Estados Unidos de América introdujo una impresora infectada de un letal virus informático que al actuar inutilizaría las computadoras durante un ataque aéreo.</li> </ul>
1997	<ul style="list-style-type: none"> <li>• Comienza el primer ataque terrorista por Internet por el grupo Liberations Tigers, el cual no tuvo éxito pero dio conciencia de los posibles daños que podría causar.</li> <li>• El ejército Norteamericano dio a conocer que fueron cambiados los bases de datos de los tipos sanguíneos de los soldados. Se demuestra el gran poder de los Hackers para alterar y atacar contra redes norteamericanas.</li> </ul>
1998	<ul style="list-style-type: none"> <li>• Whale and Dolphin Conservation Society detecta intentos de ataque contra computadoras de la Marina de los Estados Unidos de América.</li> <li>• Mayo de este año el grupo lopht demuestra ante Senado norteamericano la vulnerabilidad de la Internet, y la facilidad para deshabilitarla en treinta minutos.</li> <li>• El Servicio Secreto Alemán denuncia un Hacker que intentaba robar secretos militares Iraníes.</li> <li>• Junio de este año el grupo Hacher Portugueses contra la tiranía de Indonesia PHAIT, borran el sitio web de promoción del gobierno Indonesio.</li> <li>• En Abril de este año en México aparece el grupo X-Ploit, mediante un mensaje de protesta a favor del cuerpo de</li> </ul>

	<p>bomberos, para demostrar su poder inutilizan la página de la CONAGUA, al parecer borrando el disco duro del servidor.<sup>153</sup></p> <ul style="list-style-type: none"> <li>• En Julio de este año el grupo X-Ploit de México da a conocer a los medios de comunicación que tenían por largo tiempo un programa oculto en la red del Senado de la República donde aseguraban haber obtenido correos electrónicos de los senadores<sup>154</sup>.</li> <li>• En Noviembre el grupo X-Ploit realiza un ataque contra la página del Municipio de San Pedro Garza García, Nuevo León, alterando su información.<sup>155</sup></li> </ul>
1999	<ul style="list-style-type: none"> <li>• El departamento de energía norteamericano es atacado en protesta del bombardeo a la embajada China en Yugoslavia durante el conflicto de Kosovo.</li> <li>• Nace el grupo 18 de junio, dedicado a realizar ataques informáticos a los organismos ingleses para pedir la condenación de la deuda externa a los países del tercer mundo.</li> <li>• En Agosto de este mismo año José Ramos-Horta amenaza con iniciar una guerra informática si Indonesia no acepta el resultado de referéndum en Timor Oriental.</li> <li>• Es atacada el red del FBI e inutilizada por una semana.</li> <li>• Inicia el juicio en contra el Israelí Ehud Tenebaum de tan sólo 20 años de edad, quien ingresó contra páginas del gobierno Israelí y del gobierno Norteamericano en el que destacan la NASA y el Pentágono.<sup>156</sup></li> <li>• En Julio el grupo Brasileño Resistencia 500 ataca la página del Tribunal Supremo, la Presidencia y el Tesoro en Brasil, siendo un ataque progresivo en dos días.<sup>157</sup></li> <li>• En Agosto el grupo Mexicano X-ploit realiza un ataque contra <a href="http://www.montiel.org.mx">www.montiel.org.mx</a>, protestando e incitando a agredir páginas gubernamentales y empresariales.<sup>158</sup></li> <li>• El mundo entra en pánico por el posible error informático del nuevo milenio.</li> </ul>
2000	<ul style="list-style-type: none"> <li>• El 9 de abril de este año fueron robados la información de más de 15,700 tarjetas de la base de datos de Western Union, días después del ataque esta empresa notificó a Visa y Master Card, así a los afectados.<sup>159</sup></li> </ul>

<sup>153</sup> <http://www.matuk.com/teclado/1998/abr-27-1998.html>

<sup>154</sup> Ibem

<sup>155</sup> <http://www.lared.com.ve/archivo/Hacker31.html>

<sup>156</sup> <http://www.cnn.com/TECH/computing/9803/19/Hackers/>

<sup>157</sup> <http://www.lared.com.ve/archivo/Hacker38.html>

<sup>158</sup> <http://www.lared.com.ve/archivo/Hacker39.html>

<sup>159</sup> <http://www.lared.com.ve/archivo/Hacker51.html>

2001	<ul style="list-style-type: none"> <li>• Aparece el gusano <b>ADORE WORM</b> para el sistema Linux, escaneando el sistema a través de Internet para analizar si existe información o programas vulnerables.<sup>160</sup></li> <li>• Raphael Gray un adolescente de 19 años es arrestado tras una extenuante investigación por parte del FBI por 10 cargos de descargas y acceso no autorizado de páginas gubernamentales, siendo arrestado también un año antes por un fraude de tres millones de dólares el cual admite a ver sustraído mas de 29,000 números de tarjetas de crédito. Saltando a la fama por a ver usado los números de la tarjeta de Bill Gates presidente de Microsoft para enviarle un cargamento del medicamento Viagra.<sup>161</sup></li> </ul>
------	---

Los anteriores casos son algunos que se han dado a conocer en el mundo, sin embargo, existen muchísimos más que no han salido a la luz pública por razones de confidencialidad y sobretodo para no hacer del conocimiento al público que son sistemas de seguridad informática que ha sido vulnerada o atacada que con esa publicidad generaría un daño aún mayor. Los Bancos han sido algunas de esas instituciones afectadas que se dieron a conocer, las múltiples ocasiones en las que se han infiltrados en su sistema, lo han negado por obvias razones de imagen financiera.

Estos sujetos activos del los delito Informático, al tener otros conocimientos privilegiados podremos incluirlos en un grupo especial como en el caso de los llamados “delitos de cuello blanco” que son aquellas personas que tienen acceso a instituciones financieras o gubernamentales y son personas que pueden manejar grandes inversiones. Son conocidos bajo esa terminología ya que son personajes de impecable presentación.

---

<sup>160</sup> <http://www.vsantivirus.com/adore.htm>

<sup>161</sup> <http://news.bbc.co.uk/1/hi/wales/1248136.stm>

### **-Conductas nocivas en Internet.**

La Internet como medio masivo de difusión de información ha presentado un sin número de beneficios en todos los campos de la vida humana en cualquier parte del mundo con el simple acceso a una computadora con Internet, en México según datos del Instituto Nacional de Estadística Geografía e Informática (INEGI), en 2001 tan sólo 11.7% de los hogares poseían una computadora y de entre los cuales solamente el 6.1% de los mismos contaban con una conexión a Internet, para el 2005 sólo el 18.4% de lo hogares tienen una computadora y de los cuales tan solo el 9% contaba con acceso a Internet<sup>162</sup>, aún sin contar el número de sitios de acceso a Internet públicos (Café Internet) o desde empresas y oficinas muchas personas se encuentran expuestas a contenidos que posiblemente no son considerados como ilícitos pero sí son nocivos y en muchas ocasiones dañinas para los usuarios, que van en contra de la moral y buenas costumbres, que sin la existencia de una regulación clara y efectiva se convertirá en un problema mayor con el creciente número de personas que tienen acceso a Internet en México y en el mundo, así como, en la cada vez menor edad en la que se requiere para aprender a navegar en Internet.

**- Atentados en Internet:** Con la extensión de las computadoras personales y la Internet alrededor del mundo, la existencia en los usuarios que interactúan entre sí es inmensa y la cantidad de usuarios continuará creciendo, pero por desgracia cantidad no significa calidad y muchos usuarios no son expertos en el uso de sistemas informáticos,

---

<sup>162</sup> ESTADÍSTICA SOBRE DISPONIBILIDAD Y USO DE TECNOLOGÍA DE INFORMACION Y COMUNICACIONES EN LOS HOGARES. INEGI. México 2005. Pág. 4.

con lo que ha llevado a un serio problema de seguridad, muchos usuarios actúan sin saber lo que se les espera.

En Internet las personas actúan de cierta manera que en sus vidas no lo harían normalmente, gracias al anonimato que otorga éste sistema, con lo que pueden iniciar ataques entre los usuarios, entre los más comunes encontramos los siguientes:

**Guerras en Internet:** Estas se llevan a un nivel que el usuario promedio no podría acceder, se da entre corporaciones, gobiernos y grupos de Hackers o Crackers en mayor escala donde los ataques, herramientas y conocimientos son más sofisticados para lograr el mayor daño posible<sup>163</sup>.

**Ataques de correos:** En muchas ocasiones los usuarios intercambian correos entre sí con información variada, pero en ocasiones ésta puede ser intervenida o borrada para no llegar a los destinatarios fijos, otro problema con los correos es el denominado “correo basura o Spam” el cual se dedica a invadir la bandeja de entrada de los usuarios sin que éste se desee, por lo regular de carácter comercial. Otro problema con el correo electrónico son las invasiones realizadas por usuarios mediante miles de correos a la vez mediante programas especializados que pueden saturar una bandeja de entrada.

**Ataques en el Chat:** Durante esta actividad popular en Internet muchos usuarios fingen ser otra persona, o siendo ellos mismos agreden verbalmente a otros usuarios pero sin darse cuenta que pueden agredir a Hackers o incluso Crackers que pueden

---

<sup>163</sup> Rodao, Jesús de Marcelo. Op. Cit. Pág. 162.

atacar a dicho usuario, e incluso en chats públicos se puede ser víctima de estos usuarios al aceptar archivos como las fotografías gracias a que se han ganado su confianza o incluso al almacenar los datos de usuario y estos al ser obtenidos se encuentran en un nivel de vulnerabilidad muy alto contraataques; incluso pueden contra atacar molestando a los usuarios llenando su computadora de archivos basura bloqueándolos por completo.

- **Robo de contraseñas:** Se considera un serio problema en el mundo de la Informática debido a que las cosas valiosas son guardadas bajo fuertes mecanismos de seguridad respaldado por contraseñas que las hacen accesibles a sus legítimos dueños, desde acceso a programas en computadoras personales y móviles, correos electrónicos, hasta cuentas bancarias, un Craker realiza ésta acción primero investigando cuál es el programa en el que se desea acceder, una vez encontrado el Craker busca una copia del programa para sí dentro de su equipo para poder trabajar con él, mediante programas especializados probará en él cientos de claves a la vez, si llega a encontrar reacción en una clave en especial la probará, si tiene éxito será usada en el programa legítimo para acceder a él tantas veces como sea posible, tomando el papel de administrador teniendo libre control de la información.

### **El virus Informático.**

La palabra VIRUS fue utilizada por primera vez por David Gerrolden en su novela "*When Haerlie Was One*", que en ella describía a una computadora que emulaba al

cerebro humano que para conectarse a otras computadoras utilizaba un programa llamado *VIRUS*<sup>164</sup>.

Durante mucho tiempo la palabra virus era usada al igual que en la Biología como con los ordenadores debido a muchas semejanzas entre los dos, que con la popularización de la Informática inició la controversia del uso de éste término, hasta que se generalizó el término V.I.R.U.S que significaba “Recurso de Información Vital Bajo Acoso” (*Vital Information Resources Under Siege*)<sup>165</sup>.

Los virus informáticos son diseñados según las necesidades del usuario y la intención que se posea; muchos de los virus atacan diferentes partes de un equipo informático como: el sector de arranque, procesadores de órdenes, archivos en especial, memoria libre, instrucciones de uso y recursos de Internet.

Son programas capaces de reproducirse a sí mismos, para atacar sin ser detectado con buenas y malas intenciones, aunque en la actualidad ya existen muchas excepciones, ampliándose a diversos virus y técnicas víricas que a continuación se enlista una pequeña porción de ellos:

**ARMOURING:** Son virus con mecanismos de seguridad para evitar ser detectados o crear dificultades para ser detectados y eliminados.

---

<sup>164</sup> Idem. Pág. 75.

<sup>165</sup> Idem.

**BACK DOOR:** Es un programa creado por el mismo intruso para introducir gusanos y troyanos creando una brecha en la seguridad oculta tras los programas legítimos o víctimas para poder ser usada tantas veces sea necesario.

**BOMBA DE TIEMPO:** Son programas altamente destructivos, creados para ser ejecutados en determinado tiempo o incluso a cierta hora del día, son capaces de destruir e inutilizar equipos, redes y servidores tanto física como lógicamente.

**BOMBAS LÓGICAS:** Similares a las bombas de tiempo pero para que estas entren en funcionamiento es necesario realizar determinada conducta, una palabra determinada o teclear cierta combinación de teclas, un nivel de espacio en el disco duro o ejecutar un programa en especial.

**BUG-WARE:** Son errores provocados por el mal uso de programas legales, los cuales generan ligeros problemas en el que el usuario considera que está infectado por un virus informático al detectar errores en el sistema, que incluso pueden extenderse a otros programas.

**CABALLO DE TROYA:** Es la práctica más común en Internet, consiste en un engaño en la que el Hacker crea un programa maligno escondido en programas que a simple vista parecerían inofensivos, por lo regular en archivos de fotografía o música, pero al ingresar en el equipo de la víctima realizan su función incluso sin que éste se diera cuenta sino hasta que es demasiado tarde, por lo regular se encuentran en sitios pornográficos o en programas gratuitos, que al descargar entran en los equipos enviando

de regreso información confidencial. Entre ellos se encontraban BACK ORIFICE, KILLWINDOWS, NETBUS y SUBSEVEN.

**CAMALEÓN:** Son los similares a los Troyanos, son programas malignos disfrazados como otros programas, que por lo general son enviados por correo electrónico.

**CANCELLING:** Técnica usada para eliminar información de una lista de correos o de noticias.

**COMADRONAS:** Programas encargados de enviar virus de manera automática a equipos informáticos, redes o correos electrónicos.

**COMPANION:** Son virus como troyanos que utilizan los tiempos de inicio de programas, para poder infiltrarse en la información y actuar, ya sea actuando antes de arrancar otro programa, durante la secuencia lógica, durante el uso o al cierre del sistema.

**CONEJOS o PESTES:** Son programas creados para autoreplicarse de manera rápida, capaces de llenar los discos duros y los últimos rincones de memoria, inutilizando redes y saturando bandejas de entrada de correos electrónicos con correo basura.

**GUSANOS:** Son programas que requieren de un alto nivel de conocimiento para ser creados, no son muy comunes por esta situación, éstos pueden autoreplicarse y

viajar entre los archivos e incluso entre redes, su funcionamiento requieren en muchos casos que la víctima inicie el gusano, por lo regular son inofensivos, son empleados en muchos casos para difundir mensajes, pero existen los malignos que su función es infiltrarse en redes, derrumbar y colapsar equipos con sus replicas. Entre los gusanos más famosos se encuentran: HYBRIS, I LOVE YOU, LITLEDVINI y SANTA.

**JOKE-PROGRAMS:** No son considerados propiamente como virus, ya que son unas bromas creadas por los programadores, Hacker y personas comunes, que pueden ser presentadas de tantas formas y sin aviso, son totalmente inofensivos para las víctimas, un ejemplo muy popular son los mensajes que anuncian la destrucción de equipos e información y errores graves en el sistema de los equipos, en muchas ocasiones estos ocultan Gusanos, Troyanos y Bombas.

**KILLER:** Son virus dedicados a destruir antivirus o vacunas especializadas, desde simplemente borrar el programa, inutilizarlo, borrar la lista de virus a atacar y proteger o eliminar por completo el antivirus, muchos casos son para futuros ataques de otro tipo de virus.

**LEAPFROG:** Es un programa usando a los gusanos para leer las listas de correo de las víctimas, enviándolo a los programadores.

**MÁSCARAS:** Éste requiere de un alto nivel de conocimiento técnico debido que con esta técnica el intruso engaña al sistema adoptando la personalidad de un usuario

autorizado aprovechando huecos o fallas en el sistema y protocolos de seguridad robando información o alterando el sistema.

**MACROVIRUS:** Son virus que atacan programas que poseen algún lenguaje de interpretación donde para realizar ciertas funciones, necesitan de instrucciones preprogramadas llamados macros, estos virus alteran estas instrucciones, como las de grabado, apertura e impresión de documentos en procesadores de textos.

**MOCKINBIRD:** Son virus inofensivos e inactivos, su función es esperar a que las víctimas ingresen sus claves y contraseñas para copiarlas y enviarlas, aprovecha huecos en la seguridad o en la entrada para actuar pero nunca hacen daño para no ser descubiertos.

**REBUNDANTE:** Son virus que cuando se encuentran con otros virus con los mismos objetivos no ataca, pero existen otros que al encontrar otro con las mismas intenciones decide atacar a otros sistemas como el de arranque, pero si uno borra alguno de ellos quedara otro que retomara sus objetivo, siendo de gran peligrosidad.

**SNIFFER:** Esta técnica es comúnmente utilizada para robar claves de acceso y otros datos de interés que generalmente no causan daño y pasan inadvertidas, pero otros según el intruso pueden ser destructivos.

**SPARE:** Son virus acompañados de bombas que son detonados con determinada secuencia lógica, capaces de permanecer en los sistemas por meses, pero mientras más permanezca en la computadora inactivo más fácil será detectarlo.

**SPAMMING:** Son programas muy comunes para propaganda comercial y política el cual envía de forma masiva correos a diferentes direcciones de correo electrónico.

**SPIDERNING:** Estos programas son diseñados para viajar por Internet buscando información de un tema determinado.

**STEALTH:** Es una técnica utilizada por los virus para ocultar todo rastro de operaciones, siendo virus inefectivos debido a que se arriesga a ser detectado por el antivirus al actuar en la memoria, estos funcionan copiando el programa a atacar y plasmando dicha copia ante el escaneo del antivirus para que éste pase como archivo seguro, mientras el virus ataca el verdadero programa.

**TUNNELING:** Es una técnica usada por los virus para evitar los antivirus aprovechándose al colocar falsos puntos para que sean detectados, el antivirus busca en puntos donde se supone debería estar el virus, el cual pasa por donde el antivirus considera seguro.

**POLIFORMISMO:** Estos tipos de virus intenta escapar de los antivirus mutando al momento de ser detectado logrando evitar al antivirus, llegaron a ser peligrosos debido a que podían existir miles de mutaciones de un solo virus.

**XPLOIT:** Son programas especializados en escanear programas comerciales aprovechando errores en la programación creando puertas traseras para ser usadas tantas veces como sean necesitadas.

**VARIANTE:** Es una técnica usada por el usuario para modificar virus antiguos en su estructura o en pequeños detalles para aparentar un nuevo virus y evitar así su detección.

Como nos hemos percatado existen innumerables técnicas dentro de la Informática para realizar conductas nocivas o antisociales, siendo la labor de la Criminalística conocerlas a efecto de encontrar el *modus operandi* del sujeto activo y poder así investigar un delito informático, llevar a cabo la detención del delincuente y realizar una adecuada procuración e impartición de la justicia.

### **Contenido nocivo en Internet.**

Con los inicios comerciales de la Internet y su expansión en todo el mundo éste se ha convertido en un monumental medio de información y en especial de comunicación, en el que cualquier persona puede publicar todo tipo de contenido, expresar sus ideas y relatar hechos acontecidos, pero no siempre existe veracidad y la calidad en su contenido que se publica ni en lo que se puede llegar a encontrar y leer, ya que otro de los problemas que presenta la Internet es el escaso control en la información que se presenta publicada, ni tampoco del responsable de quien lo hace gracias una vez mas al anonimato que ofrece este valioso medio, otro problema es el contenido nocivo que se

muestra de diversas formas, tanto imagen sonido y video, que sin ser delito atentan contra la privacidad, la paz pública y la moral.

Los contenidos nocivos en Internet dependen esencialmente de elementos subjetivos inherentes a cada persona, tanto de quien publica como de quien la observa y consulta, de los que entre destacan los siguientes: la nacionalidad, el género, la religión, las ideas políticas y la moral, entre otros. La mayoría de los casos se sienten amparados por la libertad de expresión de sus respectivos países, aprovechando el anonimato y la inexistencia de restricciones para publicar que ofrece la Internet,

- Alcoholismo.
- Drogadicción.
- Tabaquismo.
- Sexo.
- Homicidio.
- Violencia Gráfica.
- Desordenes alimenticios.
- Satanismo y culto a la muerte.
- Religión y opiniones de todas las religiones del mundo.
- Suicidio y desencibilización a la muerte.
- Chismes y espectáculos.
- Noticias nacionales e internacionales.

Entre otros temas, pueden ser encontrados desde diferentes puntos de vista y abordados de maneras diversas que dependiendo de la persona puede considerarlo o no contenido nocivo, en México tenemos la Ley Sobre Delitos de Imprenta, en la que en sus artículos 1, 2, 3 hace referencia que son ataques contra la vida privada, contra la moral y el orden o la paz pública respectivamente.

