UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

"IMPORTANCIA DE LA CREACIÓN DE UN MARCO JURÍDICO APLICABLE A LA INFORMÁTICA, PARA UNA ADECUADA PREVENCIÓN Y SANCIÓN DE LOS DELITOS INFORMÁTICOS.

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADA EN DERECHO

P R E S E N T A :

VANESSA ANDREA LUNA MONTELONGO

Director de Tesis:
LIC. BERTHA PATRICIA GÓMEZ GONZÁLEZ

Revisor de tesis:
LIC. HÉCTOR MANUEL ESTEVA DÍAZ

BOCA DEL RIO, VER. 2001

TESIS
FALLA
DE
ORIGEN

PAGINACION

DISCONTINUA

A Dios:

Gracias Señor por darme la vida y por guiar cada uno de mis pasos por el camino del bien. Mi fé en tí es la fuerza que inspira a ser mejor cada día y a conseguir mis más anhelados sueños.

A mis padres:
Lic. Ernesto Luna Duarte y
Arcadia Montelongo de Luna.

En agradecimiento al inmenso amor y cariño que me han brindado a lo largo de toda mi vida.. Gracias por su apoyo incondicional, por su paciencia y su comprensión y por hacer de mí quien soy hoy.
Son mi ejemplo a seguir.
Los adoro.

A mis hermanas:
Mariela y Yahaira.

Mis más fieles amigas y confidentes.
Gracias por llenar mi vida de amor y alegría,
y por compartir a mi lado los más lindos momentos de mi existencia.
Que Dios las bendiga.

A mis abuelitos :
Ernesto ✞ y Valentín ✞

A ustedes con mucho cariño hasta donde quiera que se encuentren.
Gracias por velar mis sueños.

A mis abuelitas, tíos (as), primos (as):

Gracias por formar parte importante de mi vida, y por brindarnos felicidad y cariño a mí y a mi familia.
Los quiero mucho.

A mis mejores amigas:
Vanessa✞, Ivón, Bertha y Jenny.

En nombre de la más pura y bella amistad que se pueda llegar a imaginar.
Gracias por compartir a mi lado todos los buenos y malos momentos, y por hacer de cada uno de ellos algo especial.
Les deseo lo mejor hoy y siempre.

A mis demás amigos y compañeros:

Gracias por su apoyo, por su amistad y cariño,
y por hacer de esta etapa de mi vida una
experiencia inolvidable.

A mi Directora, Catedráticos y en general,
a todos y cada una de las personas que colaboraron
conmigo para lograr mi más anhelado sueño:

Gracias por transmitirme sus invaluables
conocimientos y su experiencia, pero sobre todo
por sus sabios consejos y su paciencia.
A todos y cada uno de Ustedes mi
más profundo agradecimiento.

A Shaky:

Por tu compañía fiel y tu inmensa ternura.
Gracias por hacerme sentir alguien
especial. Te quiero mucho.

INDICE

INTRODUCCIÓN	1
CAPÍTULO I METODOLOGÍA DE LA INVESTIGACIÓN.	
1.1. PLANTEAMIENTO DEL PROBLEMA.	4
1.2. JUSTIFICACIÓN DEL PROBLEMA.	4
1.3. DELIMITACIÓN DE OBJETIVOS.	5
1.3.1. Objetivo General.	5
1.3.2. Objetivos Específicos.	5
1.4. FORMULACIÓN DE LA HIPÓTESIS.	6
1.5. IDENTIFICACIÓN DE VARIABLES.	6
1.5.1. Variable Independiente.	6
1.5.2. Variable Dependiente.	6
1.6. TIPO DE ESTUDIO.	7
1.6.1. Investigación Documental.	7
1.6.1.1. Bibliotecas Públicas.	7
1.6.1.2. Bibliotecas Privadas.	7
1.6.2. Técnicas Empleadas.	8
1.6.2.1. Fichas Bibliográficas.	8
1.6.2.2. Fichas de Trabajo.	9
CAPÍTULO II MARCO HISTÓRICO-LEGAL DEL FENÓMENO INFORMÁTICO.	
2.1. FENÓMENO INFORMÁTICO.	10
2.1.1. La Cibernética.	10
2.1.2. La Informática.	11

2.1.3. Diferencias entre Cibernética e Informática. 13
2.1.4. Orígenes y Evolución Histórica de las Computadoras. 14
2.2. IMPLICACIONES DE LA INFORMÁTICA EN LA SOCIEDAD. 17
2.2.1. Implicaciones Positivas y Negativas. 17
2.2.2. Principales usos de las computadoras en la Sociedad. 19
2.3. INCIDENCIA DE LA INFORMÁTICA EN EL DERECHO. 20
2.3.1. Derecho Informático. 20
2.3.1.1. Antecedentes. 22
2.3.1.2. Concepto y clasificación. 24
2.3.2. Informática Jurídica. 25
2.3.2.1. Antecedentes y Evolución. 27
2.3.2.2. Concepto. 29
2.3.2.3. Clasificación. 31
2.3.3. Derecho de la Informática. 32
2.3.3.1. Antecedentes y Evolución. 33
2.3.3.2. Concepto. 36
2.3.3.3. Fuentes. 37
2.3.4. Política Informática en México. 39
2.3.5. Legislación Informática en México. 41

CAPÍTULO III DELITOS INFORMÁTICOS.
3.1. GENERALIDADES DEL DELITO. 45
3.1.1. Definición del término "delito". 45
3.1.2. Concepto jurídico del término "delito". 47
3.1.3. Elementos positivos y negativos del Delito. 49
3.2. GENERALIDADES DE LOS DELITOS INFORMÁTICOS. 53
3.2.1. Orígenes. 53
3.2.2. Concepto. 54
3.2.3. Características. 57
3.2.4. Clasificación. 59

3.2.5. Bien jurídico tutelado en los delitos informáticos. 65
3.2.6. Perfil criminológico del sujeto activo de los delitos informáticos. 70
3.2.7. El sujeto pasivo en los delitos informáticos. 73
3.3. CONDUCTAS DELICTIVAS TÍPICAS EN LOS DELITOS INFORMATICOS. 74
3.3.1. Tipos de conductas y sus características. 74

CAPÍTULO IV MARCO JURÍDICO APLICABLE A LOS DELITOS INFORMÁTICOS.
4.1. REGULACIÓN JURÍDICA DE LOS DELITOS INFORMÁTICOS. 83
4.1.1. Análisis Legislativo en la Unión Europea. 83
4.1.2. Análisis Legislativo en Latinoamérica. 90
4.1.3. Análisis Legislativo en Estados Unidos y Canadá. 97
4.1.4. Problemas que rodean a la cooperación internacional en el área de los delitos informáticos. 103
4.1.5. Perspectiva global del Derecho Mexicano ante el fenómeno informático. 105
4.1.6. Situación actual de México ante la ausencia de Legislación en materia de Delitos Informáticos. 110
4.1.7. Perspectiva de inclusión de los delitos informáticos en la Legislación Penal del país. 122
4.1.7.1. Propuesta de incorporación de los delitos informáticos en el Código Penal Federal. 124

CONCLUSIONES. 128
PROPUESTA. 131
BIBLIOGRAFÍA. 132
LEGISGRAFÍA. 134
OTROS MEDIOS DE INFORMACIÓN 135

INTRODUCCIÓN

La Informática es uno de los fenómenos más significativos de los últimos tiempos; tan es así, que su influjo ya se ha dejado sentir en prácticamente todas las áreas del conocimiento humano, dentro de las cuales el Derecho no puede ser la excepción.

En los últimos años, el fenómeno informático ha impactado abruptamente el ritmo de vida del hombre, al grado en que éste debe hacer esfuerzos de adaptación especiales para asimilar los cambios. El ritmo es tan violento, que si no logra adaptarse adecuadamente al fenómeno innovador, el hombre terminará siendo dominado por la tecnología y no a la inversa como debe ser en la realidad.

De ahí la importancia del Derecho en el avance y aparición de las novedades tecnológicas; pues será a través de él en su papel de elemento disciplinador del proceso, como se logre brindar la protección necesaria al uso de éstas nuevas tecnologías informáticas.

El avance de la tecnología informática en el ámbito del Derecho, representa hoy en día un importante y necesario campo de estudio, el cual debe tratar de delimitar los alcances y contenidos que derivan de esa relación con el fin de establecer un marco jurídico aplicable a las tecnologías de la información, que promueva su adecuado uso y aprovechamiento en los diferentes sectores del país.

México, al igual que muchos países donde la Informática aún no ha sido objeto de regulación jurídica, se enfrenta a numerosos problemas al no contar con una legislación adecuada a esta tecnología. De esta forma, mientras que para ciertos individuos el uso de las tecnologías informáticas representa una apropiación, para otros representa un despojo y por ende la vulneración de sus garantías.

Es un hecho que el marco de impunidad que prevalece en estos países en torno a la materia informática, prolifera la comisión de conductas ilícitas derivadas del uso inadecuado de las tecnologías de la información, lo que supone una ampliación de acción en las esferas de ciertos individuos aunado a graves restricciones en las esferas de los demás.

Esta situación, ha provocado que se cree un ambiente de incertidumbre e inseguridad jurídica entre la población que de alguna u otra forma hace uso de la informática, y que ante la problemática existente, reclama el respeto y protección de sus derechos fundamentales.

Una sociedad donde impera el estado de Derecho, debe saber cómo actuar frente al avance científico, cómo lo pueden usar para su desarrollo, cómo pueden evitar que sus legítimos intereses se vean atropellados por su impacto negativo, a quién y a qué deben respetar. En una palabra, debe ser el Derecho quien en medio de la vorágine tecnológica provea a los individuos de los dos grandes valores que persigue: "Seguridad jurídica y Justicia".

Por tal motivo, ante el impacto y alcance que ha tenido el desarrollo de la Informática en México como en el resto del mundo; se hace necesario adoptar un marco jurídico acorde a las necesidades que plantea este fenómeno mundial, con la finalidad de contar con disposiciones que aseguren las condiciones requeridas para su mejor aprovechamiento y desarrollo.