**Artículo 1.- Constituyen ataques a la vida privada:**

**I.- Toda manifestación o expresión maliciosa hecha** verbalmente o por señales en presencia de una o mas personas, o por medio de manuscrito, o de la imprenta, del dibujo, litografía, fotografía o de cualquier otra manera que expuesta o circulando en publico, o transmitida por correo, telégrafo, teléfono, radiotelegrafía o por mensajes, o de cualquier otro modo, **exponga a una persona al odio, desprecio o ridículo, o pueda causarle demérito o en su reputación o en sus intereses;**

**II.- Toda manifestación o expresión maliciosa hecha** en los términos y por cualquiera de los medios indicados en la fracción anterior, **contra la memoria de un difunto con el propósito o intención de lastimar el honor o la publica estimación de los herederos o descendientes de aquel, que aún vivieren;**

**III.- Todo informe, reportazgo (sic) o relación de las audiencias de los jurados o tribunales,** en asuntos civiles o penales, **cuando refieran hechos falsos o se alteren los verdaderos con el propósito de causar daño a alguna persona, o se hagan, con el mismo objeto, apreciaciones que no estén ameritadas racionalmente por los hechos, siendo estos verdaderos;**

**IV.- Cuando con una publicación prohibida expresamente por la ley, se compromete la dignidad o estimación de una persona, exponiéndola al odio, desprecio o ridículo, o a sufrir daños o en su reputación o en sus intereses, ya sean personales o pecuniarios.**

**Artículo 2.- Constituye un ataque a la moral:**

**I.- Toda manifestación** de palabra, por escrito, o por cualquier otro de los medios de que habla la fracción I del articulo anterior, **con la que se defiendan o disculpen, aconsejen o propaguen públicamente los vicios, faltas o delitos, o se haga la apología de ellos o de sus autores;**

**II.- Toda manifestación verificada** con discursos, gritos, cantos, exhibiciones o representaciones o **por cualquier otro medio de los enumerados en la fracción i del artículo 2** con la cual **se ultraje u ofenda públicamente al pudor, a la decencia o a las buenas costumbres o se excite a la prostitución o a la practica de actos licenciosos o impúdicos, teniéndose como tales todos aquellos que, en el concepto publico, estén calificados de contrarios al pudor;**

**III.- Toda distribución, venta o exposición al público, de cualquiera manera que se haga, de escritos, folletos, impresos, canciones, grabados, libros, imágenes, anuncios, tarjetas u otros papeles o figuras, pinturas, dibujos o litografiados de carácter obsceno o que representen actos lúbricos.**

**Artículo 3.- Constituye un ataque al orden o a la paz pública:**

**I.- Toda manifestación o exposición maliciosa hecha públicamente** por medio de discursos, gritos, cantos, amenazas, manuscritos, o de la imprenta, dibujo, litografía, fotografía, cinematógrafo, grabado o **de cualquier otra manera, que tenga por objeto desprestigiar, ridiculizar o destruir las instituciones fundamentales del país;** o con los que se **injuria a la nación mexicana, o a las entidades políticas** que la forman;

**II.- Toda manifestación o expresión hecha públicamente** por cualquiera de los medios de que habla la fracción anterior, con la que se **aconseje, excite o provoque directa o indirectamente al ejército a la desobediencia, a la rebelión, a la dispersión de sus miembros, o a la falta de otro u otros de sus deberes; se aconseje, provoque o excite directamente al público en general, a la anarquía, al motín, sedición o rebelión, o a la desobediencia de las leyes o de los mandatos legítimos de la autoridad; se injurie a las autoridades del país con el objeto de atraer sobre ellas el odio, desprecio o ridículo; o con el mismo objeto se ataque a los cuerpos públicos colegiados, al ejército o guardia nacional o a los miembros de aquellos** y esta, con motivo de sus funciones; **se injurie a las naciones amigas, a los soberanos o jefes de ellas o a sus legítimos representantes en el país; o se aconseje, excite o provoque a la comisión de un delito determinado;**

**III.- la publicación o propagación de noticias falsas o adulteradas** sobre acontecimientos de actualidad, **capaces de perturbar la paz o la tranquilidad de la república o en alguna parte de ella,** o de causar **el alza o baja de los precios de las mercancías o de lastimar el crédito de la nación o de algún estado o municipio, o de los bancos legalmente constituidos;**

**IV.- Toda publicación prohibida por la ley o por la autoridad, por causa de interés público, o hecha antes de que la ley permita darla a conocer al público.**

**Artículo 9.-** Queda prohibido:

**I.-** Publicar los escritos o actas de acusación en un proceso criminal antes de que se de cuenta con aquellos o estas en audiencia pública;

**II.-** Publicar en cualquier tiempo sin consentimiento de todos los interesados, los escritos, actas de acusación y demás piezas de los procesos que se sigan por los delitos de adulterio, atentados al pudor, estupro, violación y ataques a la vida privada;

**III.-** Publicar sin consentimiento de todos los interesados las demandas, contestaciones y demás piezas de autos en los juicios de divorcio, reclamación de paternidad, maternidad o nulidad de matrimonio, o diligencia de reconocimiento de hijos y en los juicios que en esta materia puedan suscitarse;

**IV.-** Publicar lo que pase en diligencias o actos que deban ser secretos por mandato de la ley o por disposición judicial;

**V.-** Iniciar o levantar públicamente suscripciones o ayudas pecuniarias para pagar las multas que se impongan por infracciones penales;

VI.- Publicar los nombres de las personas que formen un jurado, el sentido en que aquellas hayan dado su voto y las discusiones privadas que tuvieren para formular su veredicto;

VII.- Publicar los nombres de los soldados o gendarmes que intervengan en las ejecuciones capitales;

VIII.- Publicar los nombres de los jefes u oficiales del ejercito o de la armada y cuerpos auxiliares de policía rural, a quienes se encomiende una comisión secreta del servicio;

IX.- Publicar los nombres de las victimas de atentados al pudor, estupro o violación;

X.- Censurar a un miembro de un jurado popular por su voto en el ejercicio de sus funciones;

XI.- Publicar planos, informes o documentos secretos de la secretaria de guerra y los acuerdos de esta relativos a movilización de tropas, envíos de pertrechos de guerra y demás operaciones militares, así como los documentos, acuerdos o instrucciones de la secretaria de estado, entre tanto no se publiquen en el periódico oficial de la federación o en boletines especiales de las mismas secretarías;

XII.- Publicar las palabras o expresiones injuriosas u ofensivas que se viertan en los juzgados o tribunales, o en las sesiones de los cuerpos públicos colegiados.

**Artículo 10.-** La infracción de cualquiera de las prohibiciones que contiene el artículo anterior, se castigara con multa de cincuenta a quinientos pesos y arresto que no bajara de un mes ni excederá de once.

**Artículo 31.-** los ataques a la vida privada se castigaran:

I.- Con arresto de ocho días a seis meses y multa de cinco a cincuenta pesos, cuando el ataque o injuria no este comprendido en la fracción siguiente;

II.- Con la pena de seis meses de arresto a dos años de prisión y multa de cien a mil pesos, cuando el ataque o injuria sea de los que causen afrenta ante la opinión publica o consista en una imputación o en apreciaciones que puedan perjudicar considerablemente la honra, la fama, o el crédito del injuriado, o comprometer de una manera grave la vida, la libertad o los derechos o intereses de este, o exponerlo al odio o al desprecio publico.

**Artículo 32.-** Los ataques a la moral se castigaran:

I.- Con arresto de uno a once meses y multa de cien a mil pesos en los casos de la fracción I del artículo 2;

II.- Con arresto de ocho días a seis meses y multa de veinte a quinientos pesos, en los casos de las fracciones II y III del mismo artículo.

**Artículo 33.-** Los ataques al orden o a la paz pública se castigaran:

I.- Con arresto que no bajará de un mes o prisión que no excederá de un año, en los casos de la fracción I del artículo 3;

II.- En los casos de provocación a la comisión de un delito si la ejecución de este siguiere inmediatamente a dicha provocación, se castigara con la pena que la ley señala para el delito cometido, considerando la publicidad como circunstancia agravante de cuarta clase.

De lo contrario, la pena no bajara de la quinta parte ni excederá de la mitad de la que correspondería si el delito se hubiese consumado;

III.- Con una pena que no bajará de tres meses de arresto, ni excederá de dos años de prisión, en los casos de injurias contra el congreso de la unión o alguna de las cámaras, contra la suprema corte de justicia de la nación, contra el ejercito, la armada o guardia nacional, o las instituciones que de aquel y estas dependan;

IV.- Con la pena de seis meses de arresto un año y medio de prisión y multa de cien a mil pesos, cuando se trate de injurias al presidente de la republica en el acto de ejercer sus funciones o con motivo de ellas;

V.- Con la pena de tres meses de arresto a un año de prisión y multa de cincuenta a quinientos pesos, las injurias a los secretarios del despacho, al Procurador General de la Republica o a los directores de los departamentos federales, a los gobernadores del distrito federal y territorios federales, en el acto de ejercer sus funciones o con motivo de ellas, o a los tribunales, legislaturas y gobernadores de los estados, a estos con motivo de sus funciones;

VI.- Con arresto de uno a seis meses y multa de cincuenta a trescientos pesos, las injurias a un magistrado de la suprema corte, a un magistrado de circuito o del distrito federal o de los estados, juez de distrito o del orden común ya sea del Distrito Federal, de los territorios o de los estados, a un individuo del poder legislativo federal o de los estados, o a un general o coronel, en el acto de ejercer sus funciones o con motivo de ellas, o contra cualquier otro cuerpo publico colegiado distinto de los mencionados en las fracciones anteriores, ya sean de la federación o de los estados. Si la injuria se verificare en una sesión del congreso o en una audiencia de un tribunal, o se hiciere a los generales o coroneles en una parada militar o estando al frente de sus fuerzas, la pena será de dos meses de arresto a dos años de prisión y multa de doscientos a dos mil pesos;

VII.- Con arresto de quince días a tres meses y multa de veinticinco a doscientos pesos, al que injurie al que mande la fuerza publica, a uno de sus agentes o de a la autoridad, o a cualquiera otra persona que tenga carácter publico y no sea de las mencionadas en las cuatro fracciones anteriores, en el acto de ejercer sus funciones o con motivo de ellas;

VIII.- Con la pena de uno a once meses de arresto y multa de cincuenta a quinientos pesos, en los casos de injurias a las naciones amigas a los jefes de ellas, o a sus representantes acreditados en el país;

IX.- Con una pena de dos meses de arresto a dos años de prisión, en los casos de la fracción III del artículo 3.

**Artículo 36.-** Esta ley será obligatoria en el Distrito Federal y Territorios, en lo que concierne a los delitos del orden común previstos en ella, y en toda la republica por lo que toca a los delitos de la competencia de los tribunales federales.

## **Los mundos virtuales.**

La realidad virtual, ya siendo no un tema muy reciente pero muy llamativo, es la simulación de una realidad aparente por medio de máquinas y ordenadores, de las cuales se pueden presentar de dos formas, la inmersiva y la no inmersiva, en la primera la realidad virtual se presenta la interacción de la persona por medio de casco y guantes de los cuales lo colocan en apariencia en un mundo ficticio, el segundo tipo se presenta de manera más común, que mediante un monitor la personas interactúa con su computadora personal en estos mundos virtuales<sup>166</sup>.

Una realidad virtual donde toda una comunidad pueda habitar de manera casi real puede considerarse en muchos casos como un tema inimaginable, que sólo vive en las películas y libros de ciencia ficción que posiblemente no se pueda acceder en la actualidad de una manera que como se representaría una vida dentro de un sistema con una realidad falsa que sólo existe más que en las computadoras, y que en los mejor casos sería regular una economía y un estilo de vida social ordenada en el futuro cuando ésta se presente y sobrepase la incertidumbre jurídica.

La Internet, aunque tenga desventajas y defectos, ha llevado más beneficios a la vida humana, que muchos inventos del siglo pasado, desde la comunicación e información hasta el comercio y el entretenimiento, y bajo este último rubro ha surgido una novedosa forma de presentar el entretenimiento virtual y una forma especial de

---

<sup>166</sup> Wikipedia Enciclopedia Libre, Realidad Virtual. [http://es.wikipedia.org/wiki/Realidad\\_virtual](http://es.wikipedia.org/wiki/Realidad_virtual)

realidad virtual que se aparta de los videojuegos clásicos y es accesible a un gran número de personas alrededor del mundo, conocidos como Mundos Virtuales en Internet y juegos de rol multijugadores masivos en línea de sus siglas en inglés MMORPG (Masive Multiplayer Online Rol-Playing Game).

Los MMORPG son más apegados a los juegos de videos tradicionales, con la diferencia que el usuario o jugador en cualquier parte del mundo es llevado a servidores, donde se les presenta un amplio mundo virtual de gran detalle, dedicación y belleza; que como su nombre lo dice toman el rol de un personaje que puede ser creado por ellos mismos, personalizado y equipado a su voluntad que no tienden a seguir el rigor de un video juego tradicional no en línea, en estos juegos son acompañados de historias a seguir para poderse adentrar a diversos aspectos del mundo que se les presenta acompañados con miles de jugadores con los mismos objetivos que interactúan y cooperan entre sí hacen que este tipo de realidad virtual sea una grata experiencia, seguido de esto se presentan hechos sociales y económicos similares a nuestra realidad, que en algunas ocasiones no siempre son buenos y presentan problemas, ya que para poder participar dentro del juego se requiere de un cuota fija pero en otros se requiere de inversión para poder participar dentro de sus economías virtuales haciendo que el mismo dinero y objetos virtuales posean un costo muy real siendo susceptibles de apoderación ilícita.

Los MMORPGs se encuentran regulados y protegidos por las mismas empresas que pusieron en uso el sistema, quienes controlan las conductas de los usuarios, regulando sus economías y en otros casos prohibiendo transacciones de dinero virtual

por dinero real; posiblemente este ejemplo se presenta a menor escala con bajos costo de inversión por usuario, pero este tipo de juegos por servidor se encuentran miles de personas participando a la vez y que por cada MMORPG o cuentan con un sólo servidor, sino con docenas de ellos haciendo que el número de usuarios se incremente y por ende las inversiones y gastos en sus economías virtuales sea mucho mayor. dentro de este tipo de juegos de rol en línea se presentan entre otros EverQuest (Sony Computer Entertainment),<sup>167</sup> Final Fantasy XI Square-Enix)<sup>168</sup>, World of War Craft (Blizzard Entertainment)<sup>169</sup> y Star Wars Galaxies (Lucas Arts)<sup>170</sup>, dentro de los más populares con miles de jugadores en todo el mundo.

El segundo tipo, los Mundos Virtuales, similares a los MMORPGs pero alejados de la fantasía e imaginación que un videojuego podría representar, son realidades virtuales muy similares a la nuestra, del cual se tiene a Second Life(Linden Lab)<sup>171</sup> o Segunda Vida como el más popular de este género alrededor del mundo, que no posee un costo para participar y en las que se puede comunicar, jugar, interactuar y hacer negocios con otras personas en otras partes del mundo, incluso ir a tiendas virtuales con mercancía virtual que se presenta en la realidad, ir a centros nocturnos, parques y lugares públicos, poseer propiedades virtuales como casas, departamentos hasta islas privadas, lo que requiere de costo en moneda del juego que a su vez requiere de un costo en dinero real, la moneda en este mundo se conocida como Linden Dollars (L\$), que por cada Dólar Americano (US\$) equivale a 250 L\$, en este tipo de realidad virtual la inversión y gasto

---

<sup>167</sup> EverQuest Official Site. <http://everquest.station.sony.com/>

<sup>168</sup> Final Fantasy XI US Official Site <http://playonline.com/>

<sup>169</sup> World of War Craft Official Site <http://www.wow-esp.com/>

<sup>170</sup> Star Wars Galaxies Online Oficial Site <http://www.starwarsgalaxiesonline.com/>

<sup>171</sup> Second Life Official Site. [http://secondlife.com/whatis/economy\\_stats.php](http://secondlife.com/whatis/economy_stats.php).

es mucho mayor a la que serían los MMORPGs ya que por ejemplo: la renta de una isla privada puede llegar desde los 250.00 mensuales<sup>172</sup> hasta los 700.00 dólares americanos con una renta anual de 5 mil dólares y en aumento gracias al incremento de la popularidad de este juego<sup>173</sup>.

En second life, es de gran popularidad en todo el mundo, donde empresas transnacionales como Nissan, Starwood, Sony, BMG, Wells Fargo Bank, Coca Cola, Reebok, Dell, General Motors, Intel y Microsoft, han entrado a esta realidad virtual participando en la venta y distribución de sus productos tanto reales como virtuales, personajes políticos y de espectáculos han creados sus propios personajes a su imagen para publicitarse, incluso presentar conciertos exclusivos en este mundo, haciendo una monumental economía de millones de dólares en juego al rededor del planeta<sup>174</sup>.

México es el primer país latinoamericano en entrar a esta realidad virtual, en donde los usuarios han creado una gran comunidad representando el Paseo de la Reforma, el Ángel de la Independencia, el palacio de las Bellas Artes y la Diana Cazadora, construyendo restaurantes, bares y hoteles para extranjeros que deseen visitar virtualmente nuestro país, manteniendo una economía en compra-venta de objetos y servicios.

---

<sup>172</sup> Wikipedia Enciclopedia Libre, Second Life. [http://es.wikipedia.org/wiki/Second\\_life](http://es.wikipedia.org/wiki/Second_life)

<sup>173</sup> México SL, Comunidad Mexicana de Second Life. [http://www.hosteltur.com/noticias/43683\\_mexico-second-life.html](http://www.hosteltur.com/noticias/43683_mexico-second-life.html) .

<sup>174</sup> Second Life Official Site. [http://secondlife.com/whatis/economy\\_stats.php](http://secondlife.com/whatis/economy_stats.php).

Al igual que los MMORPGs los Mundos Virtuales están regulados por los creadores del sistema el cual pone las reglas de conductas y la forma en que la economía se maneja, incluso con la existencia de empresas y despachos virtuales encargada de la asesoría y regulación privada de compra y venta de productos y servicios, pero se tiene que recordar que en unos inicios la Internet comenzó a diminuta escala, como una moda, con pequeñas cantidades invertidas de manera privada para pocos usuarios, y como materia de burla para los juristas para preocuparse a regularla, pero que al paso de los años, con la popularización que generó con su uso y sin una regulación jurídica adecuada y oportuna puede llegar a tener grandes conflictos a futuro que llegaran a ser de difícil solución, ya que este tipo de vidas virtuales han demostrado el manejo de grandes capitales en objetos y servicios, así como, el gran número de usuarios participantes entre sí alrededor del mundo, que seguirá creciendo.

### **Conductas delictivas**

**Fraudes en Internet:** Con los inicios comerciales de la Internet muchas empresas han visto una oportunidad de éxito, mejorando sus ventas y crecimiento a proporciones inimaginables que sin la Internet hubiera sido difícil de lograr, creando que éste sea un mercado mundial de bienes y servicios accesibles al consumidor, pero este mundo también trae una gran desventaja debido a que muchas empresas con representantes mal intencionados o incluso usuarios aprovechen esta pequeña confianza de la Internet en el ámbito comercial para cometer fraudes, los más usados en este sistema me encontré con las siguientes características:

- **Fraudes cometidos en compra-venta y subastas por Internet:**

Consiste en muchos casos en recibir productos de menor calidad o señalamientos que no fueron expresados al momento de la transacción.

- **Engaños cometidos por empresas proveedoras del servicio de**

**Internet:** En muchas ocasiones las empresas limitan el uso de la Internet o alteran las velocidades del mismo para pagar más o igual precio al que lo hacían en otras velocidades de descarga sin previo aviso al cliente o limitan las posibilidades de uso al cliente para que éste busque el soporte del proveedor y la misma empresa pueda cobrar más.

- **Fraudes en Servicios de Internet:**

Muchas empresas ofrecen servicios en Internet que siempre son exclusivos a través de este medio, ya sea el uso exclusivo de programas en red, consulta de información y base de datos o el diseño de páginas Web, compra de productos, alquiler de servicios turísticos, médicos o laborales, pero en ocasiones al contratar estos servicios, se puede agregar o incluso disminuir la calidad y cantidad en el mismo, servicios que no fueron solicitados pero sí son reflejados en el costo, pueden presentarse cargos extras causado por el robo de números de tarjetas de crédito al proporcionarlos al adquirir estos usos, e incluso se puede entrar en un serio riesgo al proporcionar datos personales. Otro caso puede presentarse cuando algunas páginas ofrecen determinado servicio a cambio del número de tarjetas prepagadas para Internet o telefonía móvil como medio de pago.

- **Fraudes en las oportunidades de negocios:** Existen usuarios que crean empresas fantasmas que únicamente existen en Internet y ofrecen oportunidades fáciles de ganar dinero con negocios aparentemente sin pérdidas, constituyéndose en esquemas de inversión exitosos.
- **Fraudes telefónicos:** En muchas páginas de Internet de gran interés gratuito es necesario que se descarguen programas que supuestamente se conectan mediante el “modem” con la línea telefónica a una red privada pero sin darse cuenta el usuario le da oportunidad de que mediante su línea telefónica realicen llamadas de larga distancia o servicios telefónicos a cargo en la cuenta telefónica.
- **Engaño por páginas falsas de Internet:** Últimamente con el conocimiento de los usuarios para crear páginas de Internet se ha presentado el engaño para los usuarios presentándole páginas comerciales falsas aprovechándose de la ignorancia de los clientes y el rápido cambio que presenta la Internet, logrando que los usuarios depositen números de cuentas bancarias, números de tarjetas de crédito e incluso datos personales.
- **Casinos virtuales:** Con el amplio mundo de los videojuegos en Internet existen muchas páginas dedicadas a la estafa de usuarios mediante los casinos virtuales que usando tarjetas de crédito para apostar en un mundo donde

el programador tiene las reglas de modificar cada aspecto a su favor para siempre ganar, éstas páginas por lo regular dejan ganar por poco tiempo a los usuarios para ganar su confianza o incitarlos a apostar grandes cantidades y hacerlos perder, e incluso se encuentra en el peligro del robo de números de tarjetas de crédito.