En el curso de la presente investigación se aborda ampliamente el fenómeno informático, así como las implicaciones positivas y negativas que ha traído aparejado su uso y aplicación, en especial, se hace referencia al surgimiento de una nueva modalidad de conductas ilícitas derivadas del uso inadecuado que se ha hecho de las tecnologías de la información, y a las cuales muchos estudiosos del derecho han concertado en llamar "delitos informáticos".

Asimismo se plantea la situación actual que impera en México, ante la ausencia de legislación jurídica al respecto, y los múltiples problemas derivados de esta circunstancia; y se propone desde un punto de vista muy subjetivo, la posible solución a tal problemática.

CAPÍTULO 1
METODOLOGÍA DE LA INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA.

¿ Se considera importante y necesaria la creación de un marco jurídico aplicable a la Informática como un medio más idóneo para la prevención y sanción de delitos cometidos por el uso indebido de los Sistemas Informáticos ?

1.2. JUSTIFICACIÓN DEL PROBLEMA.

La irrupción de la Informática en la vida del hombre ha tenido un impacto de tal magnitud que le permite tener un acceso más ágil a la información, lo que hace posible la realización de actividades de una manera más eficiente; al grado, de que en estos días es casi imposible concebir la globalización en que se vive sin la incidencia de la Informática en la Sociedad.

En los últimos diez años, las tecnologías computacionales han irrumpido en el mundo y han ido penetrando en todos y cada uno de los aspectos de la vida cotidiana; han influido en múltiples actividades económicas, y en las esferas políticas y sociales.

México no se ha sustraído del contexto mundial que el desarrollo de la Informática presenta. Sin embargo, si bien es cierto que en los últimos años el

uso de las tecnologías de la información en el país se ha incrementado en forma significativa, esta situación no ha sido aprovechada del todo sanamente. En la actualidad, los aspectos normativos que existen en torno a la regulación de la Informática, son casi nulos en la República Mexicana.

La ausencia de disposiciones jurídicas que rijan esta área, propicia la proliferación de acciones delictivas por parte de aquellos sujetos que abusando de sus conocimientos y capacidad de acceso a los sistemas informáticos, vulneran los derechos de individualidad de las personas que hacen uso de esta innovadora tecnología causándoles importantes perjuicios, tanto económicos como morales.

Es por tal motivo, que se hace necesario analizar nuevas modalidades de conductas delictivas, derivadas del uso de las tecnologías de la información, con la finalidad de contar con elementos de juicio para su adecuada sanción; y de esta forma establecer en el país un marco jurídico completo y coherente, que brinde certidumbre y seguridad jurídica a la Sociedad, y permitan aprovechar la Informática para el logro de los propósitos que conlleven al progreso de México.

1.3. DELIMITACIÓN DE OBJETIVOS.

1.3.1. Objetivo General.

Destacar la importancia y la necesidad que reviste la creación de un marco jurídico aplicable a la Informática, con el objeto de prevenir la comisión de conductas delictivas derivadas del uso ilícito de las tecnologías de la información, y contar con disposiciones jurídicas que regulen su adecuada sanción.

1.3.2. Objetivos Específicos.

- Ilustrar la aparición del fenómeno informático en la Sociedad y su repercusión en el campo del Derecho.

- Descubrir la naturaleza jurídica del término "delito informático" y distinguir los elementos que lo integran.
- Identificar y analizar la problemática a la que se enfrenta la Sociedad al no contar con una legislación adecuada a la evolución de las tecnologías de la información.
- Destacar la creación de reglamentación jurídica aplicable a la Informática para prevenir y sancionar los delitos cometidos a través de los medios electrónicos.

1.4. FORMULACIÓN DE LA HIPÓTESIS.

La creación de una legislación adecuada a la evolución de las tecnologías de la información es indispensable, toda vez que éstas constituyen un importante factor de desarrollo en México, y su debida reglamentación favorecerá el establecimiento de un ámbito jurídico claro y estable en torno a la Informática; lo que aportará bases sólidas para la adecuada prevención y sanción de los delitos cometidos por el uso indebido de la misma, contribuyendo de esta forma a lograr un desenvolvimiento informático más justo.

1.5. IDENTIFICACIÓN DE VARIABLES.

1.5.1. Variable Independiente.

La comisión de conductas delictivas derivadas del uso indebido de las tecnologías de la información, es cada vez más frecuente ante la inexistencia de estructuras jurídicas que fijen responsabilidades legales; por lo que la creación de un marco jurídico aplicable a esta materia favorecerá un uso adecuado y un aprovechamiento más justo de la misma.

1.5.2. Variable Dependiente.

La ausencia de disposiciones jurídicas aplicables a la Informática en el país, prolifera la comisión de conductas ilícitas por parte de aquellos sujetos que

ante la impunidad existente, abusan de sus conocimientos y capacidad de acceso a los sistemas informáticos para hacer un uso indebido de los mismos.

1.6. TIPO DE ESTUDIO.

1.6.1. Investigación Documental.

Para la realización de la presente investigación fue necesaria la recopilación de información a través de visitas realizadas a diversas Bibliotecas, tanto públicas como privadas y particulares de la Entidad; en cuyas instalaciones se llevó a cabo la consulta de libros de texto relativos al tema de investigación, así como de publicaciones y revistas con artículos de gran relevancia para el tema en estudio. También fue de gran importancia y utilidad la consulta de diversas páginas vía internet, cuyos contenidos aportaron datos valiosos al presente trabajo de investigación.

Asimismo se formularon fichas bibliográficas y de trabajo, con el fin de lograr una adecuada investigación.

1.6.1.1. Bibliotecas Públicas.

- "Biblioteca Regional de la Universidad Autónoma Veracruzana (UV)".
  Av. Ruíz Cortínez s/n.
  Boca del Río, Veracruz.

- Biblioteca de la "Casa de la Cultura Jurídica de la Suprema Corte de Justicia de la Nación".
  Av. Cinco de Mayo esquina Rayón. (Altos del Palacio Federal de Veracruz).
  Veracruz, Veracruz.

1.6.1.2. Bibliotecas Privadas.

- Universidad Cristóbal Colón "Segismundo Balaguet".
  Prolongación Díaz Mirón s/n.
  Veracruz, Veracruz.

- Universidad Villa Rica.
  Av. Urano esquina Progreso. Fraccionamiento Jardines de Mocambo.
  Boca del Río, Veracruz.

- Lic. Ernesto Luna Duarte.
  Calle Mar Egeo Número 170 esquina Costa de Marfil. Fracc. Costa Verde.
  Boca del Río, Veracruz.

- Lic. Víctor Manuel Hernández Viveros.
  vimahevi@hotmail.com.
  vimahevi@xal.megared.net.mx
  vimahevi@abogados.net

1.6.2. Técnicas Empleadas.

1.6.2.1. Fichas Bibliográficas.

Para la recopilación de la información se consultaron diversos libros de texto relativos al tema en estudio; y para tales efectos, se elaboraron fichas bibliográficas propiamente dichas, las cuales se formularon acorde con los siguientes requisitos:

- Nombre del Autor.
- Título del Libro
- Tomo del Libro.
- Datos de la actualización o traducción del libro (en su caso).
- Número de Edición.
- Editor o Editorial.
- Lugar , fecha y año de impresión.

Asimismo se obtuvo información de la consulta realizada a diversas páginas de internet, motivo por el cual se elaboraron fichas informáticas las cuales cuentan con los siguientes requisitos:

- Dirección de la página web o sitio de intenet.
- Nombre del Autor de la página web.
- Título del tema consultado.

1.6.2.2. Fichas de Trabajo.

Con el mismo objeto se formularon fichas de trabajo, las cuales están elaboradas con los siguientes requisitos:

- Nombre del Autor.
- Título del Libro.
- Tomo del Libro.
- Datos de la actualización o traducción del libro (en su caso).
- Número de Edición.
- Editor o Editorial.
- Lugar, fecha y año de impresión.
- Resumen breve de la información recabada.

CAPÍTULO 2
MARCO HISTÓRICO-LEGAL DEL FENÓMENO INFORMÁTICO

2.1. FENÓMENO INFORMÁTICO.

2.1.1. La Cibernética.

Para poder entender el fenómeno informático como punto de referencia respecto al tema en estudio, es necesario realizar algunas breves consideraciones en torno a la cibernética, que es el rubro general del cual se desprende todo el desarrollo de las tecnologías de la información.

El vocablo "cibernética" fue empleado por primera vez en 1948 por el matemático estadounidense Norbert Wiener, quien aplicó dicho término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina. Su aparición se debió primordialmente a tres factores:

- El factor social, debido a que el entorno que se vivía en esa época era propicio para el surgimiento de una nueva disciplina que fuese capaz de lograr un aumento en la producción y por tanto en el capital.
- El factor técnico-científico, ya que con la unión de la ciencia y la técnica se hizo menester la aparición de una ciencia que facilitara su interrelación y desenvolvimiento.

- Y por último, el factor histórico, porque surge de la imperiosa necesidad de contar con una ciencia que controlara y vinculara a todas las demás.

De ahí el surgimiento de la "cibernética" como una unidad que abarca en forma total y multidisciplinaria a todas las ciencias.

En cuanto a su aspecto etimológico, la palabra "cibernética" toma su origen de la voz griega *"kybernetes"* que significa piloto, y *"Kibernes"*, vocablo que hace referencia al arte de gobernar; pero aludiendo a la función del cerebro respecto a las máquinas.

En términos generales "la cibernética es la ciencia de la comunicación y el control"[1] . Se concluye afirmando que la cibernética busca el empleo de métodos científicos que den explicación a fenómenos en la naturaleza o en la sociedad, a través de la representación del comportamiento humano de forma matemática en una máquina. Es una ciencia, cuya aplicación está relacionada con cualquier campo de estudio.

2.1.2. La Informática.

La informática surge al igual que la cibernética, de la inquietud racional del hombre, quien ante una cada vez mayor necesidad de información para la adecuada toma de decisiones, se ve impulsado a desarrollar nuevas técnicas que lo auxilien al logro de dichos propósitos.

A lo largo de la evolución histórica, el mundo ha sufrido diversas revoluciones tecnológicas, que han repercutido sustancialmente en el ámbito tanto económico como social.

---

[1] Téllez Valdés Julio, Derecho Informático, Edit. McGrawHill , Segunda Edición, México, 1996, pág. 4.

En la actualidad, se está viviendo una nueva revolución tecnológica, la "revolución informática". Ésta, con todo lo que en sí representa, está transformando de manera indudable el mundo.

La palabra "informática" tiene su origen en Francia en el año 1962 cuando fue sugerido por el francés Phillipe Dreyfus; y es un neologismo derivado de los vocablos *"information"* información; y *"automathique"* automatizada; que en términos generales hace referencia a un proceso de información automatizada. En un sentido más específico, dicho vocablo alude al tratamiento automático de los datos que constituyen la información.

Desde mediados de los años sesenta se ha intentado encontrar una definición de lo que es la informática, sin embargo aún no se ha logrado aplicarle una definición integral, puesto que lo que surgió como una disciplina o rama de la ciencia y de la técnica, se ha convertido en un complejo campo de conocimientos, de experiencias y de aplicaciones en todas las áreas del quehacer humano.

De acuerdo a lo establecido por el autor José Antonio Padilla Segura, en su obra "Informática Jurídica", la informática "es un conjunto de disciplinas y técnicas para la elección, captación, almacenamiento, procesamiento, organización y recuperación de datos a fin de contar con una información eficiente y con una comunicación eficaz dentro de un sistema, sea político, social o económico, tratados en forma racional, generalmente empleando medios o recursos automatizados o de difusión; tales como son las computadoras y los sistemas modernos de telecomunicación, para aplicarlos a la comprensión de situaciones y a la solución de problemas".[2]

---

[2] Padilla Segura, José Antonio. Informática Jurídica. Editorial SITESA (Sistemas Técnicos de Edición, S.A. de C.V.), IPN (Instituto Politécnico Nacional), Primera Edición, México, 1991. Pág. 5.

A este respecto, se concluye afirmando que la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información, a través de métodos y sistemas innovadores de telecomunicación, que permiten al hombre efectuar una mejor toma de decisiones.

2.1.3. Diferencias entre Cibernética e Informática.

Es indispensable enfatizar las diferencias que existen entre la Cibernética y la Informática, ya que a pesar de que ambas tienen como objetivo primordial el tratamiento de la información en forma matemática, lógica y analítica; existen ciertos aspectos que permiten distinguir a una de la otra:

- La cibernética en forma general, se ocupa de los fenómenos de control y comunicación; lo cual se traduce en el diseño y construcción de máquinas, que permitan representar el comportamiento humano en forma matemática a través de las mismas.
- La informática por su parte, surge del estudio de las computadoras, de sus principios fundamentales y de su utilización. Se centra principalmente en el tratamiento, representación y manejo automático de la información.
- La cibernética, entre otros aspectos, se relaciona con la creación de instrumentos informáticos que contribuyan a la realización de las actividades humanas, como es el caso de los robots, desarrollo de la inteligencia artificial, etc.
- La informática, es un instrumento de apoyo para el desarrollo de la cibernética.
- La cibernética implica un sistema en el cual puede o no existir la relación entre partes; en cambio,
- La informática, entraña un sistema en el cual siempre habrá relación entre las partes que lo integran.
- En términos generales, la Cibernética constituye el género del cual deviene la especie que es la Informática.

2.1.4. Orígenes y Evolución Histórica de las Computadoras.

Las computadoras constituyen los instrumentos operativos de la informática, por lo que resulta importante profundizar en el origen y evolución que las mismas han tenido en la historia de la humanidad.

Al efecto, es necesario destacar en un principio qué se entiende por computadora, término al cual el autor Juan José Ríos Estavillo hace referencia en su obra "Derecho e Informática en México", citando que "la computadora es un aparato o un conjunto de máquinas interconectadas capaz o capaces de realizar, según un programa establecido, una sucesión de operaciones que le son suministradas y que se recuperarán en las salidas"[3].

Desde la antigüedad, el hombre se ha visto en la necesidad de procesar datos. En un principio, al tratar de cuantificar sus pertenencias, animales, objetos, etc., hizo uso de los dedos de sus manos y utilizaba su memoria para almacenar toda la información posible en ella lo cual representaba una gran limitante. Sin embargo, poco a poco comienza a hacer uso de otros medios tales como cuentas, granos y objetos similares que le facilitaban en cierta forma dicha cuantificación.

Posteriormente, la comunicación humana toma otro sentido cuando el hombre comienza a inventar sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez. Es así, como entre las primeras creaciones del hombre encaminadas a facilitar las operaciones de cálculo, encontramos el ábaco, las tablas de logaritmos, la regla de cálculo, la máquina de pascal, la tarjeta perforada y la máquina de Babbage que representa el antecedente más remoto de las computadoras.

---

[3] Ríos Estavillo Juan José, Derecho e Informática en México, UNAM (Instituto de Investigaciones Jurídicas), Número 83, México, D.F., 1997, pág.40.

En 1834, el inglés Charles Babbage , ideó una máquina analítica que era capaz de ejecutar procesos complicados como la multiplicación y la división, almacenando resultados intermedios en un dispositivo interno donde efectuaba decisiones simples para finalmente entregar un resultado impreso de manera automática. La máquina de Babbage fue determinante para el desarrollo de las computadoras actuales, ya que cien años después de que él la ideó, sus bases sirvieron de pauta para la realización de la primera computadora electrónica.

La primera máquina que llevó a la realidad la idea de Babbage fue la Mark I o ASCC (Automatic Séquense Controlled Calculator); que fue creada entre los años 1937 y 1944 por Howard Aike en la Universidad de Harvard. Esta máquina era capaz de realizar largas secuencias de operaciones codificadas previamente, registrándolas en una cinta de papel perforada y calculando los resultados con la ayuda de unidades de almacenamiento (memoria). Sin embargo, esta máquina era muy lenta.

Entre 1943 y 1945, los estadounidenses John Mauchly, John Eckert y John Von Newman crean la primera computadora electrónica conocida como ENIAC (Electronic Numerical Integrator and Calculator), la cual se caracterizaba porque no tenía partes mecánicas, sino que estaba integrada por 18,000 bulbos; y era capaz de realizar cinco mil operaciones por segundo. Sin embargo, esta máquina era demasiado grande y se calentaba con gran rapidez.

Hacia los años 1945 a 1952, los mismos creadores de la máquina ENIAC construyen una segunda máquina electrónica a la cual denominaron EDVAC (Electronical Discrete Variable Automatic Computer), la cual tenía como función primordial realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente.

En 1951, aparece la primera computadora de uso comercial, conocida con el nombre de UNIVAC I (Universal Automatic Computer). Ésta tenía como característica principal el uso de cinta magnética para la entrada y salida de datos; además, contaba con capacidad de procesamiento de datos alfabéticos y numéricos, así como con un programa especial que era capaz de traducir programas en un lenguaje particular a lenguaje de máquina.

El desarrollo histórico de las computadoras fue dividido en generaciones para una mejor comprensión. Todas las máquinas anteriormente reseñadas constituyen la primera generación de computadoras, caracterizadas por el uso de bulbos de alto vacío como componentes básicos de su estructura interna. Eran máquinas de grandes dimensiones que consumían mucha energía, y por tanto, se sobrecalentaban rápidamente. Además, eran muy lentas y tenían poca capacidad de almacenamiento interno.

La segunda generación de computadoras, se distingue por la sustitución de los bulbos por transistores, los cuales permitieron reducir las deficiencias existentes, y lograr una reducción de tamaño y un aumento en la capacidad de procesamiento de datos.

Las computadoras de la tercera generación se caracterizan por la inserción de circuitos integrados monolíticos, conocidos con el nombre de chips; los cuales, aumentaron considerablemente la velocidad de la operación, incrementado su confiabilidad, y reduciendo el tamaño y costo de las máquinas.

La cuarta generación se da de los años 1972 a 1982. Aquí se produce el surgimiento de los llamados microprocesadores; que son circuitos integrados de alta densidad que constituyen un gran avance tecnológico, ya que a partir de este momento es que se origina una nueva industria, la de las computadoras personales.

Y finalmente, la quinta generación, que va del año 1982 a la fecha; y que es el periodo en el que más innovaciones tecnológicas se han dado en torno a la materia. En esta etapa la microelectrónica ha tenido grandes avances; se han desarrollado programas de software y otros sistemas que permiten un óptimo manejo de las computadoras.

2.2. IMPLICACIONES DE LA INFORMÁTICA EN LA SOCIEDAD.

2.2.1. Implicaciones Positivas y Negativas.

Durante los siglos XVIII, XIX y XX se dieron en el mundo diversos fenómenos sociales; tales como la Revolución Industrial, el pensamiento analítico, el movimiento de las codificaciones escritas, la aparición de la burocracia, de la cibernética y con ella, de la informática.

En sus inicios, la aparición de las computadoras no tuvo el impacto esperado, ya que la gente no creía en ellas. No fue sino hasta principios de la década de los sesenta, en que se les dio el impulso económico necesario para su producción a gran escala, cuando los empresarios se percataron de su utilidad comercial.

Los descubrimientos en el campo de la informática han alcanzado niveles insospechados; al grado en que han llegado a ser no solo objeto de programación económica sino que también han provocado cambios radicales en las conductas social e individual.

Dichos fenómenos son los que caracterizan hoy en día a la llamada "Revolución Informática", que impone en México, al igual que en el mundo globalizado, nuevas formas de organización en los negocios, en los gobiernos, en las instituciones educativas y, cada vez más, en todas las actividades habituales.

Considerando implicaciones más particularizadas de la informática en la sociedad, se puede decir, que las computadoras se han convertido en herramientas comunes para el hombre quien se ha involucrado con ellas de múltiples maneras.

Los avances tecnológicos han logrado que las computadoras se conciban como una de las fuerzas más poderosas de la sociedad actual, haciendo posible su uso tanto en los grandes niveles empresariales e industriales como en los propios hogares.