### **Pornografía infantil.**

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 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:

**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, **transmision de archivos de datos en red publica 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 artículo 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.<sup>175</sup>

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.

---

<sup>175</sup> 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>

En México el Turismo Sexual se puede encontrar tipificado en Artículo 203 del Código Penal Federal, el cual menciona:

**TÍTULO OCTAVO. DELITOS CONTRA EL LIBRE DESARROLLO DE LA  
PERSONALIDAD.**

**CAPÍTULO III 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.**

**Artículo 203.** Comete el delito de turismo sexual quien **promueva, publicite, invite, facilite o gestione** por cualquier medio a que una o mas 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.

**Corrupción de menores.**

Uno de los grandes problemas a superar en la Internet alrededor del mundo es poder limitar el flujo de información lo cual es virtualmente imposible para cualquier gobierno, debido que en cualquier parte del mundo cualquier persona con una computadora, y acceso a Internet puede realizar cualquier publicación amparado en muchas ocasiones por la libertad de expresión de sus respectivos países, por lo cual ésta información llega a personas incorrectas o no preparadas a los contenidos que aparecen en la Internet.

En México se puede encontrar el delito de corrupción de menores e incapaces en los artículos 200 y 201 del Código Penal Federal los cuales dicen:

**Artículo 200.** Al que comercie, distribuya, **exponga, haga circular** u oferte, **a menores de dieciocho años de edad**, libros, **escritos, grabaciones, filmes, fotografías**, anuncios impresos, **imágenes u objetos, de carácter pornográfico, reales o simulados**, sea de manera física, **o a través de cualquier medio**, se le impondrá de seis meses a cinco años de prisión y de trescientos a quinientos días multa.

No se entenderá como material pornográfico o nocivo, aquel que signifique o tenga como fin la divulgación científica, artística o técnica, o en su caso, la educación sexual, educación sobre la función reproductiva, la prevención de enfermedades de transmisión sexual y el embarazo de adolescentes, siempre que estén aprobados por la autoridad competente.

**Artículo 201.** Comete el delito de corrupción, quien **obligue, induzca, facilite o procure a una o varias personas menores de 18 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 a realizar cualquiera de los siguientes actos:**

A) **Consumo habitual de bebidas alcohólicas;**

B) **Consumo de sustancias tóxicas o al consumo de alguno de los narcóticos** a que se refiere el párrafo primero del artículo 193 de este código o a la **fármaco dependencia;**

C) **Mendicidad con fines de explotación;**

D) **Comisión de algún delito;**

E) **Formar parte de una asociación delictuosa; y**

F) **Realizar actos de exhibicionismo corporal o sexuales simulados o no, con fin lascivo o sexual.**

A quien cometa este delito se le impondrá: en el caso del inciso a) o b) pena de prisión de cinco a diez años y multa de quinientos a mil días; en el caso del inciso c) pena de prisión de cuatro a nueve años y de cuatrocientos a novecientos días multa; en el caso del inciso d) se estará a lo dispuesto en el artículo 52, del CAPÍTULO I, del TÍTULO tercero, del presente código; en el caso del inciso e) o f) pena de prisión de siete a doce años y multa de ochocientos a dos mil quinientos días.

Cuando se trate de mendicidad por situación de pobreza o abandono, deberá ser atendida por la asistencia social.

No se entenderá por corrupción, 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; las fotografías, video grabaciones, audio grabaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares.

En caso de duda, el juez solicitará dictámenes de peritos para evaluar la conducta en cuestión.

Cuando no sea posible determinar con precisión la edad de la persona o personas ofendidas, el juez solicitará los dictámenes periciales que correspondan.

La Internet se ha convertido en un amplio foro de ideas y opiniones alrededor del mundo, así como una enorme biblioteca de información que siempre se encuentra accesible a cualquier hora, siempre que se tenga un acceso a Internet en cualquier parte del mundo, pero por desgracia en muchas ocasiones la información no puede ser verdadera en el mejor de los casos pero en otros el contenido puede ser negativo, gracias a la facilidad que ofrece el uso de una computadora, la cada vez menor edad en el uso y el navegar por Internet para los menores e incapaces por lo que los coloca en un nivel de vulnerabilidad a contenido no apto para ellos poniendo en riesgo su desarrollo emocional psicológico y educativo.

Los menores de edad e incapaces se encuentran desprotegidos de tres tipos de ataques, el primero consiste mediante sitios de conversación o chats públicos en los cuales a falta de administradores responsables permiten que menores y personas con malas intenciones interactúen entre sí, intercambiando ideas y material nocivo, en la actualidad muchos servidores responsables mantiene separada las sala de chats por áreas de edad y se encuentran bajo la supervisión de administradores o incluso hackers experimentados contratados para salvaguardar a los menores, contraatacar y denunciar a personas que no actúen conforme a las reglas estrictas de conducta de determinada sala.

Otro modo de ataque contra los menores e incapaces se producen cuando reciben correos basura o son intervenidos por hackers que envían información con contenido nocivo que en muchas ocasiones son recibidos gracias a deficientes servidores de correo electrónico que no poseen filtros adecuados o antivirus no actualizados para evitar que lleguen mensajes inapropiados. Por último, el tercer ataque consiste derivado de voluntad de los menores los cuales navegan por Internet y al estar investigando caen en páginas señuelos donde supuestamente poseen contenido de interés para ellos, pero al momento de acceder o durante la navegación de estos sitios encuentran con material nocivo o incluso al realizar la búsqueda de un tema se pueden exponer a grandes volúmenes de información no apropiados para ellos debido que se encuentra ligada una o dos palabras de su búsqueda original.

Como la Internet se ha convertido en una gran biblioteca con grandes volúmenes de información sobre cualquier tema e incluso guías de “hágalo usted mismo” podemos encontrar temas que no son aptos para menores y que en México pueden constituir como delito de corrupción de menores, pero aún así son accesibles para todo el público, dentro de los temas que se pueden encontrar en Internet resaltan:

- **Alcoholismo:** Se pueden encontrar sitios donde dan direcciones físicas de lugares donde pueden comprar y consumir alcohol sin restricción para menores o compra en línea y no requieren comprobación de edad alguna, sitios donde enseñan a hacer alcohol casero o adulterarlo, y en los que incita a ingerir bebidas alcohólicas desinformando los riesgos que causa este.

Ejemplos de sitios de como hacer licores caseros:

- ✓ <http://ar.answers.yahoo.com/question/index?qid=20061030084601AA8dLDi>
- ✓ <http://es.answers.yahoo.com/question/index?qid=20071001101922AAz57jQ>
- ✓ [http://www.taringa.net/posts/offtopic/106155/Licores-hechos-en-casa\\_\\_.html](http://www.taringa.net/posts/offtopic/106155/Licores-hechos-en-casa__.html)

- **Drogadicción:** Sitios en los que señalan técnicas de cultivo de marihuana, como cortar la cocaína o producción de drogas sintéticas; sitios en los que incitan a la drogadicción minimizando daños y riesgos, y sitios en los que enseñan como ocultar los síntomas ante la autoridad, familiares y amigos.
  
- **Tabaquismo:** Sitios en los que enseñan como cultivar y procesar tabaco casero, direcciones en la que permite la compra y consumo de tabaco entre los menores, y sitios en los que incitan al tabaquismo.
  
- **Comisión de delitos:** Sitios en los que incitan a los menores a cometer una amplia gama de delitos por diversión, que indican cómo cometer delitos sin ser supuestamente detenidos o sorprendidos o en los que publican de diversas formas experiencias delictivas por diversión para motivar a otros a realizarlos y estos a su vez los vuelvan a publicar.
  
- **Incitación a la discriminación racial, étnica y económica:** Sitios que difunden la discriminación, de sectas religiosas, y grupo sociales que incitan a la discriminación o ataques contra grupos de población.

- **Alto contenido violento:** Mediante sitios en los que muestran la violencia de guerras o acontecimientos, videos caseros contenidos extremadamente violentos y sangriento.
- **Mala información:** Mediante sitios Web en los que desinforman o proporcionan información falsa sobre temas relevantes, noticias, tabúes o acontecimientos, causando desinformación.
- **Desórdenes alimenticios:** Sitios en Internet que fomenta la anorexia o bulimia, mostrando técnicas de cómo inducirse el vomito, cómo conseguir laxantes y medicamentos controlados para el control de peso, dietas y recetas perjudiciales, consejos de cómo evitar a las autoridades, padres, amigos y profesores, proporcionan tablas de peso y medida falsas, proporcionados por falsos médicos o nutriólogos.
- **Incitación al suicidio:** Con sitios en Internet en el que fomenta las actividades para quitarse la vida ofreciendo recetas caseras accesibles para los menores, falsa asesoría de psicólogos los cuales sólo incitan a la muerte destruyendo la confianza de sus víctimas.

Otra de las criticas de la Internet, es que en este tema se ha considerado como la súper carretera de la información, pero información difícil de controlar gracias al enorme volumen de usuarios que circulan todos los días alrededor del mundo y que gracias a

que cualquiera puede tener acceso a una computadora con Internet cualquier persona puede publicar lo deseado. En la actualidad muchas empresas, asociaciones y padres de familia que se han tomado la tarea de proteger a los menores contra estos contenidos mediante información a los padres y tutores, así como, la implementación de filtros los cuales restringen toda información que tenga relación con alguna palabra buscada o solicitada, además la prevención de ataques de personas con malas intenciones.

### **Redes de narcotráfico.**

La Internet junto con la Informática se han convertido en una herramienta insuperable para muchas ciencias y actividades humanas en todo el planeta, pero como también hemos visto se ha convertido en una herramienta para cometer una gran variedad de delitos, de entre los cuales podemos encontrar al narcotráfico.

El narcotráfico usa al Internet como un medio de comunicación segura, la cual mediante servidores secretos o privados pueden entablar comunicaciones con cualquier persona a lo largo del planeta, de manera inmediata, económica y secreta. Otra forma de cómo usar la Internet es mediante el lavado de dinero, al transferir fondos de manera automática de cuenta a cuenta con el fin de transferirlas a terceras cuentas lícitas debido a que no se envía el dinero sólo los montos y al final ser retirados en otras sucursales, incluso usar la transferencia electrónica de fondos para evitar cargar con grandes cantidades de dinero para sus propios fines y negocios.

Asimismo la Internet se ha convertido en su amplio mercado negro personal, debido a que pueden acceder a cualquier comprador o vendedor de armas, materiales y su mercancía, ofreciendo confidencialidad, movilidad y rapidez desde cualquier parte del mundo bajo la apariencia de compras lícitas llevadas a cabo mediante el anonimato de la Internet.<sup>176</sup>, por último la Internet ofrece una gran variedad de conocimientos útiles como rutas, vías alternas y horarios de transporte, geografía de las naciones, y consejos del manejo y uso de la droga.

#### **4.1.3. El terrorismo cibernético.**

No existe una definición universal de terrorismos internacional, en un sentido general el terrorismo es todo acto encaminado a inducir terror en una población, el Diccionario de la Real Academia Española modifica su tercera acepción en el 2003 definiendo al Terrorismo como: "Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos"<sup>177</sup>.

El Título 22 del Código de los Estados Unidos, Sección 2656f. define al terrorismo como: "violencia premeditada, políticamente motivada perpetrada contra objetivos no-

---

<sup>176</sup> Castillo García, Gustavo. **INTERNET ES USADA YA POR NARCOS PARA COMPRAR ARMAMENTO:** PGR La Jornada <http://www.jornada.unam.mx/2005/06/13/012n1pol.php>

<sup>177</sup> El Diccionario de la Real Academia Española, en su versión 2003 [http://es.wikipedia.org/wiki/Terrorismo#\\_note-0](http://es.wikipedia.org/wiki/Terrorismo#_note-0)

combatientes por grupos subnacionales o agentes clandestinos, generalmente con la intención de influenciar a una audiencia”.<sup>178</sup>

En México el Terrorismo se encuentra en los artículos 139 al 139 Ter del Código Penal Federal, el cual señala lo siguiente:

**LIBRO SEGUNDO**  
**TÍTULO PRIMERO DELITOS CONTRA LA SEGURIDAD DE LA NACIÓN.**  
**Capítulo VI. Terrorismo**

**Artículo 193.-** 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 resulte, **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 aplicara 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 aplicara 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.

**Capítulo IX Disposiciones comunes para los Capítulos de este título.**

**Artículo 145.-** Se aplicara 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 federales 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.

---

<sup>178</sup> Embajada de los Estados Unidos de América en México. **¿QUÉ ES TERRORISMO?.** [http://www.usembassy-mexico.gov/bbf/bfdossierS\\_Terrorismo\\_quees.htm](http://www.usembassy-mexico.gov/bbf/bfdossierS_Terrorismo_quees.htm)

## **TÍTULO SEGUNDO. DELITOS CONTRA EL DERECHO INTERNACIONAL.**

### **Capítulo II. Violación de inmunidad y de neutralidad.**

**Artículo 148 Bis.-** Se impondrá pena de prisión de quince a cuarenta años y de cuatrocientos a mil doscientos días de multa, sin perjuicio de las penas que correspondan por los delitos que resulten:

- I) **A quien 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 en territorio mexicano, actos en contra de bienes o personas de un estado extranjero, o de cualquier organismo u organización Internacionales, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, par tratar de menoscabar la autoridad de ese estado extranjero, u obligar a este o aún organismo u organización internacionales para que tomen una determinación.**
- II) Al que directa o indirectamente financie, **aporte o recaude fondos económicos o recursos de cualquier naturaleza**, con conocimientos de que serán utilizados, en todo o en parte, **para cometer actos terroristas internacionales**, o en apoyo de personas u organizaciones terroristas que operen en el extranjero, y
- III) **Al que acuerde o prepare en territorio mexicano un acto terrorista que se pretenda cometer o se haya cometido en el extranjero.**

**Artículo 148 Ter.-** Se impondrá de cinco a diez años de prisión y de cien a trescientos días multa, a quien encubra a un terrorista, teniendo conocimiento de su identidad o que realiza alguna de las actividades previstas en el presente CAPÍTULO.

**Artículo 148 Quater.-** Se aplicara pena de seis a doce años de prisión y de doscientos a seiscientos días multa al que amenace con cometer el delito de terrorismo a que se refiere la fracción primera del artículo 148 Bis.

Con el ataque a las torres gemelas y el pentágono de los Estados Unidos de América el 11 de setiembre de 2001, así como, los ataques a los trenes de Madrid España el 11 de marzo de 2004, se descubrió la vulnerabilidad de las naciones contra ataques terroristas, pero con la Internet y la informática ha surgido una nueva clase de terrorismo nunca antes visto e inimaginado en el mundo conocido como Ciberterrorismo (Cyberterrorism),

Sobre el Ciberterrorismo, no existe una definición clara, pero se puede definir como: “el uso de la computadoras como armas o como objetivos por movimientos

políticos nacionales, grupos de subnacionales, y agentes clandestinos, quien ataca o causa violencia y miedo de tal forma que cause influencia en la audiencia o cause que gobiernos cambien de opinión.” (“As the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies.”).<sup>179</sup> Como se puede notar en esta definición el ciberterrorismo puede ser llevado a varias formas las cuales usan a las computadoras y al Internet como medio para llegar a sus fines o como blanco de ataques.

La Internet y las computadoras han demostrado ser una herramienta con inimaginables beneficios pero también de lamentables hechos, lo cual ha traído dos nuevas clases de terrorismo nunca antes vistos en el mundo: el primero es el terrorismo usando como herramienta al Internet y la informática, los terroristas se encuentran ante una monumental biblioteca de información sobre sus blancos, el cual les puede proporcionar desde datos simples como localización geográfica, clima de la región, idioma y lenguas, religión, posibles blancos para sus fines, características de infraestructura e ingeniería, horario de servicios público y de transportes, hasta llegar a consultar guías de uso y mecánica de vehículos, avionetas y maquinaria, creación de armamento y explosivos caseros, etc.

---

<sup>179</sup> CRS Report for Congress. Wilson, Clay. **COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS**, Updated April 1 2005. Pág. 11. <http://openocrs.cdt.org/document/RL32114>.

Como ejemplo tenemos el ataque contra las torres gemelas en Nueva York, en el que el gobierno norteamericano sostiene que la Internet fue pieza esencial en la comisión de estos ataques, ya que los terroristas se encontraban ante la información de los horarios de los vuelos, las aerolíneas que los efectuarían, así como, las rutas transitables al momento, además de información sobre horarios de entrada a labores de las oficinas, ingeniería y estructura de las torres gemelas.

Por otra parte, como se observa en la actualidad el grupo terrorista Al Qaeda utiliza la Internet par difundir su mensaje de terror y violencia alrededor del mundo, entrenado a futuros terroristas de cualquier nacionalidad mediante la publicación de videos, escritos e imágenes de técnicas de combate, creación de armas y explosivos con elementos encontrados en las tiendas, incitando sus causas con la publicación de videos en los que asesinan “infieles a su causa” e incitan con mensajes de su religión, incluso para difundir en todo el mundo amenazas con rumores de posibles ataques efectuados o por efectuarse, como ejemplo tenemos las bombas en los trenes de Madrid el 11 de Marzo del 2004, en el que los perpetradores fueron parte de una célula española de Al Qaeda, entrenados, informados y motivados por estos mensajes publicados en la Internet.

Suponiendo que durante el ataque a las torres gemelas en la ciudad de Nueva York, los sistemas de emergencia llegaron hasta el límite con el caos del momento, pero un ataque contra la red del sistema de agua, energía, telefonía fija o móvil, control aéreo, marítimo o terrestre, sistema de emergencia y militares, hubiera evitado una reacción rápida de los cuerpos de rescate, así como, la movilidad oportuna de recursos

necesarios para hacer frente a este ataque, lo que hubiera causado que sin un sistema de comunicación y control aéreo nos encontramos en una situación de incertidumbre sobre el número de aeronaves secuestradas, sin un sistema de comunicación de emergencia y defensa no se hubiera podido coordinar operativos de rescate y seguridad a lo largo de la Unión Americana, ni tampoco se hubiera podido establecer y coordinar la defensa y contrataataque militar contra otros posibles ofensivas dentro del país o contra instalaciones situadas en otras partes del mundo, y sin un sistema de comunicación móvil muchas víctimas no pudieron haber sido rescatadas de los escombros de las torres gemelas. Lo que hubiera causado un lamentable incidente con muchas más pérdidas humanas y materiales gracias a la incertidumbre y oscuridad de la ignorancia que hubiera causado un ataque de este tipo.

Las computadoras como blanco, se pueden sub-clasificarlo en tres tipos de ataques: El primero, ataques físicos, los cuales pueden ser llevados mediante la destrucción física del equipo de cómputo por medio de ataques terrorista convencionales, durante el ataque contra las torres gemelas muchos sistemas de cómputo fueron destruidos en el momento del ataque y el derrumbe de las torres, perdiendo información vital financiera y privada. El segundo, ataque puede ser llevado mediante ataques eléctricos: este tipo de ataques se pueden presentar dañando el sistema interno de una computadora con una poderosa corriente eléctrica o magnética, fundiéndolos y dejando inutilizados, por medio de ataques a plantas eléctricas, cambios intencionales en le flujo eléctrico, poderosos imanes o electroimanes, o con un pulso electromagnético resultado de bombas especiales o explosión nuclear, a diferencia con el ataque físico y el eléctrico es que en el primero se compromete la integridad física de

la totalidad del sistema de cómputo y en el segundo la estructura física se encuentra completamente íntegra, pero el sistema interno es completamente inservible. El tercer tipo de ataque se encuentra muy relacionado a los ataques terroristas que usan al Internet y las computadoras como herramienta, debido a que son usadas estas herramientas para inhabilitar otras computadoras y redes públicas o privadas, mediante avanzados ataques virtuales llevados por hackers especializados usando sofisticados programas, técnicas y virus, que son de manera instantánea y sin dejar sospecha.

En un mundo cada vez más dependiente de la tecnología informática y la Internet, muchos Estados se encuentran en extrema vulnerabilidad a este tipo de ataques, los cuales pueden llegar a generar grandes pérdidas tanto económicas como humanas.

#### **-Ataques en contra del Estado.**

Como ya se ha mencionado 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 Washintong 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.

A finales de 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 perdida 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.<sup>180</sup>

---

<sup>180</sup> Duch, Juan Pablo. **BUSCA ESTONIA Y RUSIA UNA SOLUCIÓN NEGOCIADA AL CONFLICTO QUE LOS ENFRENTAN.** Periódico La Jornada, México 5 de Mayo de 2007.  
<http://www.jornada.unam.mx/2007/05/05/index.php?section=mundo&article=030n1mun>

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 Ciber-ataques de forma expresa como una acción militar, por lo que las provisiones del Artículo V del Tratado relativas a la defensa mutua...”<sup>181</sup>. 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.

---

<sup>181</sup>El País.com, LA CRISIS ENTRE ESTONIA Y RUSIA LLEGA A INTERNET. Madrid, España. 17 de Mayo de 2007.  
[http://www.elpais.com/articulo/internet/crisis/Estonia/Rusia/llega/Internet/elpepuntec/20070517elpepuntec\\_4/Tes](http://www.elpais.com/articulo/internet/crisis/Estonia/Rusia/llega/Internet/elpepuntec/20070517elpepuntec_4/Tes)

### **-Ataques a Entidades Financieras.**

Como ya se pudo apreciar anteriormente un ataque cibernético contra Estados es un problema serio que puede causar parálisis y grandes pérdidas en el funcionamiento del Estado, incluso ser vulnerables a posibles ataques bélicos, y con la expansión de las computadoras e Internet en los sistemas financieros para controlar grandes operaciones y transacciones de negocios que se han convertido en posibles ataques cibernéticos, lo que causaría grandes pérdidas económicas a empresas y particulares como causar crisis económicas de escala global.

Los sistemas financieros al igual que un ciber-ataque convencional se puede encontrar bajo diversos tipos de ataques que pueden causar los mismos daños, dentro de los cuales se pueden encontrar:

**Ataque físico y eléctrico de los sistemas financieros:** Este al igual que cualquier ataque convencional se pueden ver afectados sistemas de cómputo tanto en su estructura física como eléctrica, que tenían por objeto almacenar, controlar o administrar información esencial, invaluable y única del sistema financiero; durante los ataques a las torres gemelas cientos de computadoras que almacenaban este tipo de información fueron completamente destruidas con lo que se perdieron millones de dólares en información vital de empresas y particulares.

**Ataques personales a sistemas financieros:** Este tipo de ataques son comunes de realizar ya que cualquier empleado o experto en computación con el sistema financiero de la empresa o dependencia en la que trabaje, en sus manos tiene acceso a

información vital de las mismas, que puede manipular, alterar, desaparecer o eliminar esta información o mover grandes cantidades de dinero en su propio beneficio o de terceros, que con la transferencia electrónica se realizan todos estos movimientos de manera inmediata lo que facilita la desaparición de grandes sumas o de operaciones en cuestión de segundos.

**Ataques vía Internet a sistemas financieros:** Estos ataques son más peligrosos que los anteriores referidos ya que la Internet otorga anonimato para los expertos y facilidad de movilidad desde cualquier parte del mundo, ya que en los anteriores se podría encontrar con relativa facilidad al responsable, la Internet dificulta la forma de localizar al perpetrador y el tipo de ataque causado, pueden ser llevados en segundos sin necesidad de estar físicamente en el lugar donde se encuentren dichos sistemas, simplemente con los conocimientos necesarios, una computadora y acceso a Internet desde la comodidad del hogar pueden cometer este tipo de ataques.

Estas agresiones cibernéticas son realmente peligrosos ya que se controlan grandes cantidades de dinero e información financiera vital que puede cambiar el rumbo de los mercados de cada nación aun cuando éstas no estén controladas por sistemas avanzados de cómputo, ya que con los movimientos adecuados nadie podría darse cuenta de un ligero cambio en las cifras que en el mejor de los casos podría causar pérdidas económicas a particulares o empresas, pérdida parcial o total de cuentas bancarias, robo en números de tarjetas de crédito en cuestión de segundos, en otros el cambio de información crucial sobre el precio de determinado producto o servicio cotizado en las bolsas de valores de cualquier nación, o incluso causar crisis

económicas, devaluaciones, pérdidas de empleo, y duros golpes a cualquier economía emergente alrededor del mundo de la que difícilmente se podrían superar simplemente con presionar un botón del ratón en menos de unos cuantos segundos.

### **-Ataques a Servicios.**

En un mundo cada vez más dependiente de las computadoras y la Internet, el hombre le ha dado cada vez más responsabilidades a las máquinas para mejorar y facilitar su vida diaria, desde éste sistema se ha facilitado el control y la consulta de información para una tarea en la primaria, el control de semáforos, los sistemas de emergencia y suministro de gas, agua y luz, hasta el control de tráfico aéreo, comunicaciones, sistemas de alerta y defensa militar. Con lo que este tipo de computadoras se han convertido en el blanco perfecto de ciber-ataques, al igual que un ataque convencional estas se encuentran vulnerables a un ataque físico, eléctrico, personal y vía Internet. En la que en cuestión de segundos puede generar caos y pánico en una población, paralizando los transportes públicos, aéreos y marítimos, apagando o alterando los sistemas de tránsito como semáforos y vigilancia, inutilizando sistemas de emergencia, o incluso inhabilitando el sistema de flujo de corriente eléctrica de una importante Capital.

No sólo con retrasos y ataques a estos sistemas se han paralizado el transporte, puede poner en riesgo a poblaciones enteras con el cambio en la calidad del agua potable al público, control en la fabricación de productos y en la calidad en los alimentos en sus procesos de producción y procesamiento, incluso causar pérdidas humanas al inutilizar sistemas de emergencia, tanto de comunicación como sistemas de los

hospitales. Hasta llegar a la vulnerabilidad total contra ataques militares por otras naciones al dejar inservibles sistemas de defensa y comunicación militar.

### **La seguridad informática.**

Este concepto abarca todos aquellos pasos y métodos para la protección de datos personales, equipos informáticos, claves personales, protocolos de seguridad, ya que para un usuario le afecta tanto perder información como el propio equipo donde se encuentra la misma o incluso la protección de otros bienes dentro de su patrimonio. Durante los años se ha venido perfeccionando todo lo relacionado a los sistemas de computación, adecuándose máquinas con mayor capacidad, con mayores funciones, más rápidas, más pequeñas, con mayor duración, etc...sin olvidar las diversas formas para recibir, procesar y transmitir la información, creándose para todo ello diversos sistemas de seguridad.

Ahora existen diversos sistemas de cómputo que guardan la información en altos índices de seguridad a lo que se le ha llamado “encriptar la información” desgraciadamente los diversos delincuentes informáticos a los que hemos hecho referencia se han encontrado pasos adelante para poder cometer sus conductas delictivas.

## **4.2. Tratamiento de la delincuencia informática en organismos internacionales.**

Los delitos informáticos son un problema serio a nivel mundial y más ahora con la llegada de la Internet y todos los beneficios que ésta otorga para la comisión de una gran gama de delitos de diversas naturalezas, debido a este gran reto muchas naciones y organismos internacionales se han tomado a la tarea de combatirlos creando legislaciones efectivas y métodos de persecución, así como, modelos recomendados a seguir e incentivando la cooperación internacional para hacer frente a este nuevo problema.

### **4.2.1. En la Organización de las Naciones Unidas.**

La Organización de las Naciones Unidas se ha preocupado por la problemática de los Delitos Informáticos alrededor del mundo y tras minuciosos análisis sociales y jurídicos ha llegado regular algunas conductas al respecto como reconocer algunos ilícitos Informáticos cometidos de manera frecuente dentro de los cuales encontramos los siguientes:

#### **I. Fraudes cometidos mediante manipulación de computadoras:**

- **Manipulación de datos de entrada:** Es el delito informático más común, consiste en la sustracción de datos durante el suministro de datos a los sistemas informáticos, requiere niveles mínimos de conocimiento para realizarse.

- **Manipulación de programas:** Consiste en la alteración de programas genuinos o agregar programas adjuntos que generalmente son virus, ésta técnica requiere de altos niveles en el lenguaje de programación y se presenta en páginas donde regalan programas que generalmente tienen un costo por su uso.
- **Manipulación de datos de salida:** Consiste en manipular el sistema para obtener un resultado diferente en el comportamiento del mismo, éste se presenta en la sustracción de dinero de los cajeros automáticos mediante computadoras y decodificadores.
- **Fraudes efectuados por manipulación Informática:** consiste en manipulación de información, esta técnica se da con frecuencia en la sustracción de dinero de las instituciones financieras, alterando los datos de las cuentas.

## **II. Falsificaciones informáticas.**

- **Como objeto:** Es la alteración de datos en documentos computarizados.
- **Como instrumento:** Consiste en crear alterar o falsificación de documentos mediante el uso de las computadoras y sus componentes.

### **III. Daños o modificaciones de programa o datos computarizados.**

- **Sabotaje informático:** Es la modificación, creación o supresión de información en un sistema para obstruir el buen funcionamiento del sistema.
- **Virus.**
- **Gusanos.**
- **Bombas lógicas o cronológicas.**

### **IV. Falsificaciones informáticas:**

- **Acceso no autorizado a sistemas o servicios.**
- **Pirata informático o Hackers.**
- **Reproducción no autorizada de programas de información.**

Sobre estos últimos ya hice alusión anteriormente y los cuales son los medios comisivos de delitos informáticos en la mayor parte del mundo.

### **El G8. (Grupo de los ocho).**

Conocido como el grupo de los ocho países más industrializados en el mundo, preocupados por este problema actual, el 11 de mayo de 2004 en Washintong, se realizó la cumbre “sea Island” meeting of G8 Justice and Home Affaire Ministres, reunión de los ministros de asuntos de Justicia y Estado, en el que asistieron Canadá, Francia, Alemania, Italia, Japón y Reino Unido, junto con comisionados de la Unión Europea sobre asuntos de Justicia y Estado<sup>182</sup>, en la que sus principales temas a tratar fueron:

1. La Prevención del terrorismo y actos criminales serios.
2. Seguridad fronteriza y de transporte.
3. Combate al ciber-crimen y redoblando esfuerzos en las ciber-investigaciones.
4. Lucha contra la corrupción oficial extranjera y recaptura de activos nacionales robados.

#### **4.2.2. En la Comisión de las Comunidades Europeas.**

Los países Europeos han reflejado una gran preocupación de mantenerse unidos ante diversos acontecimientos sociales, políticos, económicos, legislativos entre otros, formando precisamente una comunidad Europa. Surge así el mercado común europeo una moneda unitaria llamada “euro” entre otras situaciones más.

---

<sup>182</sup> Meeting of G8 Justice and Home affairs ministres, “Sea Island Summit 2004” <http://www.cybercrime.gov/g82004/index.html>

En el problema de los Delitos Informáticos, la Unión Europea se ha mostrado más unida y a la vanguardia, que se ve reflejado con diversos tratados referentes a esta actual problemática, de los que destacan convenios hechos por el Consejo Europeo (Council of Europe), de los cuales resaltan: El Convenio para la Protección de las Personas Referente al Tratamiento Automático de los Datos de Carácter Personal en 1998 y el Convenio sobre Ciber-criminalidad de 2001, en el cual hay que mencionar.

### **El Convenio sobre la Ciber-criminalidad:**

Firmado en Budapest el 23 de Noviembre de 2001, por los países integrantes de la Unión Europea y Estados participantes, en la que emite sus recomendaciones sobre el trato que deberá llevarse frente a los Delitos Informáticos, en el cual sus principales objetivos son:

- Reafirmar la estrecha unión entre las naciones de la Unión Europea y países firmantes para enfrentar la Cibercriminalidad.
- Intensificar la cooperación con los estados miembros.
- Prioridad en unificar una política penal para prevenir la criminalidad en el ciberespacio con una legislación apropiada y mejorar la cooperación internacional.
- Concientizar a los Estados miembros de los cambios suscitados por la convergencia y globalización de las redes.
- Concientizar sobre la preocupación del riesgo de las redes informáticas y la informática electrónica de ser utilizadas para cometer infracciones penales, ser almacenados y exhibidos.

- Fomentar la cooperación entre los Estados e industrias privadas en la lucha contra la cibercriminalidad y la necesidad de protección del uso de la Informática para fines legítimos al desarrollo de la tecnología.
- Concientizar que la lucha contra la Criminalidad requiere la cooperación internacional en materia penal asertiva, rápida y eficaz.
- Persuadir sobre la necesidad de un equilibrio entre los intereses de la acción represiva y el respeto de los Derechos del Hombre garantizado en el convenio para la protección de éstos derechos y libertades fundamentales y reafirmar el derecho de no ser perseguido por la opinión pública, la libertad de expresión, libertad de búsqueda y el respeto a la vida privada.
- Complementar los convenios anteriores, relacionados con la materia o que otorguen soporte, con el fin de hacer más efectiva la investigación, procedimientos penales y recolección de pruebas electrónicas.
- Persuadir sobre la necesidad de mantener y proteger la confiabilidad, integridad y disponibilidad de los sistemas de cómputo, bases de datos, computadoras y redes.

De lo convenido dentro de este documento destaca la descripción hecha de las conductas delictivas llevadas por medios informáticos, de aplicación para los Estados miembros de los cuales cabe resaltar los siguientes artículos:

## **Capítulo I – Terminología**

### **Artículo 1 – Definiciones**

A los efectos del presente Convenio, la expresión:

a). "**Sistema informático**" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b). "**Datos informáticos**" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c). "**Prestador de servicio**" designa:

I. Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

II. Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d). "Datos de tráfico" designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

## **Capítulo II – Medidas que deben ser adoptadas a nivel nacional**

### **Sección 1 – Derecho penal material**

#### ***Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos***

##### **Artículo 2 – Acceso ilícito**

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prevenir **como infracción penal**, conforme a su derecho interno, **el acceso doloso y sin autorización a todo o parte de un sistema informático**. Las partes podrán exigir que la infracción **sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva**, o también podrán requerir que la infracción **se perpetre en un sistema informático conectado a otro sistema informático**.

##### **Artículo 3 – Interceptación ilícita**

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prevenir **como infracción penal**, conforme a su derecho interno, la **interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos** . Las partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción **se perpetre en un sistema informático conectado a otro sistema informático**.

##### **Artículo 4 – Atentados contra la integridad de los datos**

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prevenir como **infracción penal**, conforme a su derecho interno, la **conducta de dañar**,

**borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.**

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero **ocasiona daños que puedan calificarse de graves.**

#### **Artículo 5 – Atentados contra la integridad del sistema**

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever **como infracción penal**, conforme a su derecho interno, **la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.**

#### **Artículo 6 – Abuso de equipos e instrumentos técnicos**

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever **como infracción penal**, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a).La **producción, venta, obtención para su utilización, importación, difusión** u otras formas de puesta a disposición:

I. **De un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;**

II. **De una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5 ; y**

b). **La posesión de alguno de los elementos descritos** en los párrafos (a) (1) o (2) **con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5** . Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo **no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5** del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a)(2).

### ***Título 2 – Infracciones informáticas***

#### **Artículo 7 – Falsedad informática.**

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como **infracción penal**, conforme a su derecho interno, **la introducción, alteración,**

**borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos**, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

#### **Artículo 8 – Estafa informática.**

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como **infracción penal**, conforme a su derecho interno, **la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:**

- a). **La introducción, alteración, borrado o supresión de datos informáticos,**
- b). **Cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.**

### ***Título 3 – Infracciones relativas al contenido.***

#### **Artículo 9 – Infracciones relativas a la pornografía infantil.**

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como **infracción penal**, conforme a su derecho interno, las siguientes **conductas** cuando éstas sean cometidas **dolosamente y sin autorización:**

- a). **La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;**
- b). **El ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;**
- c). **La difusión o la transmisión de pornografía infantil a través de un sistema informático;**
- d). **El hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;**
- e). **La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.**

2. A los efectos del párrafo 1 arriba descrito, la «**pornografía infantil**» **comprende cualquier material pornográfico que represente de manera visual:**

- a). **Un menor adoptando un comportamiento sexualmente explícito;**
- b). **Una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;**
- c). **Unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.**

3. A los efectos del párrafo 2 arriba descrito, el término «menor» **designa cualquier persona menor de 18 años**. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

#### ***Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines***

#### **Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines**

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como **infracción penal**, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, **conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor**, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, **a escala comercial y a través de un sistema informático**.

2. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como **infracción penal**, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, **conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas**, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, **a escala comercial y a través de un sistema informático**.

3. Las partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de **no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo**.

Cabe señalar que esta convención hace referencia a otros temas de gran relevancia para los Delitos informáticos, de los cuales destacan:

**Artículo 11** – Tentativa y complicidad.

**Artículo 12** – Responsabilidad de las personas jurídicas.

**Artículo 13** – Sanciones y medidas.

## **Sección 2 – Derecho procesal.**

**Artículo 14** – Ámbito de aplicación de las medidas de derecho procesal.

**Artículo 15** – Condiciones y garantías.

**Artículo 16** – Conservación inmediata de datos informáticos almacenados.

**Artículo 17** – Conservación y divulgación inmediata de los datos de tráfico.

**Artículo 18** – Mandato de comunicación.

**Artículo 19** – Registro y decomiso de datos informáticos almacenados.

**Artículo 20** – Recogida en tiempo real de datos informáticos.

**Artículo 21** – Interceptación de datos relativos al contenido.

**Artículo 22** – Competencia.

**Artículo 23** – Principios generales relativos a la cooperación internacional .

**Artículo 24** – Extradición.

**Artículo 25** – Principios generales relativos a la colaboración.

**Artículo 26** – Información espontánea.

**Artículo 27** – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable.

**Artículo 28** – Confidencialidad y restricciones de uso.

**Artículo 29** – Conservación inmediata datos informáticos almacenados.

**Artículo 30** – Comunicación inmediata de los datos informáticos conservados.

**Artículo 31** – Asistencia concerniente al acceso a datos informáticos almacenados.

**Artículo 32** – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso.

**Artículo 33** – Asistencia para la recogida en tiempo real de datos de tráfico.

**Artículo 34** – Asistencia en materia de interceptación de datos relativos al contenido.

**Artículo 35** – Red 24/7 (Punto de contacto localizable las 24 horas del día, y los siete días de la semana, para asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal).

**Artículo 36** – Firma y entrada en vigor.

**Artículo 37** – Adhesión al Convenio.

**Artículo 38** – Aplicación territorial.

**Artículo 39** – Efectos del Convenio.

**Artículo 40** – Declaraciones.

**Artículo 41** – Cláusula federal.

**Artículo 42** – Reservas.

**Artículo 43** – Mantenimiento y retirada de las reservas.

**Artículo 44** – Enmiendas.

**Artículo 45** – Reglamento de controversia.

**Artículo 46** – Reuniones de los Estados.

**Artículo 47** – Denuncia.

**Artículo 48** – Notificación.

En este convenio se encuentran 39 países que han firmado de los 47 Estados miembros, de los cuales 21 ya ratificaron, y dentro de los 6 Estados no miembros del Consejo Europeo y participantes en esta convención sólo 4 han firmado y de entre los cuales únicamente Estados Unidos de América ratificó dicha Convención, se tiene que hacer mención que México como país participante no ha firmado este convenio hasta la fecha.

## ESPAÑA:

España ha adoptado seguir la tendencia global contra los Delitos Informáticos y las conductas llevadas a cabo mediante de los medios informáticos por presión social empresarial e internacional, persiguiendo conductas como la copia y el uso de programas sin permiso del autor, la defraudación y revelación de secretos por medios electrónicos como herramienta, entre otros. A continuación se enuncian los artículos del Código Penal Español<sup>183</sup> que contemplan estas conductas delictivas.

### TÍTULO X

#### DELITOS CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y LA INVOLABILIDAD DEL DOMICILIO

##### CAPÍTULO PRIMERO

###### Del descubrimiento y revelación de secretos

###### 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, **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**.

---

<sup>183</sup> <http://www.unifr.ch/derechopenal/legislacion/es/cpespidx.html>

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 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 4 del artículo 130.

## **TÍTULO XIII DELITOS CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONÓMICO.**

### **CAPÍTULO VI DE LAS DEFRAUDACIONES**

#### **Sección Primera**

## De las estafas

**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 249.** Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

## Sección Tercera

### De las defraudaciones de fluido eléctrico y análogas

**Artículo 255.** Será castigado con la pena de multa de tres a 12 meses el que cometiere defraudación por valor superior a 400 euros, 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 400 euros, será castigado con la pena de multa de tres a 12 meses.

## CAPÍTULO IX

### De los daños

**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 24 meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de 400 euros.

**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 anterior, si concurriere 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 puedan 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.**

## CAPÍTULO XI

### DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL E INDUSTRIAL, AL MERCADO Y A LOS CONSUMIDORES

#### Sección Primera

##### De los delitos relativos a la propiedad intelectual

**Artículo 270.** 1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, **reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio**, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien intencionadamente **exporte o almacene ejemplares de las obras, producciones o ejecuciones a que se refiere el apartado anterior** sin la referida autorización. Igualmente incurrirán en la misma pena los que **importen intencionadamente estos productos** sin dicha autorización, **tanto si éstos tienen un origen lícito como ilícito en su país de procedencia**; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.