Sin embargo, el uso y aplicación de las computadoras en todos los ámbitos sociales ha tenido implicaciones tanto positivas como negativas.

Entre las implicaciones positivas podemos mencionar el hecho de que se han abierto nuevas oportunidades de trabajo en áreas tales como la programación, operación de computadoras y administración de sistemas de información, lo que ha representado un gran auge, cuestión que demanda profesionales mejores capacitados en la materia.

Además, el uso de las computadoras representa una mayor satisfacción en el trabajo. Los científicos e ingenieros pueden resolver complejos problemas a través de la operación de sistemas informáticos.

En el ámbito académico y empresarial también tienen una aplicación trascendental; ya que esta tecnología ha permitido un acceso más ágil a la información y por tanto, una mayor eficacia en las actividades. De igual forma hay que agregar los grandes beneficios que el uso de las computadoras producen en las industrias, lo que se traduce en un aumento en la productividad, ya que permite una mayor eficiencia en la fabricación de los productos, así como

también evitan el desperdicio de materias primas y proporcionan un mejor servicio a los clientes.

Por otro lado, el uso de los sistemas informáticos también ha traído consigo implicaciones negativas; tales como, la continua amenaza de desempleo, al haber reemplazo de fuerza humana por máquinas automatizadas, lo cual puede provocar crisis agudas de carácter socioeconómico.

A esto hay que aunar, los problemas físicos y psicológicos ante los cuales se enfrenta la gente por el empleo de las computadoras como lo son, sentimientos de frustración, trastornos visuales, despersonalización, etc., sin omitir la problemática que los grandes descubrimientos informáticos han originado en el ámbito jurídico como lo son los de falta de seguridad y confidencialidad de la información, robo de programas, comisión de ilícitos, etc.

2.2.2. Principales usos de las computadoras en la Sociedad.

El uso y aplicación de las tecnologías de la información ha tenido injerencia en diversas áreas a nivel institucional, privado y sociocultural. El desarrollo de las computadoras ha permitido un gran avance en diversos ámbitos.

A nivel institucional; se ha logrado una automatización o informatización de las oficinas, lo cual ha permitido un mejor y más rápido desenvolvimiento de las actividades. Asimismo, se ha conseguido una adecuada formulación de políticas, planeación y conducción de estrategias de organización. Hay una mejor supervisión y control de empleados. En cuanto a la administración; se ha obtenido un adecuado control de nóminas , contabilidad, inventarios, registros, etc.

En el área industrial; con la informatización de las fábricas, se ha logrado alcanzar un gran aumento en la productividad, reduciendo los tiempos y costos.

El uso de las computadoras ha sido muy útil en el ámbito bancario, en el cual, la aplicación de los sistemas informatizados ha permitido una mayor agilidad en la realización de las transacciones financieras con sistemas de pago automatizados, autorización de créditos, transferencia de fondos, asesorías financieras, etc.

En el área de la salud; los beneficios que la informática ha logrado obtener se traducen en mejor preparación de historias clínicas, exámenes y diagnósticos más completos, mayor exactitud en las pruebas de laboratorio y un mejor control de los productos farmacéuticos.

El uso de las computadoras ha llegado incluso hasta los hogares. Hay una mejor administración del presupuesto, un mayor control en el uso de energía, análisis de inversión y preparación de la declaración de impuestos, etc. Sin dejar a un lado, que gracias a los sistemas informáticos se puede alcanzar un mejor diseño y construcción de edificios, desarrollo de nuevas ideas publicitarias, localización de personas extraviadas, recuperación de vehículos robados, control del tráfico y contaminación, predicciones meteorológicas, mejor desarrollo de la educación y de la investigación, fotografía y animación por computadora, diversión y entretenimiento.

En general, como se puede apreciar; el uso de las computadoras tiene aplicaciones en casi todos los ámbitos de la sociedad, lo que resalta su creciente importancia en la vida del hombre.

2.3. INCIDENCIA DE LA INFORMÁTICA EN EL DERECHO

2.3.1. Derecho Informático.

A lo largo de este siglo han surgido grandes avances tecnológicos que han impactado el ritmo de vida del hombre. Sin embargo, es necesario que la

humanidad se adapte a ese ritmo tan violento con el fin de que sea el hombre quien domine a la tecnología y no a la inversa.

La irrupción de la informática en la sociedad le ha permitido realizar más y mejores actividades, de tal forma, que es casi imposible concebir la globalización en que se vive, sin el uso de las tecnologías de la información.

Ante tal perspectiva, el papel del derecho en el avance y aparición de las tecnologías de la información es imprescindible, como un elemento disciplinador del proceso.

Vittorio Frosini señala a este respecto que " el binomio informática y derecho indica con claridad la interacción entre dos ciencias, de la cual surge un campo fecundo del saber: por una parte, la computadora se considera un instrumento utilizado por el jurista para crear bancos de datos jurídicos y para facilitar la administración de justicia, y por otra, recurrir a la computadora plantea una serie de problemas que deben ser regulados por la ley."[4]

El empleo de las nuevas tecnologías puede suponer apropiación para ciertos individuos y despojo para otros; por lo que resulta inevitable la aplicación del derecho, con el fin de brindar la protección necesaria para su adecuado desarrollo y de esta forma proveer a la sociedad de los dos grandes valores que el Derecho persigue: Seguridad jurídica y Justicia.

En tal sentido, es conveniente afirmar que la Informática es un fenómeno que debe ser regulado por el Derecho, pero a la vez, es una herramienta que éste debe aprovechar.

---

[4] Ríos Estavillo Juan José. Obra citada. Pág.69.

2.3.1.1. Antecedentes.

El Derecho Informático como una nueva rama del Derecho, es una disciplina en continuo desarrollo. Las alusiones más específicas sobre la interrelación entre el Derecho y la Informática se dan a partir del año 1949 con la obra de Norbert Wiener intitulada "Cibernética y Sociedad", en la cual hace referencia a la influencia que ejerce la cibernética en el ámbito jurídico. Dicha interrelación asegura el autor, se da a través de las comunicaciones. Esa relación interdisciplinaria sugería una conjunción entre el "ser " y el "deber ser".

En ese mismo año, el juez norteamericano Lee Loevinger publicó un artículo en la revista Minnesota Law Review intitulado "The next step forward" ("El próximo paso hacia delante"), en cuyo texto menciona que el próximo paso adelante en la vida del hombre, debía ser el de la transición de la Teoría General del Derecho hacia la Jurimetría, que es la investigación científica acerca de los problemas jurídicos.

Estas primeras manifestaciones interdisciplinarias se dieron en términos de las implicaciones que la Informática tenía respecto al Derecho; y no como se comienza a dar a partir de la década de los sesenta, en donde el hombre se empieza a ver en la necesidad de dar estudio a las implicaciones jurídicas motivadas por el uso de las tecnologías de la información.

El Derecho Informático posee ciertas características que provocan que sea imposible ubicarlo dentro de los departamentos jurídicos o de normatividad tradicionales, ya que existen destacadas diferencias que se hacen necesarias con el fin de que éste sea realmente eficaz.

Entre las particularidades que hacen que se conceptúe al Derecho Informático como una rama autónoma del Derecho están:

- Su cronología de acción procede antes de que ocurra el derecho vigente. Es decir, primero se da el hecho y posteriormente el derecho que lo regula.

- Su campo de investigación es a nivel internacional, ya que persigue la búsqueda de consensos aplicables en interacción con otros países, y el respeto también, de las leyes nacionales.

- Se basa primordialmente en el estudio del Derecho Comparado.

- Sus fuentes de información no pueden ser generalmente libros, ya que su investigación se sitúa antes de que estos sean publicados. La mayoría de las veces esas fuentes de información las constituyen revistas especializadas en la materia, o los documentos y memorias de los Congresos que se han dado con respecto al Derecho Informático.

- El número de publicaciones que en español se han dado en torno a la materia de Derecho Informático es muy bajo, por lo que se hace necesario el manejo de otros idiomas con el fin de obtener mayor información respecto al tema.

- El Derecho Informático busca el diseño y justificación de estructuras nuevas o corregir las ya existentes en torno a la materia; basándose desde luego, en los principios particulares que la propia Constitución establezca.

- Sus metas se encausan a la obtención de un dinamismo jurídico en la materia, y a proveer fiabilidad a la estructura que se proponga o corrija.

- Sus fines serán siempre de orden público y de interés social.

2.3.1.2. Concepto y clasificación.

Cuando se hace referencia al término informática, se debe entender que se está en presencia de información automatizada, por lo que, al interrelacionarla con el derecho, se debe determinar la existencia de una ciencia jurídica que se encarga de normar y regular los efectos que ocasiona el uso y aplicación de las tecnologías de la información. Dicha ciencia jurídica es lo que se conoce con el nombre de Derecho Informático.

Sin embargo, en la práctica ha surgido una gran confusión en determinar si es correcto o no denominar a la materia con el nombre de Derecho Informático.

El 30 de abril de 1980, el Consejo de Europa recomendó que la nomenclatura utilizada fuera la de " Derecho e Informática", incluyendo dicha acepción, el análisis de dos disciplinas con objeto de estudio diverso, la informática jurídica y el derecho de la informática.

En la actualidad, el derecho informático y el derecho de la informática se entienden conceptualizados bajo un mismo término; aunque existen posturas que asientan que esto constituye un error, ya que una cosa es hablar de derecho informático como ciencia de estudio de la informática jurídica, y otra muy diferente es referirse al derecho de la informática.

Julio Téllez Valdés concibe al Derecho Informático como "una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)."[5]

En función de lo anterior, es evidente afirmar que el Derecho Informático se clasifica para su estudio en dos vertientes fundamentales que son la Informática

[5] Téllez Valdés Julio. Obra citada. Pág. 22.

Jurídica y el Derecho de la Informática. En líneas subsecuentes se detallan en forma más pormenorizada los elementos que integran ambas disciplinas.