3. Será castigado también con la misma pena quien **fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.**

## TÍTULO XVIII DE LAS FALSEDADES

### CAPÍTULO III DISPOSICIÓN GENERAL

**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 rivelare la información obtenida**, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

En cuanto al tratamiento de la información, la Unión Europea ha demostrado grandes adelantos con el fin de resolver problemas serios sobre el trato y protección de la información, llegando así al Convenio número 108 del Consejo de Europa para la Protección de las personas con relación al tratamiento automatizado de datos de carácter personal firmado el 28 de enero de 1981 en Estrasburgo, Francia<sup>184</sup>, de los cuales ratificaron Alemania y España el 19 de junio de 1985, Noruega el 20 de febrero de 1984, Suecia el 29 de septiembre de 1982 y tan sólo Francia aprobó este convenio el 24 de Marzo de 1983, del cual resaltan los siguientes artículos:

## CAPÍTULO. I

### **Artículo 1.** Objeto y Fin.

El fin del presente convenio es garantizar, en el territorio de cada parte, a toda persona física, cualquiera que fuera su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales y en especial de su **derecho a la intimidad**, con respecto al tratamiento automático de los datos de carácter persona que le concernieren ("protección de datos").

### **Artículo 2.** Definiciones

A los efectos del presente Convenio:

- a) «**Datos de carácter personal**» significa **cualquier información relativa a una persona** física identificada o identificable («persona concernida»);
- b) «**Fichero automatizado**» significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado;
- c) Por «**tratamiento automatizado**» se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados:

---

<sup>184</sup> **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>

**Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;**

d) Autoridad «controladora del fichero» significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

## **CAPÍTULO II**

### **PRINCIPIOS BÁSICOS PARA LA PROTECCIÓN DE DATOS**

#### **Artículo 4.** Compromisos de las Partes

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

**Artículo 5.** Calidad de los datos Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) Serán exactos y si fuera necesario puestos al día;

e) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

#### **Artículo 7.** Seguridad de los datos

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

#### **Artículo 10.** Sanciones y recursos

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

#### **Artículo 11.** Protección más amplia

Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio.

## **CAPÍTULO IV**

### **AYUDA MUTUA**

#### **Artículo 13. Cooperación entre las Partes**

1. Las Partes se obligan a concederse mutuamente asistencia para el cumplimiento del presente Convenio.

2. A tal fin,

a) Cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa;

b) Cada Parte que haya designado a varias autoridades indicará en la comunicación a que se refiere el apartado anterior la competencia de cada una de dichas autoridades.

3. Una autoridad designada por una Parte, a petición de una autoridad designada por otra Parte:

a) Facilitará informaciones acerca de su derecho y su práctica administrativa en materia de protección de datos;

b) Tomará toda clase de medidas apropiadas, con arreglo a su derecho interno y solamente a los efectos de la protección de la vida privada, para facilitar informaciones fácticas relativas a un tratamiento automatizado determinado efectuado en su territorio con excepción, sin embargo, de los datos de carácter personal que sean objeto de dicho tratamiento.

## **CAPÍTULO V**

### **COMITÉ CONSULTIVO**

#### **Artículo 18. Composición del Comité**

1. Después de la entrada en vigor del presente Convenio se constituirá un Comité Consultivo.

2. Cada Parte designará a un representante y a un suplente en dicho Comité.

Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio tendrá el derecho de hacerse representar en el Comité por un observador.

3. El Comité Consultivo podrá, mediante una decisión tomada por unanimidad, invitar a cualquier Estado no miembro del Consejo de Europa, que no sea Parte del Convenio, a hacerse representar por un observador en una de las reuniones.

#### **Artículo 19.** Funciones del Comité

El Comité Consultivo:

- a) Podrá presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio;
- b) Podrá presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21;
- c) Formulará su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, con arreglo al artículo 21, párrafo 3; d) podrá, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio.

Derivado de este convenio y con la preocupación latente sobre el tratamiento de información la comunidad Europea se ha encontrado con un gran reto sobre la diversificación de leyes que lograron resolver en conjunto creando leyes modelos y directivas a seguir por sus Estados miembros, para poder dar solución a este problema del cual destaca la Directiva 95/46CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos<sup>185</sup>, de los cuales se puede resaltar:

## **CAPÍTULO I**

### **DISPOSICIONES GENERALES**

#### **Artículo 1.** Objeto de la Directiva.

1. Los Estados miembros garantizarán con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

---

<sup>185</sup> ANEI, Asociación Nacional de Empresa, España. **Directiva 95/46CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos** . [http://www.a-nei.org/documentos/Dir\\_9546CE.pdf](http://www.a-nei.org/documentos/Dir_9546CE.pdf)

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

## **Artículo 2.** Definiciones.

A efectos de la presente Directiva, se entenderá por:

a) «Datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) «Tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c) «Fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d) «Responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

e) «Encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f) «Tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g) «Destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h) «Consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

## SECCIÓN I

### PRINCIPIOS RELATIVOS A LA CALIDAD DE LOS DATOS

#### Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:

a) Tratados de manera leal y lícita;

b) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;

c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) Exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas;

e) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con finesm, históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

## SECCIÓN V

### DERECHO DE ACCESO DEL INTERESADO A LOS DATOS

#### Artículo 12. *Derecho de acceso*

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) Libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) En su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) La notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

## SECCIÓN VI

### EXCEPCIONES Y LIMITACIONES

#### **Artículo 13.** *Excepciones y limitaciones*

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) La seguridad del Estado;

b) La defensa;

c) La seguridad pública;

d) La prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) Un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) Una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) La protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos

de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

## SECCIÓN VIII

### CONFIDENCIALIDAD Y SEGURIDAD DEL TRATAMIENTO

#### **Artículo 16.** Confidencialidad del tratamiento.

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

#### **Artículo 17.** Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- Que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- Que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

## CAPÍTULO III

### RECURSOS JUDICIALES, RESPONSABILIDAD Y SANCIONES

#### **Artículo 22.** *Recursos*

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

#### **Artículo 23. Responsabilidad**

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

#### **Artículo 24. Sanciones**

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

## **CAPÍTULO VII**

### **MEDIDAS DE EJECUCIÓN COMUNITARIAS**

#### **Artículo 31. El Comité**

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. 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 el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El **presidente** no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:

- La Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;

- El Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

### **4.2.3. En la Sociedad de la Información.**

La sociedad de la información es aquella en la que las nuevas tecnologías actúan en beneficio de la sociedad para alcanzar los objetivos de comunicación e información, Julio Téllez Valdez define a la Sociedad de la Información como: "el uso masivo de tecnologías de la información y comunicación para difundir el conocimiento e intercambio de la sociedad<sup>186</sup>".

Los beneficios que ha traído la informática y la Internet en el mundo han cambiado la vida en la tierra en todas sus ciencias, aun como en la sociedad, en los gobiernos y en la forma de como ver la vida, por lo que la ONU junto con la Unión Internacional de Telecomunicaciones convocaron en Túnez la Cumbre Mundial de la Sociedad de la Información, siendo los participantes los miembros de las Naciones Unidas, empresas privadas y la sociedad civil, siendo el principal punto a discutir la eliminación de la brecha digital existente en el acceso a las nuevas tecnologías en el mundo con el fin de alcanzar beneficios a cada persona en cualquier parte del mundo

Apartar de este importante hecho la Unión Europea, preocupada por hacer accesible las nuevas tecnologías informáticas a cada uno de sus países miembros se emitieron las Directivas 98/34/CE de 22 de junio y 98/48/CE de 20 de julio de 1998 del Parlamento Europeo y del Consejo<sup>187</sup>, las cuales tenían el objeto de eliminar en lo

---

<sup>186</sup> Téllez Valdés, Julio. Op. Cit. Pág. 6.

<sup>187</sup> Eur-LEx, Directiva 93/34CE. [http://eur-lex.europa.eu/LexUriServ/site/es/oj/1998/l\\_204/l\\_20419980721es00370048.pdf](http://eur-lex.europa.eu/LexUriServ/site/es/oj/1998/l_204/l_20419980721es00370048.pdf)

posible o de reducir los obstáculos en el intercambio comercial de productos industriales, agrícolas y pesqueros, así como la libre prestación de servicios de la sociedad de la información dentro de la Unión con la implementación de cada país miembro de reglamentos o leyes tendientes a crear mecanismos de comunicación y transparencia entre Estados, o el público.

Tiempo después se emitió la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en particular el comercio electrónico en el mercado interior, la cual surge para regular determinados aspectos del comercio electrónico llevado entre los países miembros de la Unión Europea, desprendida de las anteriores directivas sobre la Sociedad de la Información.<sup>188</sup>

Entre los Estados miembros de la Unión Europea que han adoptado seguir esta Directiva se presenta España, emitiendo la Ley de Servicios de la Sociedad de la Informática y del Comercio Electrónico o Ley 34/2002 de 11 de julio de 2002, la cual en su Artículo 1º, de esta Ley determina el objeto de la regulación del régimen jurídico de los servidores de la sociedad de la información y de la contratación por vía electrónica, y a las obligaciones de los prestadores de servicios intermediarios en la prestación de contenido de la información en las redes de telecomunicaciones<sup>189</sup>.

---

<sup>188</sup> Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, [www.mityc.es/NR/rdonlyres/62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva\\_2000\\_31\\_CE.pdf](http://www.mityc.es/NR/rdonlyres/62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva_2000_31_CE.pdf)

<sup>189</sup> Área del Derecho civil de la Universidad de Girona, España. <http://civil.udg.es/normacivil/estatal/contract/LSSI.htm>

### **4.3. La Criminalística Informática.**

Independientemente de la problemática que se presenta en la ley en cuanto a su técnica legislativa, y otras que se han analizado en Capítulos anteriores, es menester hacer referencia a otro de los graves problemas al que se ha enfrentado el Derecho Penal que es la localización y detención del delincuente, para lo cual se asiste de diversas ciencias auxiliares como son la Criminología y la Criminalística.

La Criminología consiste en una Ciencia explicativa y encuentra su principal objetivo precisamente al pretender explicar las causas por las que surge un delito, es decir, encontrar los diversos factores criminológicos que se dan para la comisión de un ilícito, haciendo aparición a la Antropología Criminal, a la Sociología Criminal, a la Psicología Criminal, entre otras.

La Criminalística está enfocada principalmente al hallazgo del delincuente a la que le asignaré los apartados siguientes en torno a los Delitos Informáticos.

#### **4.3.1. La Criminalística.**

Como ciencia auxiliar del Derecho Penal encontramos a la Criminalística que se asiste de las diversas ciencias naturales, disciplinas y técnicas a efecto de encontrar el *modus vivendi* y *operandi* del delincuente, es decir, para lograr principalmente su localización a través de los diversos vestigios que pueden ser dejados en la comisión de un delito.

La Criminalística se encuentra constituida por un conjunto de conocimientos heterogéneos encaminados al hallazgo de los delincuentes, al conocimiento del *modus operandi* del delito y al descubrimiento de las pruebas y de los procedimientos para utilizarlas.<sup>190</sup>

Los objetivos de la Criminalística son:

- a) Investigar técnicamente y demostrar científicamente la existencia de un hecho en particular probablemente delictuoso.
- b) Determinar los fenómenos y reconstruir el mecanismo del hecho, señalando los instrumentos y objetos de ejecución, sus manifestaciones y las maniobras que se pusieron en juego para realizarlo.
- c) Aportar evidencias o coordinar técnicas o sistemas para la identificación de la víctima si existiere.
- d) Aportar evidencias para la identificación de los presuntos autores y coautores.
- e) Aportar las pruebas materiales con estudios técnicos científicos para probar el grado de participación del o de los presuntos autores y demás involucrados.<sup>191</sup>

Así, la Criminalística cumple con las siguientes finalidades:

- a) Auxiliar al órgano investigador en sus funciones para que realice adecuadas conclusiones en su labor en la procuración de justicia.
- b) Apoyo a través de dictámenes periciales a los órganos de procuración y de impartición de justicia.

---

<sup>190</sup> Castellanos Tena, Fernando. Op. Cit. Pág. 29.

<sup>191</sup> Montiel Sosa, Juventino: **CRIMINALÍSTICA**. Editorial Limusa. Segunda edición México 2007. Pág. 86.

- c) Participar en las diligencias ministeriales y judiciales para tratar de llegar a la verdad histórica.

La Ciencia de la Criminalística tiene principios que la regulan enfocados a relacionar las evidencias del lugar de la investigación con las personas que participaron en la comisión del delito: La mayoría de los autores manejan principalmente cuatro principios tales como son:

- a) **El principio de intercambio.-** Este consta en que siempre existe un intercambio de evidencias entre el delincuente y el lugar de los hechos.
- b) **El principio de correspondencia de características.-** Consistente en la relación lógica de la evidencia encontrada en el lugar de la investigación con el probable responsable.
- c) **El principio de reconstrucción.-** Basado en la investigación en la que los datos que durante esta se recaben y los testimonios de quienes presenciaron los hechos, los expertos pueden realizar una reconstrucción lo más apegada a la verdad histórica.
- d) **El principio de probabilidad.** En donde la reconstrucción de los hechos nos acerca al conocimiento de la verdad pueden ser en un bajo o mediano o alto grado de probabilidad o simplemente nula la probabilidad.

La Criminalística debe entonces servir para desentrañar los indicios o evidencias físicas o materiales que será aprovechada por el Derecho Penal para llegar a una adecuada conclusión.

Dentro de las ciencias, disciplinas y técnicas que pueden servir dentro de la Criminalística se encuentran a las siguientes: medicina, física, química, contabilidad, entre otras muchas más, las cuales convirtiéndose en las llamadas “Ciencias Forenses” pueden servir para desentrañar delitos tales como homicidio, lesiones, violación, financieros, entre otros, ya que estas ciencias aportan múltiples conocimientos especializados.

#### **4.3.2. La Criminalística en la Informática.**

En los delitos informáticos estudiados en la presente investigación definitivamente, dentro de la especialización requerida para descubrir el *modus operandi* de los delincuentes o sujetos activos son la Informática y la Cibernética desde todos los enfoques analizados en el Capítulo Primero; es decir, podemos asistirnos desde la Informática en general, así como a la propia informática Jurídica, y de otras ciencias auxiliares; como ejemplo sería la contabilidad, para el caso de que se sustraiga información contable contenida en medios informáticos, o bien en aquellos delitos financieros cometidos a través de medios informáticos. Cabe recordar que el Derecho se encuentra inmerso en un mundo interdisciplinario en donde puede asistirse de inimaginables medios con el fin de llegar a la verdad histórica.

Surge así la “Informática Forense” la cual va a tratar sobre la aplicación de las diversas técnicas científicas y analíticas sobre la infraestructura de sistemas

computacionales, para identificar, preservar, analizar y presentar las evidencias para encontrar el *modus operandi* del delincuente informático.

Problemática a la que se han enfrentado las investigaciones de los delitos informáticos:

- a) Uniformar disposiciones sobre los delitos informáticos. Situación que se analizó en el Capítulo 2 de la presente investigación.
- b) Facultad de especialización en los órganos de procuración y administración de justicia para el tratamiento de los delitos informáticos.
- c) La ausencia en la creación de órganos auxiliares en la procuración de justicia para la adecuada investigación de los delitos informáticos, tales como una policía especializada, así como un cuerpo de expertos en la materia.
- d) El carácter transnacional de las múltiples operaciones realizadas a través de los sistemas computacionales.
- e) Ausencia de tratados internacionales para resolver múltiples problemas relacionados con los delitos informáticos, que van desde la celebración de convenios internacionales de colaboración, así como de extradición o de intercambio de reos por estos delitos.
- f) Escaso control de las compañías de computadores, así como de sus servicios como el de Internet.

La Informática Forense puede también ser utilizada como un efectivo proceso de aclaración interno de incidentes computacionales de riesgo antisocial, de errores o negligencias al interior de organizaciones, realizando un reporte discrecional hacia las

autoridades públicas ya que puede haber razones de peso estratégico que afectarían la continuidad operativa, viabilidad o imagen de una organización en particular si se revelase información sensible sobre sistemas o aplicaciones vulnerables.

#### **4.3.3. La Policía Cibernética.**

De gran función en la Criminalística resultan los cuerpos policíacos que son los que acuden al lugar en donde se cometieron los hechos realizando lo que se conoce como trabajo de campo y su labor principal es recabar los indicios que le servirán al órgano de procuración de justicia para integrar adecuadamente su averiguación previa.

En otros países sobre todo de origen anglosajón como los Estados Unidos de América se encuentran cuerpos de policía especializados como el Federal Bureau of Investigation (FBI) que concentra la información recabada en el lugar de los hechos y dentro de ella la concentran en oficinas especializadas que realizan funciones de Inteligencia Criminal a efecto de depurar los datos recabados y solamente analizar lo que realmente importen para una investigación, apareciendo oficinas para el análisis de los vestigios que requieren de la especialización de cada delito, como sería el caso de los informáticos, originándose la creación de la llamada “Policía Cibernética”.

Definitivamente que la policía debe tener un grado de especialización para la investigación de los delitos existiendo academias en todo el mundo en donde surge una disciplina conocida como “La Policía Científica”.

En la Criminalística Forense es indispensable comprender que identificar y seguir la pista a la evidencia digital y protegerla, es la parte trascendental de una adecuada investigación; la Policía Cibernética debe saber enfocar su atención a los hechos del delito en donde aparece tanto al delincuente informático como el sistema de cómputo que ha utilizado y en dónde lo ha usado, ya que como sabemos puede utilizar una computadora de escritorio, una lap top, propia o ajena, o inclusive otro sistema de cómputo aún más compacto como las conocidas “palm o pocket pc”, en un país o en el extranjero o inclusive en varios países; la evidencia digital puede estar contenida en la computadora de la víctima o en un dispositivo de almacenamiento como un disquete, en los archivos de una empresa de servicios de Internet, en la computadora del sujeto pasivo o en sus disquete o discos o “usb” o bien, en otras ubicaciones de la red; una gran labor para el Policía Cibernético.

Una de las principales labores de toda policía es saber conservar el lugar de los hechos con todos los conocimientos especializados para ello, ya que desgraciadamente sabemos en la práctica de campo muchas corporaciones policiacas creen que cumplen con ello solamente con recabar toda información sin saber que hay técnicas especializadas para ello. Ejemplo sería en un robo a casa habitación en donde la policía solamente se concreta a tomar declaraciones de los testigos e introducir en bolsas algunos objetos que pudieron haber servido como instrumentos del delito sin tener el cuidado de que cada objeto debe ser preservado con su técnica especial ya que podemos encontrar algunos que con el tiempo se puedan destruir, o bien, sin tener la precaución de tomar las posibles huellas digitales que pudieran haber dejado los sujetos activos.

## **- La Unidad de Policía Cibernética de la Policía Federal Preventiva en México.**

Uno de los medios dentro de la investigación de los delitos ha sido la creación de policías especializadas para combatir cierto tipo de delincuencia, mientras se encuentre dentro de las corporaciones policíacas que demarca la Constitución Política de los Estados Unidos Mexicanos y las legislaciones secundarias, para no caer en agrupaciones que actúen fuera de la ley, como fue el caso de la llamada "DIP".

En México se ha venido profesionalizando cada día a los integrantes de las diversas policías, exigiéndose variados requisitos para pertenecer y permanecer en ellas, tales como la edad, la estatura, la complexión, su nivel académico, etc, debiendo cuidar también aspectos subjetivos tales como: su responsabilidad, su capacidad moral, su honestidad, entre otros más.

Definitivamente es de gran importancia la interrelación que se guarde entre las diversas agrupaciones policiales de México, como con las entidades federativas que la conforman y con las de otros países ya que como se ha mencionado los Delitos Informáticos como otros tienen trascendencia internacional, ya que con el uso de un sistema informático se puede violentar la información en otros sistemas en el lugar más apartado del mundo, llevándose a cabo investigaciones especializadas para lograr localizar al delincuente cibernético.

En México se ha tenido también la gran preocupación de prevenir y combatir los ilícitos que le han ocasionado graves daños a la sociedad desde los años 90's, tales como los delitos contra la salud, los de delincuencia organizada, los de naturaleza financiera y los informáticos, entre otros, fortaleciendo en algunos casos su marco jurídico correspondiente y en otros creando legislaciones novedosas.