2.3.2. Informática Jurídica.

Como ya se ha destacado en párrafos anteriores, la Informática es uno de los fenómenos más significativos de los últimos tiempos, y ha influido determinantemente en casi todas las áreas del conocimiento humano, dentro de las cuales el Derecho no puede ser la excepción, dando lugar a lo que es conocido en términos instrumentales con el nombre de "Informática Jurídica".

La Informática Jurídica se materializa propiamente con el tratamiento y sistematización de la información jurídica.

Para el desarrollo de la Informática Jurídica es necesario considerar ciertos aspectos como son la aplicación lógica del derecho o raciocinio jurídico, el análisis del discurso jurídico, la aplicación de la teoría de los sistemas, la aplicación de una teoría de la información, etc. Lo anterior con el fin de constituir la base fundamental sobre la cual se desarrolla el objeto mismo de la Informática Jurídica.

Por lo que respecta al razonamiento jurídico, Marcelo Bauza señala que dicho razonamiento no constituye una operación aislada, sino que se integra de un proceso compuesto de varias etapas. En este sentido, cada una de esas etapas en las que se desarrolla este proceso, constituye a la vez otros sectores de desenvolvimiento de la Informática Jurídica, los cuales requieren ser objeto de investigación con el propósito de poder converger finalmente en su aplicación concreta.

En cuanto hace al análisis del discurso jurídico, éste conlleva el estudio del lenguaje jurídico con el fin de crear instrumentos que permitan el acceso a la

información jurídica, es por tal motivo que se asevera que la simple captura de información jurídica no es informática jurídica, sino que ésta va más allá que la simple captura. El discurso jurídico se basa en un sistema normativo, que parte de proposiciones lógicas en cuanto al ser y deber ser. Para el desarrollo de la Informática Jurídica se emplean dos instrumentos lingüísticos: el léxico y el thesaurus. El léxico, es la agrupación de palabras que se encuentran contenidas en cada uno de los documentos de un banco de información, que organizados constituyen la base documental. En tanto el thesaurus, es un conjunto de conceptos sobre un área del conocimiento determinada, relacionados por su significado, y cuya función principal es auxiliar al usuario a diseñar estrategias conceptuales de búsqueda. Los problemas de técnica legislativa que se suscitan por las limitaciones del lenguaje en la materia informática son resueltos en este sentido, por el léxico y el thesaurus, de ahí su importancia.

Respecto a la teoría de los sistemas, se concibe como la integración de un todo organizado mediante elementos de reglas y normas. Aplicando dicha teoría al sistema jurídico se tiene que "se consideran sistemas jurídicos o legales las organizaciones encargadas de administrar justicia y, de igual manera, se designa a los procedimientos seguidos para impartir justicia. En consecuencia, el derecho es un sistema en el que intervienen conceptos, reglas y procedimientos."[6] Por lo tanto, se puede decir que el desarrollo de la Informática Jurídica debe partir del establecimiento de un sistema cuyos elementos tiendan a su vez a la creación de otros sistemas que organicen y estructuren la información jurídica.

Expuesto lo anterior es conveniente citar que la Informática Jurídica analiza, reestructura, desarrolla y precisa términos informáticos aplicables al propio derecho.

---

[6] Ríos Estavillo Juan José. Obra Citada. Págs. 48,49.

2.3.2.1. Antecedentes y Evolución.

La Informática Jurídica nació propiamente en 1959 en los Estados Unidos y ha sufrido cambios acorde con la evolución general de la informática.

Las primeras manifestaciones en torno a la recuperación de documentos jurídicos en forma automatizada se remontan a los años cincuenta, en que se comienzan a utilizar las computadoras ya no sólo con fines matemáticos, sino también lingüísticos.

Estos esfuerzos fueron realizados en el Health Law Center de la Universidad de Pittsburg, Pennsylvania; bajo la dirección de John Horty quien ante la necesidad de encontrar medios satisfactorios para tener acceso a la información legal, ordenó colocar todas las codificaciones legales de Pennsylvania en cintas magnéticas. Esta fue la primera exhibición de un sistema legal automatizado de búsqueda de información.

Dicho sistema fue rediseñado y explotado comercialmente por la Corporación de Sistemas Aspen.

A principios de 1966, algunos estados de la Unión Americana adoptaron el sistema y se propusieron desarrollar un sistema interno de recuperación de documentos legales.

Hacia el año 1968, cincuenta estados de ese país habían acogido dicho sistema para la computarización de sus respectivos ordenamientos legales.

El segundo logro por parte del Health Law Center fue el sistema LITE creado en 1969; actualmente conocido con el nombre de FLITE (Información Legal Federal a través de Computadoras), que fue desarrollado por la Universidad de Pittsburg bajo el auspicio de la Fuerza Aérea Norteamericana.

Como se puede apreciar, la década de los sesenta marcó el desarrollo de diversos sistemas relacionados con la Informática Jurídica. Aunados a los sistemas puestos en práctica por el Health Law Center; incursionan en el mercado algunos sistemas de procesamiento de datos legislativos, los cuales eran comercializados en ese entonces por la Corporación Americana de Recuperación de Datos.

Otra importante irrupción en torno a la materia, la constituyó la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR), compañía que lanza al mercado sistemas de procesamiento y recuperación de datos legislativos pero enfocados ya no a instituciones públicas, sino a los abogados litigantes.

A partir de ese momento, comienzan a comercializarse nuevos y mejores sistemas en el área de recuperación de documentos legislativos, y entre otros, uno de los más importantes fue el sistema LEXIS difundido en el mercado por la Compañía Mead Data Central.

Para 1969 el estado norteamericano de Washington, empezó a utilizar el sistema de la IBM llamado IBM-TEXTPAC en el área de procesamiento de documentos, programa que posteriormente fue reemplazado por el sistema STAIRS de la misma compañía. Y de esas fechas a la actualidad, se han desarrollado un sin fin de sistemas en torno a la recuperación y procesamiento de datos y documentos legislativos, cada vez mejor diseñados y estructurados; cuestión que ha permitido, una mayor agilidad y eficacia en la impartición de justicia y un significativo desarrollo en el campo del Derecho.

Como se puede apreciar, la Informática Jurídica surgió con la utilización de las computadoras en el ámbito jurídico.

2.3.2.2. Concepto.

El término Informática Jurídica, no siempre fue conocido como tal. La interrelación de la informática con el derecho, dio lugar a innumerables definiciones aplicables a la materia. La primera denominación que se le dio fue el de Jurimetrics (Jurimetría), término creado por el juez norteamericano Lee Loevinger y que como se reseñó en páginas anteriores, es la investigación científica de los problemas jurídicos.

Posteriormente, se adoptó la denominación de Giuscibernética (Juscibernética), difundida por Mario G. Lozano, quien acogió dicho término, luego de sostener que la cibernética aplicada al derecho ayuda a la depuración tanto cuantitativa como cualitativa de éste.

Otras denominaciones surgidas en torno a la materia fueron el de Computers and Law (Computadoras y Ley) que fue aplicado principalmente por países anglosajones; Rechtsinformatique, término que se le dio en Alemania; Rechtcibernetik, denominación que fue manejada primordialmente en países de Europa Oriental y Jurismática, designación que se le otorgó en México. Sin embargo, la acepción más conveniente en términos prácticos es la de Informática Jurídica.

Existen diversas definiciones aplicables al término Informática Jurídica, entre las que se destacan los siguientes:

Julio Téllez Valdés en su libro Derecho Informático, conceptualiza a la Informática Jurídica como "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables 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".[7]

Por su parte, el Doctor Juan José Ríos Estavillo la define como "las técnicas a las que se recurren para permitir memorizar las informaciones jurídicas y recuperarlas mediante la utilización de la computadora; esto es, la realización de ámbitos prácticos en la explicitación y estructuración de información jurídica".[8]

Antonio Rivero establece que "no es sino la informática considerada como sujeto del derecho; es decir, como instrumento puesto al servicio de la ciencia jurídica".[9]

Para Alain Chouraqui, la Informática Jurídica "es la ciencia y las técnicas del tratamiento lógico y automático de la información jurídica".[10]

Y por último, Héctor Fix Fierro debe entenderse "como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho, o más precisamente, a los procesos de creación, aplicación y conocimiento del derecho".[11]

En virtud de lo anterior se puede concluir que la Informática Jurídica es una ciencia que permite la aplicación de la informática en el campo del Derecho, con el fin de dar un tratamiento lógico y sistematizado a la información jurídica y de esta forma hacer más accesible y dinámica la difusión y aplicación del Derecho en la sociedad.

---

[7] Téllez Valdés Julio. Obra Citada. Pág. 26.
[8] Ríos Estavillo Juan José. Obra citada. Pág. 54.
[9] Obra citada. Pág. 56.
[10] Obra citada. Pág. 56.
[11] Fix Fierro Héctor, Informática y Documentación Jurídica, UNAM, México, D.F., 1990, Pág.56.

2.3.2.3. Clasificación.

Desde el punto de vista del análisis y ordenación de la información jurídica, la Informática Jurídica se divide en tres ramas:

- Informática Jurídica Documental o Documentaria (almacenamiento y recuperación de textos jurídicos),
- Informática Jurídica de Control, Gestión o Administración (Desarrollo de actividades jurídico-adjetivas), e
- Informática Jurídica de ayuda a la decisión o Informática Jurídica Metadocumental y/o Metadecisional (apoyo en la decisión, educación, investigación y previsión del Derecho).

A continuación se precisa en forma independiente cada una de estas vertientes para su mejor comprensión:

La Informática Jurídica Documental o Documentaria es el área más antigua de la Informática Jurídica y su aplicación busca la creación de un banco de datos jurídicos relativo a cualquiera de las fuentes del Derecho (excepto la costumbre); previo análisis y recopilación de la información contenida en documentos jurídicos.

La Informática Jurídica de Control, Gestión o Administración abarca los ámbitos jurídico-administrativo, judicial, registral y despachos de abogados, primordialmente. Su importancia en la Administración Pública obedece a que mediante la adecuada aplicación de la Informática Jurídica de Control, Gestión o Administración en este sector; se puede lograr un mejoramiento en las estructuras jurídico-administrativas y en los sistemas de operación, medida imprescindible para que las entidades del sector público puedan alcanzar sus objetivos esenciales que se traducen en el logro de la justicia y bien común, a través de la aplicación y apoyo de la tecnología moderna. En los órganos jurisdiccionales también ha tenido un uso trascendental, toda vez que las

actividades automatizadas a nivel de judicatura son muy numerosas y variadas; entre otras se pueden mencionar, la formulación agendaria de los jueces, redacción automática de textos jurídicos, elaboración de sentencias; aceptación, registro y seguimiento de los expedientes, etc. La Informática Jurídica también ha incursionado en la automatización de oficinas de índole jurídica, tal es el caso de los despachos de abogados y de las notarías, en donde las labores propias de dicho entorno se han podido simplificar gracias al empleo y manejo de los sistemas informáticos.

Por lo que se refiere a la Informática Jurídica Metadocumental y/o Metadecisional; ésta tiene un ámbito de aplicación muy especial. Sus ámbitos de injerencia lo constituyen principalmente: la ayuda en la decisión, en la educación, en la investigación, en la previsión y en la redacción del Derecho. Por lo tanto, su manejo trasciende más allá de la esencia de los fines documentarios anteriormente descritos.

2.3.3. Derecho de la Informática.

El Derecho de la Informática como instrumento regulador de la informática en la sociedad, no ha sido estudiado en los mismos términos que la informática jurídica. Esto ha sido en virtud de que se le ha dado más importancia a los beneficios que ha traído aparejado el uso de las computadoras, que a los perjuicios ocasionados por el manejo de las mismas.

Sin embargo, se considera que el Derecho de la Informática no puede estar aislado del entorno social, ya que surge como una ineludible respuesta al fenómeno informático. De ahí que para muchos autores, el Derecho de la Informática sea un derecho "en el que su existencia precede a su esencia"[12], tal y como lo afirma Julio Téllez en su obra Derecho Informático.

[12] Téllez Valdés Julio. Obra citada. Pág. 58.

Como se mencionó en páginas anteriores, muchos tratadistas no se ponen de acuerdo aún sobre el particular, de si la materia debe denominarse Derecho Informático o Derecho de la Informática; pero hoy en día, ambos términos se engloban bajo un mismo elemento integrador conocido como Derecho Informático, lo cual como ya se hizo referencia, para ciertos autores constituye un error; ya que el Derecho Informático engloba tanto a la Informática Jurídica como al Derecho de la Informática, por lo que éste solamente constituye una rama o vertiente de aquél.

En términos generales, el hablar de Derecho de la Informática sugiere referirse a una disciplina nueva, normativa y reguladora, de los efectos provocados por el uso ya sea activo o pasivo de una computadora.

2.3.3.1. Antecedentes y Evolución.

Como ya se hizo mención anteriormente, los precursores informáticos nunca se imaginaron el alcance que llegarían a tener las computadoras en la vida del hombre y aún más, nunca vislumbraron que el Derecho llegaría a regular a la Informática.

El fenómeno informático provocó diversas inquietudes, motivadas en un principio, por las aplicaciones comerciales de las computadoras. Pero no fue sino hasta finales de los sesenta, en que la gente comienza a sentir las repercusiones negativas implicadas por el uso y aplicación de los sistemas informáticos.

Tales circunstancias, fueron las que obligaron a darle un tratamiento especial al fenómeno informático. Surge entonces, la necesidad de aplicar el Derecho como un elemento disciplinador del proceso que fuese capaz de brindar a los usuarios de las tecnologías de la información, la protección y seguridad jurídica indispensables para el adecuado desarrollo las mismas.

Es así como aparece una nueva disciplina del Derecho denominada "Derecho de la Informática", cuyo objeto esencial es establecer una normatividad jurídica aplicable al fenómeno informático.

Sin embargo, para algunos autores, la existencia de un Derecho de la Informática como regulador de los efectos producidos por el uso y aplicación de la informática, reviste ciertos aspectos tanto positivos como negativos.

Al respecto, el Doctor Juan José Ríos Estavillo señala en su libro "Derecho e Informática en México" los puntos positivos y negativos de tal presunta existencia, y en relación a los negativos menciona que:

- El Derecho de la Informática no puede concebirse como un cuerpo normativo con naturaleza propia e independiente; por lo tanto, no es considerado como una rama autónoma del campo jurídico.

- Todo cuerpo normativo debe estar respaldado por normas tanto sustantivas como adjetivas, o bien, por reglas propias reguladoras del ser, hacer o no hacer, así como de reglas propias para la solución de controversias. En México, la existencia de legislación que regule la materia informática es casi nula, por lo que prevalece un vacío en la ley en tal sentido. De ahí que sea prudente resaltar, que las problemáticas que surjan debido al impacto de las tecnologías informáticas en el derecho, deben ser resueltas por el aparato jurídico propiamente hablando, y no por las reglas informáticas. Es decir, el derecho no debe supeditarse a la informática, sino es ésta quien debe supeditarse al derecho, por lo que el Derecho de la informática como tal, no existe.

- La norma jurídica tiene su origen en el desarrollo y convivencia de los individuos en una sociedad; tales individuos plantean una serie de hechos

que el derecho regula, por lo que el avance normativo depende en sí del individuo y no de los avances tecnológicos. En este sentido, se ve que el hecho es primero que el derecho; de tal forma, que la sociedad no puede estar supeditada al derecho, sino el derecho a la sociedad, y ante esto, el hombre es quien debe dominar a la tecnología y no a la inversa; por lo tanto, el Derecho de la Informática no puede existir como tal, ni puede dársele valores autónomos.

En cuanto a los aspectos o puntos positivos que pueden determinar la existencia del Derecho de la Informática están los siguientes:

- El hecho de que el Derecho de la Informática pertenezca o no estrictamente a un objeto de estudio del derecho, no lo hace que pierda su propia naturaleza de observación como fenómeno de estudio. No obstante que su existencia deriva de una naturaleza distinta a la del derecho, finalmente emana propiamente de él.

- No todo objeto jurídico de estudio guarda normas sustantivas y adjetivas; y suponiendo que ese fuera el caso, el sistema jurídico imperante en el país soluciona el problema bajo uno de los principios generales del derecho; determinando, que a pesar de la inexistencia de normas jurídicas que complementen el supuesto planteado, el juzgador tiene la obligación de emitir una resolución al respecto; esto es, los propios valores jurídicos y normativos tienen existencia procesalmente hablando, a pesar de estar ante la inexistencia de norma adjetiva expresa. Esto quiere decir, que una norma adjetiva no está supeditada en forma determinante a la norma sustantiva.

- Además, la afirmación de que el hecho va primero que el derecho no es válida en México, según lo aseverado por el propio autor. Aunque es

cierto que las normas jurídicas están supeditadas a la convivencia social o de los gobernados, la regla a esta afirmación admite excepciones planteadas por el propio derecho, por lo que ambos objetos interactúan; ya sea que la sociedad se supedite al derecho, o el derecho a la sociedad, ya que lo único que limita al derecho es en sí, el propio derecho.

- Es por tales argumentos, que el Derecho de la Informática puede abarcar su propio campo de estudio; por lo que la clasificación tradicional del derecho en público y privado, no restringe científicamente a esta disciplina, ya que guarda su propio objeto de estudio y por tanto, su propia metodología. En este sentido, la autonomía no implica que se separe de la ciencia a la cual pertenece, sino que aborde los problemas con métodos e instrucciones propias.

2.3.3.2. Concepto.

Son diversas las acepciones que algunos abogados y estudiosos del derecho y del fenómeno informático, le han atribuido al Derecho de la Informática.

Para Carrascosa López, el Derecho de la Informática es "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones"[13].

Emilio Suñé cita al respecto, que "es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma".[14]

Fix Fierro, no da un concepto preciso de lo que es el derecho de la

[13] Ríos Estavillo Juan José. Obra citada. Pág. 73.
[14] Obra citada. Pág.73.

informática, sin embargo, considera que "la informática como objeto de regulación jurídica ha dado origen al llamado derecho de la informática".[15]

Por otro lado, Julio Téllez asevera que el "Derecho de la Informática es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".[16]

Finalmente, el Doctor Juan José Ríos Estavillo conceptualiza el Derecho de la Informática como " el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas".[17]

En tal sentido se afirma, que el Derecho de la Informática es el conjunto de normas jurídicas que regulan los efectos producidos por el uso y aplicación de la informática en la sociedad.

2.3.3.3. Fuentes.

Como toda rama autónoma, el Derecho de la Informática, tiene sus propias fuentes de creación, de las cuales emanan ese conjunto de conocimientos.

Dentro de las fuentes del Derecho de la Informática se puede mencionar a la Legislación; la cual como ya se mencionó con anterioridad, en muchos países, incluyendo México, es relativamente incipiente al respecto. Sin embargo, existen disposiciones aplicables a otras áreas del Derecho, que guardan cierta relación con respecto al fenómeno informático; tales como, en materia Constitucional, Civil, Penal, Laboral, Fiscal, Administrativa, Procesal, Internacional, etc.

---

[15] Fix Fierro Héctor. Obra citada. Pág.53.
[16] Téllez Valdés Julio. Obra citada. Pág. 58.
[17] Ríos Estavillo Juan José. Obra citada. Pág. 73.

También existen algunos pronunciamientos en cuanto a jurisprudencia, doctrina y literatura en algunos países que ya han hecho referencia sobre el particular. Incluso en algunas revistas y obras especializadas, han aparecido teorías y artículos respecto a los problemas suscitados por la informática.

Es conveniente citar, que existe mucha información respecto al tema vía Internet; sin embargo, como fenómeno derivado del uso y aplicación de las tecnologías de la información, el internet todavía no ha sido asumido en su totalidad, como un medio confiable de información.

Con respecto al fenómeno Internet se debe hacer mención que el Internet es un medio de comunicación informático constituido por una red gigante que interconecta a su vez, una enorme cantidad de redes locales de computadoras a los sistemas informáticos de múltiples organizaciones en el mundo. Hay varias formas para interconectar esas redes, ya sea, a través de líneas telefónicas regulares, de líneas de alta velocidad, de fibra óptica, satélites y microondas.