La Secretaría de Seguridad Pública Federal creó en el año 2000 la Unidad de Policía Cibernética y Delitos contra Menores teniendo como las siguientes finalidades:

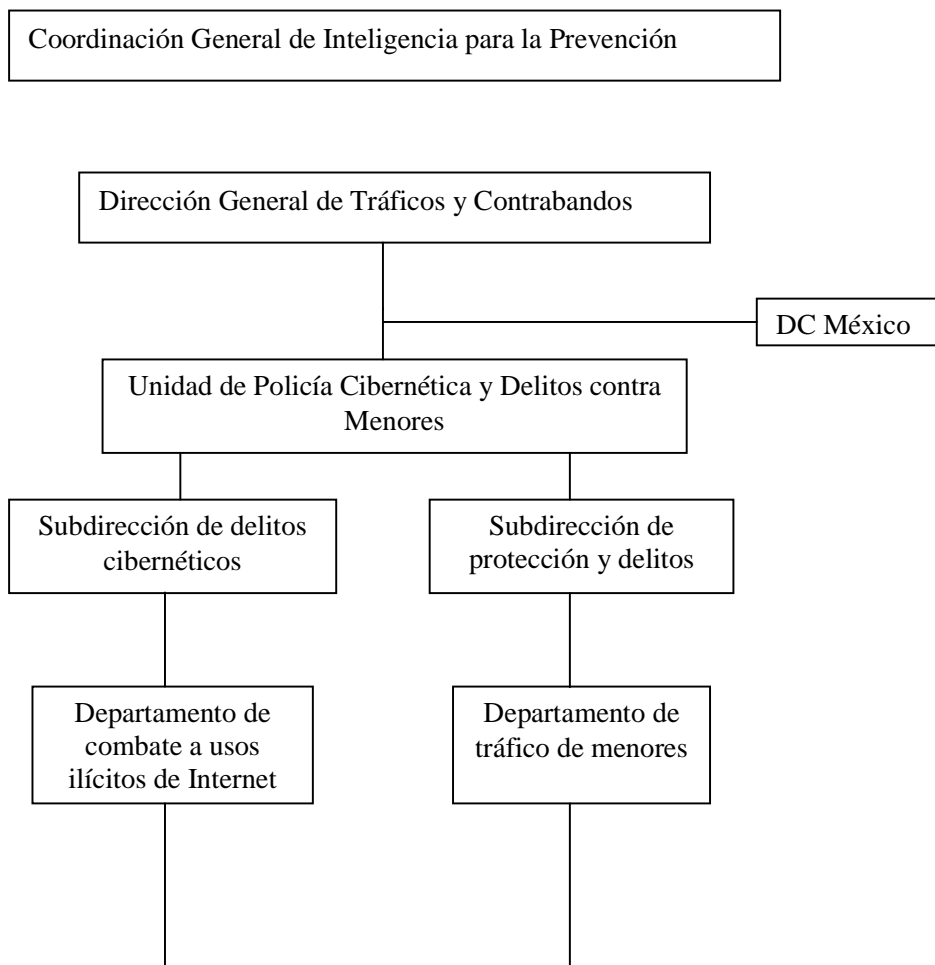
- Combatir la explotación sexual infantil;
- Atención a fraudes computacionales;
- Detección de intrusiones y robo de identidad;
- Analizar daños a sistemas;
- Identificar virus, gusanos, etc.;
- Detección de intrusos como *Hackers* y *Crackers*
- Proteger la infraestructura interinstitucional;
- Detección de sitios de alto riesgo criminal;
- Detección de espionaje industrial;
- Venta de drogas y armas;
- Combatir el terrorismo, *snuff* y crímenes violentos contra menores, y
- Combatir el robo, sustracción y tráfico de menores.

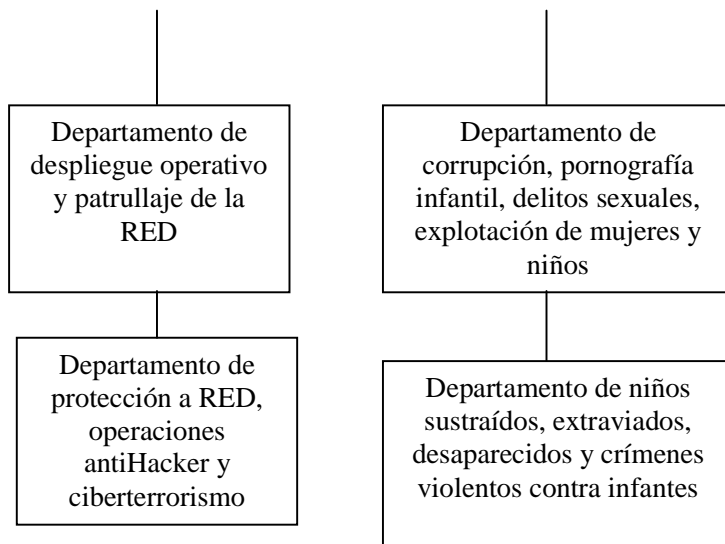
El 9 de diciembre de 2002, entró en operación la Unidad de Delitos Cibernéticos en México, teniendo como objetivo primordial garantizar la seguridad y la capacidad

preventiva reactiva para combatir ilícitos provocados por la acción humana en la red “internet”, es conveniente manifestar que esta unidad es un grupo de coordinación interinstitucional de delitos cibernéticos en los que participa el gobierno y la iniciativa privada, pues unen esfuerzos para combatir los delitos antes mencionados.

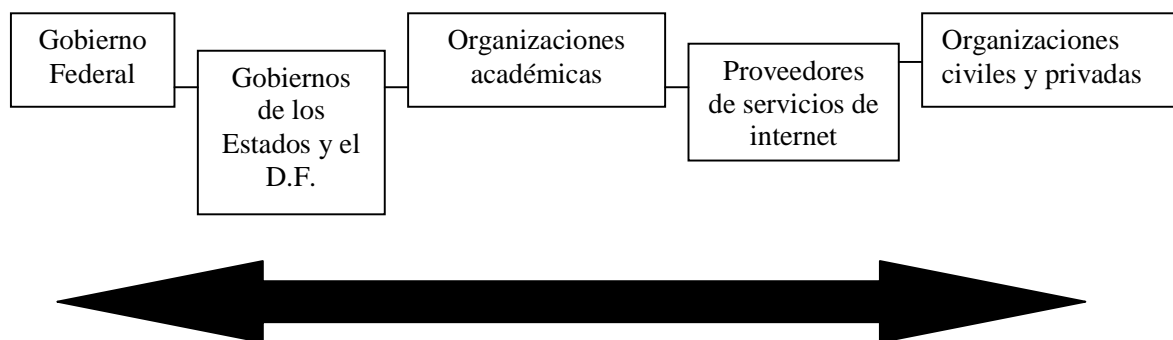
Su misión es la identificación, monitoreo, rastreo y localización de manifestaciones informáticas delictivas tanto en el territorio mexicano como fuera de él.

La estructura orgánica de la Unidad de Delitos Cibernéticos es la siguiente:





La estructura de la DC México o mejor conocida como “Delitos Cibernéticos México” es la siguiente:



Actualmente, la Policía Cibernética colabora con las siguientes instituciones en el mundo:

- *US Customs Cybermuggling Center (C3).*
- Servicio Secreto de los Estados Unidos de América.
- *Nacional Center for Missing & Exploited Children.*
- Brigada Tecnológica de España.

- *International Association of Law Enforcement Intelligence Analysts.*
- *High Technology Crime Investigation Association.*
- *APEC Counter-Terrorism Action plan: promoting cybersecurity.*
- *24/7 Task Force.*

Para la Policía Cibernética de la Policía Federal Preventiva, las tecnologías de la información desempeñan un papel importante en sus labores de investigación, por ejemplo, el patrullaje en la red de la Internet, rastreo de sitios web y comunidades, así como del monitoreo de las actividades de los grupos delictivos.

### **- Policías internacionales.**

#### **- Organización Internacional de Policía (INTERPOL).**

Actualmente, la “Comisión Criminal Internacional del Policía” conocida también como: “La Organización Criminal Internacional de la Policía - INTERPOL - es la organización internacional más grande de la policía del mundo ya que a ella se han afiliado más de 186 países miembros. Fue creado en 1923, con el objetivo de facilitar la cooperación fronteriza del policía, así como apoyar y asistir a todas las organizaciones, autoridades y servicios. Su misión más importante es prevenir o combatir el crimen internacional.

La Interpol procura facilitar la cooperación internacional del policía, sin embargo, no puede intervenir en actividades de índole política, militar, religiosa o racial.

Cada país miembro de la Interpol mantiene una Oficina Central Nacional (NCB) proveída de personal constituido por oficiales del Estado Miembros. El NCB es el punto de contacto señalado por la Secretaría General; las oficinas regionales son utilizadas como el punto de contacto entre el Estado Miembros de la Interpol cuando éstos requieren ayuda respecto a investigaciones de ultramar, así como la localización y aprehensión de fugitivos.

#### **- Oficina Europea de Policía (EUROPOL).**

El establecimiento de la Europol fue convenido en el tratado de *Maastricht* en la Unión Europea del 7 de febrero de 1992 en La Haya, Países Bajos, En la Europol comenzaron operaciones limitadas el 3 de enero de 1994 bajo la forma de unidad de las drogas de Europol (EDU). La Europol comenzó sus actividades el 1º de julio de 1999, y el día 1o. de enero de 2002, el mandato de Europol fue extendido al reparto con todas las formas serias de crimen internacional según lo enumerado en el anexo a la convención de Europol.<sup>192</sup> Todos los Estados Miembros ratificaron y entraron en la

---

<sup>192</sup> El anexo se refiere a lo previsto en el artículo 2 de la convención en donde se incluye la persecución de las siguientes conductas criminales: “*murder, grievous bodily injury - illicit trade in human organs and tissue - kidnapping, illegal restraint and hostage-taking - racism and xenophobia. Against property or public goods including fraud: organized robbery illicit trafficking in cultural goods, including antiquities and works of art swindling and fraud racketeering and extortion counterfeiting and product piracy forgery of administrative documents and trafficking therein forgery of money and means of payment computer crime corruption Illegal trading and harm to the environment: illicit trafficking in arms, ammunition and explosives, illicit trafficking in endangered animal species, illicit trafficking in endangered plant species and varieties, environmental crime illicit trafficking in hormonal substances and other growth promoters. In addition, in accordance with Article 2(2), the act of instructing Europol to deal with one of the forms of crime listed above implies that it is also competent to deal with the related money-laundering activities and the related criminal offences. With regard to the forms of crime listed in Article 2(2) for the purposes of this Convention: -"crime connected with nuclear and radioactive substances" means the criminal offences listed in Article 7(1) of the Convention on the Physical Protection of Nuclear Material, signed at Vienna and New York on 3 March 1980, and*

convención de Europol el 1 de octubre de 1998. Después de un número de actos jurídicos se relacionó con la convención, Europol comenzó sus actividades completas el 1 de julio de 1999.

La Europol apoya las actividades de la aplicación de ley de los Estados

Miembros principalmente contra:

- Tráficos de droga;
- Redes ilícitas de la inmigración;
- Terrorismo;
- Falsificación del dinero (euro) y otros medios de pago;
- Traficar con seres humanos incluyendo pornografía del niño;
- Traficar vehículos ilícitos, y
- Lavado de dinero.

Además, otras de las principales prioridades para la Europol incluyen el combate a los crímenes contra personas, los de índole financiero y los del *cybercrime* (Delitos Informáticos). Esto se aplica donde está implicada una estructura criminal organizada y que afectan dos o más Estados Miembros.

La Europol presta ayuda para desarrollar las siguientes actividades:

---

*relating to the nuclear and/or radioactive materials defined in Article 197 of the Euratom Treaty and Directive 80/836 Euratom of 15 July 1980”.*

- Facilitar el intercambio de información, de acuerdo con el derecho nacional, entre los oficiales del enlace de Europol (ELOs); ELOs es secundado a Europol por los Estados Miembros como representantes de sus agencias en la aplicación de Derecho Nacional;
- Para el análisis operacional en apoyo de operativos;
- Para la generación de los informes estratégicos para combatir la criminalidad a través del análisis del crimen en base a la información y de la inteligencia proveídas por los Estados Miembros.
- Proporcionar ayuda técnica para las investigaciones y las operaciones realizadas dentro de la Unión Europea, bajo la supervisión y responsabilidad legal de los Estados Miembros referidos.

La convención de Europol manifiesta que la misma establecerá y mantendrá un sistema automatizado de análisis de datos. La convención coloca un marco terminante para la protección de los derechos humanos y de los datos, el control, la supervisión y la seguridad.

El sistema informático de Europol (TECS) tiene tres componentes principales:

- Un sistema de información.
- Un sistema del análisis.
- Un sistema del índice.

Los sistemas del análisis y del índice ya están operando en los países europeos pues desde 2005 el sistema de información desarrollado (ES) es usado en Europol y desde octubre de 2005 está listo para ser utilizado por los Estados Miembros.

Puesto que el crimen organizado internacional no se detiene en las fronteras nacionales, la Europol, ha mejorado su cooperación internacional en la aplicación del Derecho mediante acuerdos operacionales o estratégicos bilaterales de negociación con otros Estados y organizaciones internacionales de países como: Bulgaria, Canadá, Colombia, *Eurojust*, Banco Central Europeo, Comisión de las Comunidades Europeas (OLAF incluyendo), Centro de Supervisión Europeo para las Drogas y el Apego de Droga, Islandia, Noruega, Rumania, Rusia, Suiza, Turquía, oficina de Naciones Unidas en las drogas y el crimen en los Estados Unidos de América.

La Europol tiene como objetivo el mejorar la eficacia y la cooperación de las autoridades competentes en los Estados Miembros para prevenir y combatir el terrorismo, tráfico de drogas ilegales y otras formas serias del crimen organizado internacional.

La Europol es financiada por contribuciones de los Estados Miembros según su Producto Interno Bruto, pudiendo señalarse que su presupuesto para el año 2006 fue de 63.4 millones de euros.

Las cuentas anuales de Europol se realizan mediante una intervención, ésta es realizada por el Comité Común de la Intervención, que se compone de tres miembros designados por Tribunal de Cuentas de las Comunidades Europeas.

Europol es responsable ante el Consejo de Ministros para la Justicia y los Asuntos Caseros. El Consejo es responsable de la dirección y del control de Europol; designa al director y a los diputados directores y aprueba el presupuesto; el Consejo de Ministros contiene representantes de todos los Estados Miembros, y el requisito para las ayudas unánimes de las decisiones aseguran un control democrático de Europol.

#### **- El Buró Federal de Investigaciones (FBI).**

El Servicio de Seguridad del Estado, *Federal Bureau of Investigation*, por sus siglas en inglés (FBI), es una división del Departamento de Justicia de los Estados Unidos, en una de las más poderosas e influyentes organizaciones en el mundo. Con más de 8,000 agentes especiales en el país tanto en grandes ciudades como en pueblos pequeños o fijos, tiene su sede en la ciudad de Washington, D.C., el FBI es responsable de aplicar cientos de leyes criminales federales. Entre los casos que investigan se encuentran: secuestros y robos a bancos, localización de fugitivos y análisis de fraudes contra el gobierno, también tiene jurisdicción sobre asuntos de inteligencia enemiga, por ejemplo: encontrar y apresar a espías extranjeros trabajando en los Estados Unidos, y en varias ocasiones en la historia Norte Americana cumplió como el mandato imprecisamente definido de proteger la llamada seguridad interna del país.

La División de Identificación del FBI, establecida en 1924, mantiene los archivos más extensos en huellas digitales, conteniendo más de 170 millones de huellas. Como laboratorio científico, establecido en 1932, sus servicios están disponibles a otras agencias de la aplicación de la ley.

El FBI mantiene varios sistemas de computadoras, el más común es llamado *National Crime Information Computer* (Computadora Nacional de Información Criminal (NCIC) que mantiene una base de datos de información acerca de cosas como vehículos robados, botes robados, personas desaparecidas, personas buscadas por la ley, registros de arrestos. Proporciona acceso rápido a dichos archivos sólo a agencias estatales, locales y federales de la aplicación de la ley, pero no permite que el público vea dichos archivos. El NCIC está directamente enlazado con el sistema de computadora TECS del Departamento de Hacienda y con muchos otros sistemas de computadoras Estatales.

Cuando un oficial de policía detiene un vehículo y no está seguro a quién va a encontrar cuando salga de la patrulla, él puede llamar por radio o simplemente usar la computadora de su patrulla para entrar en el sistema NCIC y en cuestión de pocos segundos puede encontrar si la persona que ha detenido es un fugitivo, o si tiene reporte de robo. Casualmente, ellos reciben casi 700,000 pedidos de ésta naturaleza todos los días en el sistema NCIC.

Cuando un agente de la policía arresta o investiga a un sujeto, éste suministra a la computadora del FBI con la mayor cantidad posible de la siguiente información: nombre y número de caso, alias o apodo, raza, sexo, estatura, peso, color de cabello, color de

ojos, descripción de cualquier marca de identificación, cicatriz, o tatuajes, fecha de nacimiento; lugar de nacimiento; número de Seguro Social, número de pasaporte, última dirección conocida; nacionalidad; si es naturalizado ciudadano de los Estados Unidos, fecha, lugar, y número del certificado; ocupación, la violación criminal por la cual éste sujeto es acusado; fecha de la orden judicial (*warrant*); tipo de orden judicial (*warrant*) - tribunal, magisterial, etc; agencia que tiene la orden judicial (*warrant*); cualquier información acerca de si el sujeto es considerado peligroso, si actualmente se conoce si posee un arma, o si tiene tendencias suicidas, o ha escapado previamente de la custodia; número de la licencia de conducir, año de expiración y Estado que lo otorgó; número de la licencia del vehículo, avión, o embarcación que el sujeto sea dueño o se sepa que usa, incluyendo el año y el Estado; descripción del vehículo, avión o embarcación que el sujeto sea dueño o se sepa que usa; asociados del sujeto; número del FBI, y nombre y teléfono de la persona a contactar cuando el sujeto es apresado.

Uno de los mayores problemas con el sistema es que la agencia que somete una entrada es responsable de mantenerla actualizada.

Otro sistema de computadora del FBI es su Sistema de Información de Soporte Investigativo (*Investigative Support Information System* <ISIS>). Este sistema sólo se usa para proporcionar soporte para investigaciones importantes que requieran el manejo de grandes volúmenes de información compleja. Está limitado a manejar un máximo de 20 casos a la vez.

El sistema ISIS fue utilizado durante la investigación del asesinato del Juez Federal John Wood en San Antonio, Texas. En éste caso, el FBI ingresó 300,000 piezas

de información, incluyendo 6,000 entrevistas, información de registro de hoteles de todos los hoteles del área, etc. El acusado, durante el juicio, afirmó que él se encontraba a varios cientos de millas lejos.

El FBI tiene un sistema llamado Sistema de Información del Crimen Organizado (*Organized Crime Information Systems*) (OCIS) cuyo antiguo director William Webster está “particularmente orgulloso”. El sistema empezó en 1980 en Detroit, Michigan y es uno de sus más sofisticados programas. El sistema es funcional en más de 40 ubicaciones.

El sistema OCIS fue utilizado en mayor investigación de heroína de la Mafia Siciliana, comúnmente referida como “*The Pizza Connection*” (La Conexión de la Pizza). De acuerdo a Webster, “OCIS brindó ayuda directa para cotejar información relativa a la intervención telefónica que la corte autorizó para el análisis del caso por un jurado de acusación”.

Actualmente todavía en desarrollo está el Sistema de Manejo de Información de Oficina de Campo (*Field Office Information Management System*) (FOIMS). El propósito de éste sistema es para automatizar totalmente las funciones administrativas y de registro de las oficinas de campo y residentes.

El sistema Carnívoro (*Carnivore*) del FBI se dio a conocer públicamente en Junio del 2000 a un selecto grupo de expertos de las industrias de la telecomunicación para

demostrar la habilidad del FBI para interferir teléfonos a solicitud de la Comisión Federal de Comunicaciones.

Utilizando personal externo para que instale en las computadoras servidores ISP, Carnívoro opera en un sistema de “olfateo” que puede analizar grandes pedazos de datos electrónicos mientras viajan por la Internet. Pero como el sistema Carnívoro que se basa en *Windows 2000* éste opera independientemente del resto de los sistemas de comunicación ISP, un ISP no puede monitorear las actividades de vigilancia del FBI y asegurar que estén cumpliendo con las órdenes de la Corte.

El FBI ha respondido también a la crítica pública de la habilidad del sistema de vigilancia diciendo que el sistema era necesario para sus investigaciones de espionaje, crimen organizado, y narcotráfico. De acuerdo a la página de Internet del FBI, el uso del sistema Carnívoro protegerá, no pondrá en peligro los derechos de privacidad de los ciudadanos: Esto es asunto de obtener legalmente por medio de nueva tecnología información importante mientras proveemos una mejor protección de la privacidad. El dispositivo Carnívoro proporciona al FBI la habilidad “quirúrgica” de interceptar y recolectar las comunicaciones que son objeto de órdenes legales e ignorar las comunicaciones a las que ellos no están autorizados a interceptar. Este tipo de herramienta es necesaria para satisfacer los requerimientos de los estatutos federales de intervención de las comunicaciones.<sup>193</sup>

Una de las libertades básicas en éste país es el derecho de la Primera Enmienda a la libertad de asociación. El Acta de Privacidad fue decretada para detener las

---

<sup>193</sup> [www.fbi.gov](http://www.fbi.gov)

invasiones a la privacidad por parte del gobierno, e incluir una provisión para que específicamente prohibiera la recolección de información respecto al ejercicio de actividades de la Primera Enmienda. El FBI y otras agencias gubernamentales ignoran totalmente tanto a la constitución americana como al acta de privacidad cuando recolectan y archivan información sobre los ciudadanos, incluso si esos ciudadanos no han cometido ningún crimen.

Puede decirse que el objetivo principal del FBI es la aplicación de la legislación federal, además de realizar labores de prevención e investigación de cualquier amenaza potencial contra del pueblo norteamericano, lo anterior sin importar el uso de cualquier método que esté a su alcance. De este objetivo se desprende que las técnicas y métodos utilizados por el FBI no siempre son legales y en ocasiones se atenta sobretodo con el derecho a la privacidad de las personas ya sean nacionales o extranjeros.