Se calcula que el Internet enlaza hoy en día a 60 millones de computadoras personales, lo que demuestra el crecimiento extraordinario que dicho fenómeno ha alcanzado en pocos años.

El Internet también es considerado como "un sistema internacional de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general".[18]

[18] Barrios Garrido Gabriela; Muñoz de Alba M. Marcia; Pérez Bustillo Camilo. Internet y Derecho en México. Editorial Mc Graw Hill. Sociedad Internet de México. México, D.F., 1998, Págs. 5, 6.

Los servicios más populares que ofrece el Internet en la actualidad son: correo electrónico, transferencia de archivos, acceso remoto a recursos de cómputo por interconexión (Telnet), world wide web, grupos de discusión (Usenet), comunicación en tiempo real (IRC o Internet Relay Chat).

El Internet, o también conocido como "red de redes", es un enorme generador de relaciones entre personas y es visto, como una herramienta indispensable para la globalización.

Sin embargo, es un fenómeno carente de regulación jurídica, y los efectos de su aplicación ya se han dejado sentir ocasionando múltiples problemas que en muchos casos aún no encuentran una solución favorable al respecto.

En México, se vive una etapa caracterizada por la "autorregulación" del Internet, situación que ha generado incertidumbre para los usuarios de dicho medio, toda vez que al haber ausencia de normatividad aplicable al fenómeno, quedan desprotegidos los derechos y garantías individuales de las personas que acceden a dicho medio de información masiva.

2.3.4. Política Informática en México.

La informática tiene un carácter estratégico en la vida del hombre, en virtud de que sus aplicaciones han afectado prácticamente todas las actividades humanas, modificando las estructuras existentes en ámbitos como la producción, comercialización, organización de instituciones, generación de nuevas tecnologías, difusión de conocimientos, etc.

Pero para que exista un adecuado desarrollo de la informática, es menester realizar una planificación, a través de normas y objetivos que permitan orientarla y aprovecharla para beneficio del país.

Esta planificación especifica en torno a la informática, es lo que se conoce con el nombre de Política Informática y sus principales objetivos están encausados al adecuado desarrollo de la industria de construcción de equipos de cómputo y materiales de programación, difusión y aplicación del fenómeno informático, contratación gubernamental de bienes y servicios informáticos, elaboración de normas y estándares aplicables a la materia informática, etc.

En México, el Plan Nacional de Desarrollo 1995-2000, aprobó mediante Decreto Presidencial, el "Programa Especial de Mediano Plazo denominado de Desarrollo Informático".

Este programa fue establecido considerando que el Plan Nacional de Desarrollo 1995-2000 perseguía en materia de informática; el compromiso de impulsar la generación, difusión y aplicación de las innovaciones tecnológicas, la formación de especialistas en todos los niveles, su aprovechamiento en todos los sectores, así como la promoción de mecanismos para asegurar la coordinación, promoción, seguimiento y evaluación de las actividades relativas a la informática en el ámbito nacional. Lo anterior, con el fin de aprovechar los beneficios de la informática, alcanzar un pleno desarrollo democrático, impulsar el bienestar social y promover el desarrollo económico del país.

El Programa de Desarrollo Informático se fundamentó en las siguientes premisas, con el fin de lograr un máximo aprovechamiento de las tecnologías de la información:

- Incorporar la tecnología de acuerdo con las necesidades y prioridades del país;
- Proporcionar condiciones de acceso universales y abiertas tanto a la infraestructura y a la tecnología como a los mecanismos de fomento;
- Realizar una continua evaluación que permitiera prever necesidades y oportunidades; y

- Asegurar una acción concertada con la comunidad informática para la instrumentación de las acciones que se realizaran.

Tomando en cuenta estas premisas, dicho programa planteó a su vez seis objetivos generales:

1. Promover el aprovechamiento de la informática en los sectores público, privado y social del país.
2. Impulsar la formación de recursos humanos y el desarrollo de la cultura informática.
3. Estimular la investigación científica y tecnológica en informática.
4. Fomentar el desarrollo de la industria informática.
5. Propiciar el desarrollo de la infraestructura de redes de datos.
6. Consolidar instancias de coordinación y disposiciones jurídicas adecuadas para la actividad informática.

Es claro el reconocimiento que hizo el Poder Ejecutivo Federal en el Programa de Desarrollo Informático; al prever que para consolidar un verdadero aprovechamiento de la informática en todos los sectores, es indispensable la formación de recursos humanos de alto nivel que reúnan conocimientos de Derecho de la Informática, y la consolidación de disposiciones jurídicas que normen la materia y que aseguren condiciones adecuadas para favorecer un adecuado aprovechamiento de la informática y un viable desarrollo de infraestructura en la materia.

2.3.5. Legislación Informática en México.

La Legislación Informática es "un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática..."[19].

[19] Téllez Valdés Julio. Obra citada. Pág. 59.

En la actualidad, son muy pocos los países que cuentan con una legislación aplicable a la informática.

En Europa, países como Francia, España e Inglaterra, han comenzado a integrar una normatividad aplicable a la informática dentro de sus sistemas legales.

Lo mismo sucede en algunos países de América como Estados Unidos, Canadá y Argentina, en donde ya se han asentado precedentes sobre la regulación jurídica de la informática.

Sin embargo, en México, la normatividad legal aplicable a las tecnologías de la información, es casi nula. A pesar de los índices de crecimiento en el uso de las computadoras y de Internet, México enfrenta un problema social radicado en lo que se denomina " analfabetismo informático".

Este problema, ha alcanzado a la mayoría de la población de México; incluyendo a los miembros de los Poderes Legislativo y Judicial del país. Es difícil prever el pronunciamiento de los Tribunales Federales o de la Suprema Corte de Justicia mexicanos en un caso cuya resolución se fundamente esencialmente en un problema derivado del uso y aplicación de los sistemas informáticos; lo mismo para el caso de vislumbrar la existencia de un cuerpo legislativo aplicable a la informática, toda vez que muchos congresistas, jueces y magistrados están ajenos a la problemática actual que el fenómeno informático presenta.

En 1984, la Gran Comisión del Senado de la República encomendó a su Comisión Especial de Informática, identificar las necesidades de legislación en esta materia, y en su caso proponer un proyecto para el establecimiento de un marco normativo.

En 1985, se creó el Centro de Informática Legislativa del Senado (CILSEN) como órgano dependiente del Senado de la República; y cuya encomienda principal se basó en la elaboración de un documento titulado "Marco Normativo de la Informática en México", el cual a grandes rasgos, presentaba un aspecto general del estado de la normatividad existente en torno a la informática en México, un proyecto de exposición de motivos sobre la necesidad de establecer un marco normativo en materia de informática, y un proyecto por el que se adicionaba la palabra informática a la fracción X del Art. 73 Constitucional.

De dicho proyecto se realizó un análisis sustentado principalmente en dos áreas de estudio: en la primera, se estudió el rubro relativo a la "Legislación relacionada con la informática", la cual comprende todas aquellas leyes, reglamentos, acuerdos, tratados internacionales, entre otros que son aplicables a las tecnologías de la información. Y en la segunda se estudió primordialmente lo relativo a la "Legislación específica sobre Informática", integrada específicamente por normas que hacen referencia expresamente a dicho término.

Algunas de las conclusiones sustanciales que se obtuvieron del estudio realizado, fueron que:

- No existe a nivel constitucional disposición específica en torno a la materia informática. Solo algunas disposiciones constitucionales son aplicables en ciertos casos a dicha tecnología.
- Además, la Constitución no otorga facultad al Congreso de la Unión para legislar en materia informática. Ninguna de las facultades explícitas preceptuadas en el Art. 73 Constitucional, son aplicables como fundamento para legislar en torno a la materia.
- Por otra parte, algunos cuerpos legislativos plantean numerosos problemas y situaciones en los que la informática está presente.

- Ante la ausencia de un marco jurídico aplicable a la informática, se ha tenido que recurrir a la creación de reglamentos, con el fin de dar solución a situaciones concretas que ya se han presentado, derivadas del uso y aplicación de la informática en la sociedad.
- Las entidades federativas por su parte, también han expedido en forma reglamentaria, algunas normas con el fin de regular algunos aspectos motivados por la aplicación de la informática.

De lo anterior se concluye, que existe en México un gran vacio legislativo en torno a la materia Informática; por lo que se tiene la imperiosa necesidad de legislar al respecto, tanto a nivel constitucional, como a nivel de legislación ordinaria; fundamentalmente en aspectos tales como: garantías individuales, sociales y politicas; seguridad nacional, soberania nacional, flujo de datos transfronterizos, contratos informáticos, regulación de bienes informacionales, protección de programas computacionales, promoción del desarrollo científico, promoción de la enseñanza de la informática en los niveles de educación básica y formación de profesionistas e investigadores, valor probatorio de los soportes modernos de información y; en materia de delitos informáticos, que es la problemática que se aborda en el cuerpo de la presente.

CAPÍTULO 3
DELITOS INFORMÁTICOS

3.1. GENERALIDADES DEL DELITO.

3.1.1. Definición del término "delito".

Para determinar la existencia de los delitos informáticos, es necesario en primer término definir qué se entiende por delito. De acuerdo a lo establecido por el autor Fernando Castellanos Tena en su obra "Lineamientos Elementales de Derecho Penal", la palabra delito "se deriva del verbo latino *delinquere,* que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley"[20].

Los simpatizantes de la "Escuela Clásica" elaboraron diversas definiciones respecto al término delito. El principal exponente de esta corriente, Fernando Carrara, lo define como "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"[21].

Para Carrara, el delito es un ente jurídico, en virtud de que su esencia deriva de una violación al Derecho. También lo considera como una infracción a

[20] Castellanos Tena, Fernando. Lineamientos Elementales de Derecho Penal (Parte General). Trigésima Cuarta Edición. Editorial Porrúa., México, D.F., 1994. Pág.125.
[21] Obra citada. Págs. 125,126.

la Ley del Estado, toda vez que un acto se convierte en delito al transgredir dicha Ley, la cual ha sido promulgada para proteger la seguridad de los ciudadanos. Además, precisa que el delito es una infracción resultante de un acto externo, positivo o negativo del hombre; con lo cual se determina que solamente el hombre puede ser agente activo del delito, tanto en sus acciones como en sus omisiones. Y finalmente considera que dicho acto es moralmente imputable al hombre por estar el individuo sujeto a leyes criminales en virtud de su naturaleza moral.