Sin embargo, es necesario reconocer el avance tecnológico con que cuenta el FBI para combatir el crimen organizado, ya sean en la capacitación de los miembros del buró o de los aparatos con que cuenta para realizar su trabajo el problema de lo anterior es que esas mismas herramientas de vanguardia pueden ser utilizadas para fines distintos como el espionaje, favoreciendo así a intereses personales de quienes se encuentran en el poder, utilizando recursos gubernamentales en agravio de los particulares.

#### **4.3.4. Políticas en la Criminalística Informática.**

Las políticas para la atención de los Delitos Informáticos versan sobre dos vertientes:

- a) La legal, y
- b) La técnica.

Sobre el aspecto legal ya se han hecho diversas reflexiones en torno a la creación de adecuadas legislaciones ley precisamente para mantener una seguridad jurídica sobre todo en la aplicación de la ley, tomando en consideración el ámbito de validez espacial de la ley penal tanto en el fuero común como en el federal, e inclusive el aspecto internacional, ya que el fenómeno de la delincuencia informática no guarda grandes diferencias en el mundo, pudiendo observar que no existen radicales diferencias respecto a las figuras jurídicas que cada país legisla para enfrentar esa problemática, no obstante de que existen países en donde el fenómeno informático puede encontrarse más desarrollado.

Dentro de este aspecto legal cabe reflexionar sobre la existencia de una legislación especializada para atender los fenómenos de la informática y de sus diversos ilícitos que son cometidos por una nueva delincuencia mundial.

Dentro de una defensa técnica podemos encontrar los medios de prevención, descubrimiento y obtención de pruebas del Delito Informático en cualquier lugar en donde existan computadoras y cuya información se quiera proteger.

Esta defensa puede ir desde simples recomendaciones sobre medidas de seguridad, hasta la creación de modernos sistemas de protección existiendo empresas que actualmente se dedican a ello.

No cabe la menor duda que una de las mejores estrategias para prevenir cualquier delito entre los que encontramos el Informático es la educación que se le de al sujeto pasivo para que se encuentre en aptitudes de realizar actos preventivos. Asimismo, también se debe enfocar la educación al sujeto activo de un delito para que tome conciencia de que no debe de cometer ningún ilícito, para lo cual también funge un gran papel la ley, ya que ésta encuentra su objetivo preventivo desde el momento que forma una amenaza para quienes pretendan llevar a cabo la comisión del ilícito.

La educación a la denuncia por la comisión de cualquier delito, para lo cual también cobra importancia todas las medidas que se adopten en la procuración de justicia, desde facilitar la propia presentación de la denuncia, agilizar el trámite de las comparecencias, así como el de las investigaciones las cuales deben de mantener la profesionalización correspondiente, para no convertir todo ello en una “calvario” para el denunciante quien a pesar de haber sufrido como víctima del delito, también lo hace en el transcurso de las indagatorias.

Dentro de una adecuada política criminal se debe tener siempre presente los siguientes objetivos:

- a) **La disuasión.** Consistente en inducir a los delincuentes a desistir de la comisión de ilícitos.
- b) **De prevención y detección.** En caso de que el sujeto decida cometer el delito, la autoridad debe de tener los medios necesarios para detectar la conducta ilícita y llevar a cabo lo necesario para prevenir su realización.
- c) **De prueba.** Consistente en la adecuada recopilación de pruebas que acredite la comisión de un delito, y que a nivel indagatorio se encuentre dirigido a la integración del cuerpo del delito y de la probable responsabilidad. En nuestro sistema jurídico el Derecho lo tiene el que lo sabe probar y en su momento.
- d) **Minimizar los riesgos.** Debiéndose simplificar la recuperación y corrección de los daños cometidos. Para la comisión de los Delitos Informáticos se debe elaborar frecuentemente copias de resguardo y protegerlas.
- e) **De respeto a la ley.** Toda política criminal debe estar siempre en respeto a la legislación correspondiente, así como la que tiene relación con el fenómeno respectivo.

En la actualidad diversas instituciones principalmente del gobierno y de naturaleza financiera han cobrado conciencia de la gravedad de la problemática informática estableciendo medidas preventivas tanto en su interior, así como con los usuarios de los respectivos servicios, que van desde la identificación de claves para los usuarios (NIP), hasta los más modernos sistemas de “encriptamiento” de la información.

Importante también es el avance tecnológico para descubrir la comisión de un Delito Informático y la detección del sujeto activo o delinciente, ya que como he

comentado la Informática avanza todos los días, la computadora considerada como la más moderna, ya no lo será en escasos meses, semanas o días, debiéndose actualizar a todos aquellos que intervienen en la procuración y también en la administración de justicia sobre esas técnicas que serán indispensables para conocer la verdad histórica de un ilícito y poder llegar exitosamente a convertirla en una verdad jurídica.

En nuestros días la información que pretende protegerse con los Delitos Informáticos es de gran importancia ya que es sabido en todas parte del mundo que quien se allega a ella tendrá una superioridad sobre los demás, sin embargo, ésta no debe alcanzarse de manera ilícita.

Como se ha visto la gran importancia de la informática no obstante su nueva aparición ha creado para las diversas actividades del ser humano facilitándole el acceso a los medios de información y que incluso han sido pocas las obras escritas que han manejado su problemática encontrando la mayor parte de su información presentada a través de ese medio conocido como Internet que es el que principalmente se ha utilizado en el desarrollo del presente Capítulo.

#### **4.4. La Procuración de Justicia en México en relación a los Delitos Informáticos.**

No obstante la intervención de la Policía Cibernética de la Policía Federal Preventiva cuya naturaleza en sus funciones radica en prevenir la comisión de Delitos Informáticos, también encontramos su apoyo para la localización de los delincuentes cibernéticos a aquellos órganos encargados de la procuración de justicia a nivel federal,

así como en las entidades federativas, que contemplan en sus legislaciones de alguna manera a esta clase de ilícitos en las diferentes acepciones que se han manejado, lo que ha originado que las diversas procuradurías les den también variados tratamientos.

Así, se les ha encomendado a áreas de las Procuradurías de justicia la investigación de ésta clase de delitos atendiendo a los bienes jurídicos mencionados, tales como la confidencialidad de la información, la integridad de los sistemas informáticos, o bien, de la gran gama de delitos que pueden ser cometidos asisténdose de medios informáticos, como los ilícitos patrimoniales de robo y fraude, los ambientales, los de corrupción de menores, en contra de la moral, etc...encargándose esa función en el ámbito federal a la Procuraduría General de la República a áreas como la Unidad Especializada en Investigación de delitos contra los Derechos de Autor y la Propiedad Industrial en donde se integran averiguaciones referentes a los ilícitos relacionados a derechos de autor, de propiedad industrial y de aquellos ilícitos informáticos relacionados con estas materias a la propia Subprocuraduría de Investigación Especializada en Delincuencia Organizada cuando por ejemplo se investigan delitos como los financieros, los de secuestro, los de corrupción de menores y pornografía infantil, etc; o bien a las llamadas Fiscalías como la de Delitos Financieros, de delitos no violentos, de delitos patrimoniales, entre otras; dándose similar tratamiento en las entidades federativas. No existiendo un área específica para la investigación de los delitos informáticos a nivel federal cuando el bien jurídico es la confidencialidad de la información.

Es menester que exista una definición clara sobre la competencia de las áreas que investiguen los Delitos Informáticos en los ámbitos federal y locales, toda vez que

ésta clase de delitos como se ha analizado guarda una problemática tanto jurídica y técnica, que no nada más impacta a las entidades federativas, o bien al ámbito federal, sino es un problema globalizado.

## CONCLUSIONES

**Primera.-** La historia de la Informática se remonta a los años 50s existiendo previamente a ello diversos aparatos que de manera rudimentaria facilitaba las labores del ser humano tales como las calculadoras, la llamada “máquina diferencial”, instrumentos para realizar operaciones a través de tarjetas perforadas, inclusive hasta llegar al rudimentario ábaco, llegando así hasta las computadoras que han sufrido múltiples modificaciones a través de las denominadas “Generaciones”, en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada.

Dicho avance ha implicado también una evolución cotidiana en el número de componentes de las computadoras recibiendo sus correspondientes denominaciones, situaciones que deben ser conocidas por los legisladores tanto para su debida regulación, así como para considerarlas al pretender formare algún tipo penal, ya que existen códigos punitivos en donde se incluyen tales conceptos como lo es el del Estado de Aguascalientes en donde prevé que la transgresión puede efectuarse a un programa de computación o software.

La Cibernética difiere a la Informática en que la primera trata de explicar y dar solución a eventos de control y comunicación ya sea de fenómenos acontecidos en la naturaleza, en la sociedad o producto de los hombres, mientras que la Informática pretende desarrollar máquinas capaces para que la Cibernética cumpla con sus objetivos pretendiendo desarrollar lo que se ha conocido como “Inteligencia Artificial”, reflejando un beneficio en las Ciencias Naturales, Sociales, así como en las diversas técnicas y en sí en todas las actividades del ser humano.

**Segunda.-** Las nuevas tecnologías en un mundo globalizado, siempre presentarán nuevos y dinámicos beneficios en cada aspecto de la vida humana pero también implica que nuevas formas delictivas surjan en días, que sin una legislación que prevea o al día en cuestión de estos aspectos, causarán que los nuevos problemas con nuevas tecnologías sean más difíciles de combatir,

La Internet ha venido a evolucionar la historia del hombre como lo fue el descubrimiento de la penicilina para la medicina, dándose su aplicación en actividades tales como en la comunicación, en la mensajería, en la información, entre otras más, convirtiéndose este sistema en una herramienta en beneficio del hombre y en cada unos de sus aspectos que lo rodean, pero siempre existirá el lado negativo que es resultado del crecimiento global, la facilidad que lleva su uso, y las malas intenciones de la personas, en el que una regulación global será un trabajo arduo ya que un país por si solo no podrá combatir, pero el primer paso para prevenir los delitos informáticos proviene de la educación y conocimientos de los usuarios.

**Tercera** La influencia de la Informática en el Derecho ha originado la existencia del denominado Derecho Informático enfocado a la protección de datos informáticos o la información concentrada en medios magnéticos o digitales, teniendo una gran relación con el Derecho a la Información, en el que se pretende regular el acceso a la libre información; siendo el Derecho Informático definido por Julio Téllez Valdez como “una rama de las ciencias jurídicas que consideran a la Informática como instrumento y objeto de estudio”; siendo el análisis de ambas de suma importancia para la regulación de los Delitos Informáticos.

Así, la Informática ha servido para facilitar sus variados campos de aplicación de las diversas ramas del Derecho, como sería la Civil, Mercantil, Administrativa, Laboral, Penal, entre otras, por lo que con ello el legislador adquiere una gran responsabilidad para la creación de normas jurídicas en cada uno de esos campos. Al respecto, existe una gran cantidad de operaciones jurídicas que se realizan a través de la Informática, así como facilitar el manejo de bibliografías jurídicas, criterios jurisprudenciales, entre otros productos jurídicos más se han concentrado en discos compactos o inclusive en pequeñas tarjetas de memoria conocidas como “USB”, así como facilitar su consulta a través de la Internet.

Se ha dado la existencia de proyectos para la creación de las llamadas “Ciberjusticia y de los “Cibertribunales”, los cuales serían temas importantes para ser tratados en investigaciones por separado, ya que se pudiera “deshumanizar” al Derecho y se le restaría la labor loable a aquellas personas que de alguna manera tienen la tarea de aplicar la ley a los casos concretos, debiéndose reflexionar aún más sobre estos puntos, sobre todo al considerar el origen romano-germánico del Derecho Mexicano, a diferencia de las propuestas hechas en países cuyo Derecho deriva del sistema anglosajón.

Dentro del Derecho Informático encontramos la preocupación de la protección jurídica de datos contenidos en los sistemas informáticos, así como de sus sistemas computacionales por lo que han surgido diversos intentos legislativos para tal efecto, incluyéndose la creación de tipos penales acerca de sus conductas antisociales.

**Cuarta.-** De acuerdo a la protección de diversos bienes jurídicos en la regulación jurídica de los delitos informáticos se han encontrado otras leyes con las que pudieran existir algunas contradicciones para su adecuada aplicabilidad; tal es el caso de la protección de los programas de computación (ejemplo el Estado de Sinaloa) , que también son protegidos por el propio Código Penal Federal con los delitos acerca de los derechos de autor, toda vez que son protegidos como obras por la Ley Federal del Derecho de Autor; así como cuando se refiere a la protección de la información contenida en medios informáticos, ya que ésta también se encuentra regulada por la Ley de Propiedad Industrial.

La Ley Federal de Transparencia y Acceso a la información Pública Gubernamental también pretende proteger a la información que poseen los Poderes de la Unión, por lo que será considerado una infracción administrativa cuando un servidor público quien la

transgreda conforme a las hipótesis señaladas en esa Ley entre las que encontramos usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida información que se encuentre bajo su custodia, entre otras conductas más. Sin embargo la aplicación de esta legislación es independiente de los ordenamientos penales.

**Quinta.-** En México se ha tenido la preocupación de legislar acerca de los Delitos Informáticos tanto a nivel federal como local ya que encontramos entidades federativas tales como la de Sinaloa y de Veracruz en donde se contemplan tipos penales en donde se pretende proteger la información contenida en los medios informáticos, existiendo además Estados como Aguascalientes (que hace referencia a la violación de programas de software o base de datos, así como de programas informáticos), Colima, Chiapas, Estado de México, Durango, Distrito Federal (con las reservas de ser una entidad federativa), Guerrero, Nuevo León, Quintana Roo, Tamaulipas, Morelos, Yucatán, Zacatecas, Tabasco, Jalisco y Baja California que han incluido en sus legislaciones diversas figuras delictivas que pueden ser cometidas a través de los sistemas computacionales, encontrando así ilícitos como el robo, fraude, falsificación de documentos, corrupción de menores, pornografía infantil, en contra de las vías de comunicación, secuestro, revelación de secretos, contra la moral pública y ambientales.

Las legislaciones penales que prevén los Delitos Informáticos y que han servido para realizar un análisis dogmático jurídico-penal son el Código Penal Federal y el Código Penal para el Estado de Sinaloa, contemplándose en el primero la protección a la información, mientras que en el segundo, además de esta protección también lo hace respecto a la integridad de los sistemas de cómputo, así como de ciertos delitos patrimoniales cometidos por medios computacionales.

Los Delitos Informáticos previstos en el Código Penal Federal pertenecen al grupo de los delitos referentes a la “revelación de secretos y acceso ilícito a sistemas y equipos de informática”, mientras que los contemplados en el Código Penal para el Estado de Sinaloa se encuentran en el título referente a los “delitos contra el patrimonio”.

**Sexta.-** La Dogmática Jurídico Penal a través de la Teoría del Delito sirve para estudiar a un delito como es el Informático, ya que se analizan todos y cada uno de sus elementos integradores para llevar a cabo su aplicación a los casos concretos, sobre todo por ser un ilícito de reciente creación.

Dentro de los elementos del Delito Informático la Tipicidad y su correspondiente Tipo Penal cobran gran importancia ya que las descripciones que hacen los legisladores Federal y del Estado de Sinaloa encontramos una diversidad de confusiones en sus descripciones que inclusive pudieran contraponerse con otras figuras delictivas como los del Derecho de Autor y los de propiedad industrial.

Hasta ahora se han considerado a los Delitos Informáticos como ilícitos no graves, sin embargo ante la gran problemática en el mundo de los hechos existe la tendencia de que en un futuro no muy lejano el legislador vea la necesidad de considerarlos como delitos

graves, a efecto de no permitir a los sujetos activos su libertad provisional, situación que debe de analizarse detenidamente.

Los delitos informáticos previstos en la legislación federal son perseguidos de oficio, mientras que los establecidos en el Código Penal para el Estado de Sinaloa su persecución es de querrela

Con fundamento en los tipos penales federal y del Estado de Sinaloa se realizó en éste trabajo un análisis pormenorizado de sus elementos tanto en su aspecto positivo como negativo, así como la vida de esos delitos conocida como *iter criminis* y el concurso de delitos y de personas que pueden aparecen en estos ilícitos informáticos que han sido cuestionados en éste trabajo.

**Séptima.-** Si bien es cierto, la delincuencia en todas sus inclinaciones ha avanzado en el uso de medios más modernos para realizar sus fines delictivos como lo es el uso de computadoras, también lo es que se deben modernizar las formas de combatirla, siendo el arma más adecuada el establecimiento de legislaciones acordes con esa problemática, tanto a nivel federal, local, así como internacional, toda vez que se está hablando de una delincuencia que se lleva a cabo en todos los rincones del mundo.

La problemática de la Delincuencia Informática ha sido tan complicado ya que como se ha mencionado el avance de la tecnología informática ha sido tan impresionadamente rápido que ese avance se ha reflejado en los medios computacionales utilizados por la delincuencia; avances que han aparecido en los sistemas para guardar información dentro de esos sistemas informáticos con una mayor seguridad utilizando el sistema conocido de “encriptación”, sin embargo la delincuencia se ha asistido de expertos en informática para violar esas seguridad, encontrando así a los denominados Hacker, Lamer, Wracker, Cracker, Phreaker Script-Kiddies, Speaker y Rider; delincuencia informática que ha generado en el mundo desde los años 70s grandes daños a personas en lo particular, a empresas, a entidades financieras y a los propios Estados, al grado tal que han existido posibilidades de conflagraciones internacionales, que h utilizado inclusive la Internet para facilitar sus diversas conductas ilícitas, asistiéndose de los llamados “viru”

**Octava.-** Dentro del mundo informático en la Internet ha surgido el llamado “Mundo Virtual” en el que se puede llevar a cabo una multiplicidad de operaciones “imaginarias” en las que el usuario puede ver cumplidos sus deseos que en el mundo real no pudiera llevar a cabo, como comprar inmuebles, barcos, edificios, participar en casinos, etc.. sin embargo, lejos de cumplir esos deseos satisfactoriamente pueden ser objetivos de la delincuencia informática o bien participar activamente en ella, a través de operaciones ilícitas relacionadas con robos, fraudes, pornografía infantil, narcotráfico, entre otras muchas más, además de recibir información distorsionada acerca del tabaquismo, medicinas, desórdenes alimenticios, etc...situaciones que debe considerar el legislador para establecer un adecuado marco jurídico.

También ha surgido el llamado “Terrorismo Cibernético” considerado por el Diccionario de la Real Academia Española como: “la actuación criminal de bandas organizada, que reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos”, encontrando ya en nuestra legislación penal federal a la figura del terrorismo.

Ese “Ciberterrorismo” a nivel internacional ha servido para realizar actos bandálicos como los suscitados en los ataques a las torres gemelas de Nueva York, en los Estados Unidos de América el 11 de septiembre de 2001, así como el de los trenes en Madrid España, el 11 de marzo de 2004.

Los sistemas financieros en todo el mundo se han visto afectados por la delincuencia informática para afectar a la economía mundial.

**Novena.-** Por ser un problema mundial la delincuencia informática ha sido regulada jurídicamente por diversos organismos internacionales entre los que encontramos a la O. N . U., el llamado “Grupo de los Ocho Países” y la Comisión de las Comunidades Europeas, siendo ésta última la que ha tenido mayores logros debido a la consolidación que han tenido los países europeos, creando convenios entre ellos como el de la “Ciber-criminalidad”, del 23 de noviembre de 2001, que precisa un marco jurídico avanzado en la materia. Dentro de esos países europeos España han establecido también una legislación detallada en cuanto al marco jurídico de los delitos informáticos.

Uno de los grandes problemas de toda clase de delincuencia es el de detectar el *modus vivendi* y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad encontramos a la Criminalística que enfocada a Los Delitos Informáticos va a ser indispensable para lograr la aprehensión del delincuente informático que utiliza los grandes avances tecnológicos para sus fines delictivos y que se oculta y huye a través de las líneas alámbricas e inalámbricas de esos sistemas computacionales.

Las investigaciones de los Delitos Informáticos han enfrentado grandes problemas de origen técnico de la Informática, así como en su grado de conocimiento de las personas de los diversos sectores en donde se comete esta clase de ilícitos, así como de quienes se encargan de la procuración y administración de justicia, y de quienes establecen su marco normativo.

**Décima.-** La Policía es de gran importancia para la investigación de los delitos, y los informáticos no son la excepción, por lo que surge a nivel internacional en diferentes países la “Policía Cibernética”, que deberá utilizar todos los conocimientos en Informática para localizar y detener al delincuente informático.

En México encontramos la existencia de la “Policía Cibernética” en la estructura de la Policía Federal Preventiva a partir del año 2000 que dentro de sus objetivos es combatir a la corrupción de menores y a la delincuencia informática, coordinándose con otras corporaciones policiales en los Estados de la República Mexicana, así como a nivel internacional.

A nivel internacional destacan grupos policiales en contra de la delincuencia informática tales como: la INTERPOOL, la EUROPOL y el FBI.

Las políticas en la Criminalística Informática se encuentran siempre avanzando y van dirigidas principalmente a cubrir las vertientes legal y técnica.

En México, la Procuraduría General de la República y las procuradurías de cada uno de los Estados que de alguna manera contemplan en sus legislaciones a los Delitos Informáticos en los diversos enfoques que se han señalado durante la presente investigación acordes a los bienes jurídicos que se pretende proteger (integridad de los sistemas informáticos o ilícitos cometidos por medios informáticos), han venido realizando sus actividades para integrar tales ilícitos en áreas especialidades como: la de delitos de derechos de autor, financieros, patrimoniales, delitos no violentos, e inclusive en la propia Subprocuraduría de Investigación Especializada en Delincuencia Organizada, enfrentándose a las problemáticas jurídicas y técnicas que se han comentado; sin existir concretamente un área a nivel federal encargada de los Delitos Informáticos cuando el bien jurídico es la confidencialidad de la información.

## **PROPUESTAS.**

**1.-** No cabe duda que uno de los factores más importantes para prevenir y combatir a los delitos es necesaria la educación a todos los niveles; en cuanto a los ilícitos informáticos en donde se involucra una interrelación de Ciencias como sería el Derecho, la Informática, la Cibernética, entre otras más, las cuales avanzan constantemente y en donde existen conocimientos tan amplios que deben llegar a todo a aquél que tenga que ver con las actividades informáticas en donde pueden estar involucrados a particulares, escuelas, empresas, entidades financieras, a los propios Estados y en sí, a todo a aquél que utilice una computadora.

**2.-** El legislador es un personaje que debe contar con toda la educación que le pueda aportar el Derecho Informático, y conjuntamente con esos conocimientos y la realidad social que pretende regular, formular una adecuada legislación entorno a su problemática dentro de todas las ramas de Derecho, ya que la Informática ha venido a asistir al ser humano en todas sus actividades. Por lo que respecta en el Derecho Penal y crear figuras delictivas hacerlo con toda la técnica legislativa.

**3.-** Es conveniente se limite la competencia para que se legisle en materia de delitos informáticos, considerando que pudiera darse la exclusividad federal, tanto en la protección de los bienes jurídicos relativos a la confidencialidad de la información contenida en medios informáticos, como cuando se atente en contra de éstos, siendo que su uso pudiera considerarse también dentro de la legislación federal, debido a que la especial naturaleza en su novedosa tecnología, así como de la Internet implican un medio de comunicación globalizado, y en el caso de los ilícitos informáticos, éstos son cometidos desde distintas partes de la Federación Mexicana para tener efectos en otros rincones de la misma, o inclusive del mundo, originándose con ello una legislación uniforme para todo el país, evitándose así posibles contradicciones con otras legislaciones, y así combatir con mayor facilidad esta clase de delitos.

**4.-** Dentro de la legislación penal a definir debe hacerse una clara distinción de los ilícitos informáticos conforme a los bienes jurídicos que se pretende tutelar, ya sea cuando se hace mención a la confidencialidad de la información contenida en medios informáticos, en relación a la protección de éstos medios informáticos, o bien cuando se refieren a otra clase de delitos cometidos por medios informáticos, debiéndose asistir de la Dogmática Jurídico-Penal.

**5.-** Se deben establecer políticas especializadas para combatir las diversas conductas antisociales realizadas por medios informáticos que pueden incurrir en infracciones o inclusive delitos, por lo que su atención debe ser en los tres poderes tanto el legislativo, ejecutivo y judicial.

**6.-** El gobierno debe tener una activa participación en este flagelo en donde se coordinen instituciones tanto del ámbito federal tales como la Procuraduría General de la República, la Secretaría de Seguridad Pública, la Secretaría de Gobernación, etc.. y sus homólogas en las entidades federativas, y no sólo adopten un papel de observadores.

**7.-** La Policía Cibernética debe contar con elementos altamente capacitados bajo los principios de la Policía Científica, asistiéndose tanto del Derecho Informático como de las diversas Ciencias auxiliares, disciplinas y artes que le ayuden para la localización y detención del delincuente informático que puede ser a nivel internacional, toda vez que debe hacerlo a través de los medios utilizados de los sistemas computacionales, situación sumamente difícil en comparación de la persecución de un delincuente que ha asaltado un banco con un arma de fuego.

**8.-** Es necesario que México pertenezca a organismos internacionales para llevar a cabo el combate de todo tipo de delincuencia que se da a nivel globalizado como la organizada, la financiera, el terrorismo, así como la informática, manteniendo siempre los principios constitucionales y las directrices en las que se ha mantenido nuestro sistema jurídico mexicano.

**9.-** Para una adecuada legislación de los Delitos Informáticos no nada más deben contemplarse posibles reformas o adecuaciones a los Códigos Penales, en sus correspondientes apartados, sino modificar otros textos legales como serían la Ley Federal del Derecho de Autor, la Ley de la Propiedad Industrial, entre otras, a efecto de que no se presten a posibles confusiones; y delimitar así los bienes jurídicos que deben ser protegidos por los ilícitos informáticos.

Por lo anterior se considera que debe ser exclusivo de esta clase de delitos solamente la “confidencialidad de la información protegida por sistemas informáticos”, tal y como se aproxima a ello el Código Penal Federal, sin embargo, podría modificarse el artículo 211 bis 1 de este Ordenamiento vigente, de la siguiente manera:

**Artículo 211 bis 1.- Al que sin autorización conozca, copie, altere o dañe la información contenida en sistemas o equipos de informática se le impondrá de dos a cuatro años de prisión y de doscientos a cuatrocientos días multa.**

**10.-** La información de datos ha sido considerada tan importante en nuestros días que deben existir acciones conjuntas entre los diversos niveles del gobierno y la iniciativa privada para su protección. Al respecto es paradójico pensar que el costo de un disquete es de 5 pesos, el de un disco compacto es de 3 pesos, el costo de un dvd de 10 pesos, el costo de una memoria de 1gb de capacidad es de 100 pesos, una computadora desde 5mil pesos, el costo de salario mínimo en México máximo de 50 pesos diarios, sin embargo, que se apoderen, alteren o dañen de información vital almacenada de cualquiera de estos dispositivos que posiblemente sea información vital de una empresa, un trabajo, o incluso una idea que pueda generar millones, no tiene precio.

## FUENTES DE CONSULTA.

### **BIBLIOGRAFÍA**

1. AZPILCUETA HERMILIO, Tomas. **Derecho Informático**. Editorial Abeledo-Perrot Buenos Aires Argentina 1996.
2. CÁMPOLI, Gabriel Andrés. **Derecho Penal Informático en México**. Editorial INACIPE, México 2004.
3. CARRANCÁ Y TRUJILLO, Raúl y CARRANCÁ Y RIVAS, Raúl. **Derecho Penal Mexicano. (Parte general)**. Vigésima tercera edición. Editorial Porrúa. México 2007.
4. CASTELLANOS TENA, Fernando. **Lineamientos elementales de Derecho Penal. (Parte General)**; Cuadragésima séptima edición actualizada por Horacio Sánchez Sodi, primera reimpresión. Editorial Porrúa, México 2007.
5. CORREA, CARLOS M. Carlos, **Derecho Informático**. Editorial Desalma Buenos Aires Argentina 1994.
6. CUELLO CALÓN, Eugenio. **Derecho Penal. Parte General**. Décima octava edición. Editorial Nacional. México 1980.
7. HASKIN, David. **Multimedia fácil**. (Traducción. Sánchez García Gabriel). Editorial Prentice Hall. México 1995.
8. JIMÉNEZ DE ASÚA, Luis. **La Ley y el Delito**. Décima primera edición, Editorial Sudamericana, Buenos Aires Argentina. Mayo 1980.
9. JIMÉNEZ DE ASÚA, Luis. **Tratado de Derecho Penal**. Tomo III, Tercera edición actualizada. Editorial Losada, S.A. Buenos Aires 1965.
10. JIMÉNEZ HUERTA, Mariano. **Derecho Penal Mexicano**. Tomo I. Quinta edición, Editorial Porrúa. México 1992.
11. LÓPEZ BETANCOURT, Eduardo. **Teoría del delito**. Décima cuarta edición. Editorial Porrúa, México 2007.
12. MALO CANACHO, 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.

13. MÁRQUEZ PIÑERO, Rafael. **Derecho Penal. Parte General.** Cuarta edición. Primera reimpresión agosto 1999. Editorial Trillas. México 2006.
14. MATEOS MUÑOZ, Agustín. **COMPENDIO DE ETIMOLOGÍAS GRECO-LATINAS DEL ESPAÑOL.** Editorial Esfinge. Cuadragésima sexta edición. México 2007.
15. MEZGER, Edmundo. **Tratado de Derecho Penal.** Tomo I. Traducción de J. Arturo Rodríguez Muñoz. Editorial Revista de Derecho Privado. Madrid España 1955.
16. MONTIEL SOSA, Juventino. **Criminalística.** Editorial Limusa. Segunda edición México 2007.
17. MORENO MARTÍN, Arturo. **Diccionario de Informático y telecomunicaciones ingles y español.** Editorial Ariel Barcelona 2001.
18. MUÑOZ CONDE, Francisco. **Teoría general del delito.** Segunda edición. Editorial Toblandú. 2005.
19. PAVÓN VASCONCELOS, Francisco. **Manual de Derecho Penal Mexicano.** Décima edición debidamente corregida y puesta al día. Editorial Porrúa. México 1991.
20. PORTE PETIT CANDAUDAP, Celestino. **Apuntamientos de la parte general de Derecho Penal.** Vigésima edición. Editorial Porrúa. México 2003.
21. 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.
22. REYNOSO DÁVILA, Roberto. **Teoría general del delito.** Sexta edición. Editorial Porrúa. México 2006.
23. RODAO, Jesús de Marcelo. **Piratas cibernéticos. cyberwars, seguridad Informática e Internet.** Editorial- Ra-ma. España 2005.
24. ROJAS AMANDI, Víctor Manuel. **El uso de la Internet en el derecho.** Segunda Edición. Editorial Oxford, México 2001.
25. TÉLLEZ VALDÉS, Julio. **Derecho Informático.** Tercera Edición. Editorial Mc Graw Hill, México 2003.
26. TORRES LÓPEZ, Mario Alberto; **Las leyes penales.** Editorial Porrúa. Quinta Edición. México 2005.
27. VILLALOBOS, Ignacio. **Derecho Penal Mexicano.** Quinta edición. Editorial Porrúa. México 1990.

28. ZAFFARONI EUGENIO, Raúl. **Manual de Derecho Penal**. Segunda edición. Editorial Cárdenas. México 2007.

### **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.

### **RESOLUCIONES JUDICIALES.**

1. Resolución del juicio de amparo en revisión 703/2004, de la Primera Sala de la Suprema Corte de Justicia de la Nación de fecha 25 de enero de 2005. Plasmada en la tesis de Jurisprudencia 5/2008 cubro rubro dice "ATAQUES A LAS VÍAS DE COMUNICACIÓN. LA FRACCIÓN II DEL ARTÍCULO 171 DEL CÓDIGO PENAL FEDERAL QUE PREVEÉ ESE DELITO, VIOLA LOS PRINCIPIOS DE EXACTA APLICACIÓN Y RESERVA DE LEY EN MATERIA PENAL".

### **LEGISLACIONES**

**(Consultadas en las páginas de Internet del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México y de la Suprema Corte de Justicia de la Nación [www.juridicas.unam.mx/infju/leg/](http://www.juridicas.unam.mx/infju/leg/) [www.scjn.gob.mx-sepreamacorte](http://www.scjn.gob.mx-sepreamacorte) [www.diputados.gob.mx/leyesbiblio/](http://www.diputados.gob.mx/leyesbiblio/))**

2. Constitución Política de los Estados Unidos Mexicanos.
3. Código Penal Federal.
4. Ley Orgánica del Poder Judicial de la Federación.
5. Ley Federal del Derecho de Autor.
6. Ley de la Propiedad Industrial.
7. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

8. Código Penal para el Distrito Federal.
9. Código Penal para el Estado de Sinaloa.
10. Legislación Penal para el Estado de Aguascalientes.
11. Código Penal del Estado de Colima.
12. Código Penal del Estado Libre y Soberano de Chiapas.
13. Código Penal del Estado de México.
14. Código Penal del Estado de Durango.
15. Código Penal del Estado de Guerrero.
16. Código Penal para el Estado de Nuevo León.
17. Código Penal del Estado de Quintana Roo.
18. Código Penal para el Estado de Tamaulipas.
19. Código Penal del Estado de Colima.
20. Código Penal para el Estado de Morelos.
21. Código Penal para el Estado de Yucatán.
22. Código Penal para el Estado de Zacatecas.
23. Código Penal del Estado de Tabasco.
24. Código Penal para el Estado Libre y Soberano de Jalisco.
25. Código Penal para el Estado de Baja California.
26. Código Penal para el Estado de Coahuila de Zaragoza.
27. Código Penal para el Estado de Guanajuato.
28. Código Penal para el Estado de Nuevo León.
29. Código Penal para el Estado Libre y Soberano de Veracruz-Llave.

## **MEDIOS ELECTRÓNICOS**

1. **LA HISTORIA QUE LLEVO A CONSTRUIR LA PRIMERA COMPUTADORA.** [com/trabajos14/histcomput/histcomput2.shtml](http://trabajos14/histcomput/histcomput2.shtml)
2. <http://es.wikipedia.org/wiki/Internet#Historia>
3. CASTILLO GARCÍA, Gustavo. **Internet es usada ya por narcos para comprar armamento:** PGR La Jornada  
<http://www.jornada.unam.mx/2005/06/13/012n1pol.php>
4. GUTIÉRREZ CORTÉS, Fernando e ISLAS CARMONA, Octavio. **Apuntes académicos para una historia de internet en México.** [.www.mexicanadecomunicacion.com.mx/tables/FMB/foromex/apuntes.html](http://www.mexicanadecomunicacion.com.mx/tables/FMB/foromex/apuntes.html).
5. 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>
6. Internet Society. **HISTORIA DE LA INTERNET EN MÉXICO.** <http://www.isocmex.org.mx/historia.html>
7. NIC-México, **HISTORIA DE NIC-MÉXICO,** <http://www.nic.mx/es/NicMexico.Historia>
8. EMBL HEIDELBERG, EUROPEAN MOLECULAR BIOLOGY LABORATORY. <http://www.embl-heidelberg.de/>
9. **INTERNATIONAL NUCLEOTIDE SEQUENCE DATABASE COLLABORATION** <http://www.ncbi.nlm.nih.gov/projects/collab/>
10. **VIRTUAL MAGISTRATE:** <http://www.vmag.org/>
11. **THE ONLINE OMBUDS OFFICE:** <http://www.ombuds.org/center/ombuds.html>
12. **ERESOLUTION:** <http://www.udrpinfo.com/eres/>
13. **Constitución.Española** [http://www.constitucion.es/otras\\_constituciones/espana/index.html](http://www.constitucion.es/otras_constituciones/espana/index.html)
14. **CONVENIO Nº 108 DEL CONSEJO, de 28 de Enero de 1981, DE EUROPA PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL** <http://www.apdcat.net/media/246.pdf>
15. OECD, **COMPUTER RELATED CRIMINALITY: ANALYSIS OF LEGAL POLICY IN THE OECD AREA.** ICCP, 84:22, 1984.

16. <http://es.wikipedia.org/wiki/Informaci3n>
17. <http://www.matuk.com/teclado/1998/abr-27-1998.html>
18. <http://www.lared.com.ve/archivo/Hacker31.html>
19. <http://www.cnn.com/TECH/computing/9803/19/Hackers/>
20. <http://www.lared.com.ve/archivo/Hacker38.html>
21. <http://www.lared.com.ve/archivo/Hacker39.html>
22. <http://www.lared.com.ve/archivo/Hacker51.html>
23. <http://www.vsantivirus.com/adore.htm>
24. <http://news.bbc.co.uk/1/hi/wales/1248136.stm>
25. Wikipedia Enciclopedia Libre, Realidad Virtual.  
[http://es.wikipedia.org/wiki/Realidad\\_virtual](http://es.wikipedia.org/wiki/Realidad_virtual)
26. EverQuest Official Site. <http://everquest.station.sony.com/>
27. Final Fantasy XI US Official Site <http://playonline.com/>
28. World of War Craft Official Site <http://www.wow-esp.com/>
29. Star Wars Galxies Online Oficial Site <http://www.starwarsgalaxiesonline.com/>
30. Second Life Official Site. [http://secondlife.com/whatis/economy\\_stats.php](http://secondlife.com/whatis/economy_stats.php).
31. Wikipedia Enciclopedia Libre, Second Life. [http://es.wikipedia.org/wiki/Second\\_life](http://es.wikipedia.org/wiki/Second_life)
32. México SL, Comunidad Mexicana de Second Life.  
[http://www.hosteltur.com/noticias/43683\\_mexico-second-life.html](http://www.hosteltur.com/noticias/43683_mexico-second-life.html) .
33. Second Life Official Site. [http://secondlife.com/whatis/economy\\_stats.php](http://secondlife.com/whatis/economy_stats.php).
34. El Diccionario de la Real Academia Española, en su versi3n 2003  
[http://es.wikipedia.org/wiki/Terrorismo#\\_note-0](http://es.wikipedia.org/wiki/Terrorismo#_note-0)
35. Embajada de los Estados Unidos de Am3rica en M3xico. **¿QU3 ES TERRORISMO?**.  
[http://www.usembassy-mexico.gov/bbf/bfdossierS\\_Terrorismo\\_quees.htm](http://www.usembassy-mexico.gov/bbf/bfdossierS_Terrorismo_quees.htm)
36. CRS Report for Congress. Wilson, Clay. **COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS**, Updated April 1 2005. Pag. 11.  
<http://openocrs.cdt.org/document/RL32114>.

37. Duch, Juan Pablo. **Busca Estonia y Rusia una solución negociada al conflicto que los enfrentan.** Periódico La Jornada, México 5 de Mayo de 2007.
38. <http://www.jornada.unam.mx/2007/05/05/index.php?section=mundo&article=030n1mun>
39. El País.com, **La crisis entre Estonia y Rusia llega a Internet.** Madrid, España. 17 de Mayo de 2007. [http://www.elpais.com/articulo/internet/crisis/Estonia/Rusia/llega/Internet/elpepunc/20070517elpepunc\\_4/Tes](http://www.elpais.com/articulo/internet/crisis/Estonia/Rusia/llega/Internet/elpepunc/20070517elpepunc_4/Tes)
40. Meeting of G8 Justice and Home affairs ministers, "Sea Island Summit 2004" <http://www.cybercrime.gov/g82004/index.html>
41. <http://www.unifr.ch/derechopenal/legislacion/es/cpespidx.html>
42. **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>
43. ANEI, Asociación Nacional de Empresa, España. **Directiva 95/46CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos .** [http://www.anei.org/documentos/Dir\\_9546CE.pdf](http://www.anei.org/documentos/Dir_9546CE.pdf)
44. Eur-LEx, Directiva 93/34CE. [http://eur-lex.europa.eu/LexUriServ/site/es/oj/1998/l\\_204/l\\_20419980721es00370048.pdf](http://eur-lex.europa.eu/LexUriServ/site/es/oj/1998/l_204/l_20419980721es00370048.pdf)
45. Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, [www.mityc.es/NR/rdonlyres/62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva\\_2000\\_31\\_CE.pdf](http://www.mityc.es/NR/rdonlyres/62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva_2000_31_CE.pdf)
46. Área del Derecho civil de la Universidad de Girona, España. <http://civil.udg.es/normacivil/estatal/contract/LSSI.htm>

El anexo se refiere a lo previsto en el artículo 2 de la convención en donde se incluye la persecución de las siguientes conductas criminales: *"murder, grievous bodily injury - illicit trade in human organs and tissue - kidnapping, illegal restraint and hostage-taking - racism and xenophobia.*

*Against property or public goods including fraud: organized robbery illicit trafficking in cultural goods, including antiquities and works of art swindling and fraud racketeering and extortion counterfeiting and product piracy forgery of administrative documents and trafficking therein forgery of money and means of payment computer crime corruption*  
*Illegal trading and harm to the environment: illicit trafficking in arms, ammunition and explosives, illicit trafficking in endangered animal species, illicit trafficking in endangered plant species and varieties, environmental crime illicit trafficking in hormonal substances and other growth promoters. In addition, in accordance with Article 2(2), the act of instructing Europol to deal with one of the forms of crime listed above implies that it is also competent to deal with the related money-laundering activities and the related*

*criminal offences. With regard to the forms of crime listed in Article 2(2) for the purposes of this Convention:*

*-"crime connected with nuclear and radioactive substances" means the criminal offences listed in Article 7(l) of the Convention on the Physical Protection of Nuclear Material, signed at Vienna and New York on 3 March 1980, and relating to the nuclear and/or radioactive materials defined in Article 197 of the Euratom Treaty and Directive 80/836 Euratom of 15 July 1980".*

www.fbi.gov

## **HEMEROGRAFÍA**

1. **ESTADÍSTICA SOBRE DISPONIBILIDAD Y USO DE TECNOLOGÍA DE INFORMACION Y COMUNICACIONES EN LOS HOGARES. INEGI. México 2005.**