Para la Escuela del Positivismo, cuyo principal exponente fue el jurista Rafael Garófalo; el delito es un fenómeno o hecho natural que se da como consecuencia necesaria de factores hereditarios, de causas físicas y de fenómenos sociológicos.

De acuerdo a la concepción sociológica de Rafael Garófalo, el delito natural es "la violación de los sentimientos altruistas de probidad y de piedad, en la medida media indispensable para la adaptación del individuo a la colectividad"[22].

Esta noción sociológica del delito no tiende a definir al delito como un hecho natural, ya que el delito como tal debe entenderse como un acto; en cierto sentido lo que buscaba dicha definición, era describir la esencia del delito como fruto de una valoración de ciertas conductas, según determinados criterios de utilidad social, de justicia, de altruismo, de orden, de disciplina, etc., que determinen aquéllas conductas que habrán de ser consideradas como delictuosas.

[22] Castellanos Tena, Fernando. Obra citada. Pág. 126.

3.1.2. Concepto jurídico del término "delito".

La concepción jurídica del término delito es formulada desde el punto de vista del Derecho; y al respecto se han elaborado tanto definiciones de tipo formal como de carácter sustancial.

Por lo que hace a la noción formal del término delito, ésta es proveída por la ley positiva, al advertir la imposición de una pena o sanción por la ejecución u omisión de ciertos actos. De ahí que no sea posible hablar de delito, sin la existencia de una ley que sancione una determinada conducta.

Para Edmundo Mezger, el delito es en su acepción jurídica "una acción punible; esto es, el conjunto de los presupuestos de la pena"[23]. Lo que Mezger quería significar al referirse al delito como una acción punible, era que por delito debía entenderse toda acción que estuviera sancionada con una pena.

En México, el ordenamiento jurídico que define al delito es el Código Penal Federal; el cual dispone en su artículo 7°, primer párrafo, que "delito es el acto u omisión que sancionan las leyes penales". De tal modo, que de esta definición se advierte, que nada puede ser castigado sino por hechos que la ley ha definido previamente como delitos; ni tampoco podrá ser sancionado con otras penas que las establecidas en la propia ley. De igual forma se entiende, que la consumación de un delito se obtiene por el simple hecho de infringir la ley, independientemente del resultado que se dé a consecuencia de ello. En el momento preciso en que se vulnera la ley, se provoca el delito.

El Código Penal para el Estado de Veracruz, no define en su articulado lo que debe concebirse como "delito", únicamente se concreta a estipular en su Artículo 9° que "el delito puede ser realizado por acción u omisión"; por lo que se considera que la alusión que el Código Penal del Estado hace respecto al

[23] Castellanos Tena, Fernando. Obra citada. Pág. 128.

término delito es vaga e imprecisa; situación que provoca se tenga que remitir al Código Penal Federal, para encontrar la definición formal que la propia ley le otorga al término en estudio.

Por lo que respecta a la noción jurídica – sustancial del término delito, existen dos sistemas encargados del estudio jurídico - esencial del delito: el sistema unitario o totalizador, y el sistema analítico o atomizador.

El primer sistema establece que el delito no puede dividirse, por ser parte integrante de un todo orgánico, se trata pues, de un concepto indisoluble. Para los seguidores de esta doctrina, el delito se presenta como un bloque monolítico, que no es fraccionable de modo alguno.

En cambio, los afiliados al sistema analítico o atomizador; estudian el ilícito penal por sus elementos constitutivos. Ellos consideran que para entender el todo, se precisa del conocimiento cabal de cada una de sus partes integrantes; sin embargo aceptan que el delito integra necesariamente una unidad.

En base a estos dos sistemas, Mezger elabora una definición jurídica - sustancial del término delito, en la cual expresa que "el delito es la acción típicamente antijurídica y culpable"[24].

En el mismo sentido, Cuello Calón, concibe al delito como "la acción humana antijurídica, típica, culpable y punible"[25].

Por su parte, Jiménez de Asúa, considera que el "delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal"[26].

---

[24] Castellanos Tena, Fernando. Obra citada. Pág. 129.
[25] Obra Citada. Pág. 129.
[26] Obra citada. Pág. 130.

La definición jurídico-sustancial de delito formulada por Jiménez de Asúa, integra como elementos del delito: la acción, la tipicidad, la antijuridicidad, la imputabilidad, la culpabilidad, la punibilidad y las condiciones objetivas de punibilidad; elementos que serán descritos a continuación.

3.1.3. Elementos Positivos y Negativos del Delito.

Los elementos del delito son estudiados desde dos perspectivas o puntos de vista, de acuerdo al sistema propuesto por Guillermo Sauer y retomado a su vez por Jiménez de Asúa.

De acuerdo a dicho método se contrapone lo que el delito es, a lo que no es; y así se tiene que los elementos integrantes del delito son en su:

ASPECTO POSITIVO	ASPECTO NEGATIVO
• La actividad.	• Falta de acción.
• Tipicidad.	• Ausencia de tipo o Atipicidad.
• Antijuridicidad.	• Causas de justificación.
• Imputabilidad.	• Causas de inimputabilidad.
• Culpabilidad.	• Causas de inculpabilidad.
• Punibilidad.	• Excusas absolutorias.

El primer elemento objetivo del delito en su aspecto positivo lo es la actividad. En sentido amplio, el delito es ante todo una conducta humana, en la cual se incluye tanto el hacer positivo "acción", como el negativo "omisión".

Ahora bien, se advierte que este primer elemento objetivo del delito puede presentarse en forma de acción, omisión o comisión por omisión. Mientras que la acción se manifiesta a través de la ejecución de una actividad voluntaria, la omisión y la comisión por omisión se conforman por una inactividad. El aspecto

que diferencia a la omisión y a la comisión por omisión es, que en la omisión hay violación de un deber jurídico de obrar, en tanto que en la comisión por omisión hay violación de dos deberes jurídicos, uno de obrar y otro de abstenerse.

En sentido estricto, la acción "es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación"[27].

En cambio, la omisión, radica en una abstención de obrar; es " dejar de hacer lo que se debe de ejecutar"[28]. Por lo tanto, se considera que la omisión es una forma negativa de la acción; ya que en los delitos de acción el sujeto activo ejecuta un acto prohibido por la ley, en tanto que en los delitos de omisión, éste deja de hacer lo estipulado expresamente por la misma.

Por lo que hace a la ausencia de acción, como aspecto negativo del primer elemento objetivo del delito; se afirma que si falta alguno de los elementos esenciales del delito, éste no puede integrarse; en consecuencia, si hay ausencia de conducta, no se produce el delito.

El segundo elemento objetivo del delito en su aspecto positivo lo es, la tipicidad, entendiéndose por ésta "el encuadramiento de una conducta con la descripción hecha en la ley"[29]. Es en pocas palabras, la adecuación de la conducta al tipo penal descrito por la ley.

En tal sentido, se considera que no existe delito sin tipicidad. Cuando no se integran todos los elementos descritos en el tipo penal, se da el aspecto negativo de la tipicidad , que es la ausencia de adecuación de la conducta al tipo o

---

[27] Castellanos Tena, Fernando. Obra citada. Pág. 152.
[28] Obra citada. Págs. 152,153.
[29] Obra citada. Pág. 168.

también llamada "atipicidad". Si la conducta no se amolda al tipo descrito por la ley, no puede ser considerada un delito.

En cuanto a la antijuridicidad como tercer elemento objetivo del delito, se dice que éste es un concepto negativo. La antijuridicidad radica "en la violación del valor o bien protegido a que se contrae el tipo penal respectivo"[30]. En otras palabras, una conducta es antijurídica, cuando transgrede una norma jurídica establecida por el Estado, causando en ese acto un daño o perjuicio social producto de dicha rebeldía.

La ausencia de antijuridicidad como factor negativo del elemento del delito en cuestión, lo constituyen las causas de justificación. Puede ocurrir que la conducta típica esté aparentemente en oposición al Derecho, sin embargo, no será antijurídica si existe una causa de justificación. Las causas de justificación, son aquellas condiciones que tienden a excluir la antijuridicidad de una conducta establecida en el tipo penal; de tal modo, que en tales condiciones, la acción realizada no será considerada antijurídica, en virtud de existir una justificante que hace que dicha conducta resulte apegada a Derecho. Las causas de justificación previstas por la ley penal son: la legítima defensa, el estado de necesidad, cumplimiento de un deber, ejercicio de un derecho, obediencia jerárquica e impedimento legítimo.

La imputabilidad es el cuarto elemento objetivo del delito, y se define como "la capacidad de entender y de querer en el campo del Derecho Penal"[31]. Se puede considerar entonces que un sujeto será imputable, si reúne todas aquellas condiciones psíquicas exigidas por la ley al momento de realizar el acto típico penal, las cuales lo capacitan por tanto para responder del mismo. Se afirma que

[30] Castellanos Tena, Fernando. Obra citada. Pág. 178.
[31] Obra citada. Pág. 218.

la imputabilidad está determinada por dos aspectos de tipo psicológico: un mínimo físico representado por la edad del sujeto (desarrollo mental), y otro de carácter psíquico consistente en la salud mental.

La inimputabilidad constituye el aspecto negativo de la imputabilidad. Son causas de inimputabilidad, todas aquéllas capaces de anular o inhabilitar el desarrollo o salud mental del sujeto, en cuyo caso, éste carecerá de aptitud psicológica para ser sujeto del delito. En el Código Penal Federal son consideradas causas de inimputabilidad: la minoría de edad, el trastorno mental, el desarrollo intelectual retardado, el miedo grave y el temor fundado. De esta forma, los protegidos por las eximentes de inimputabilidad deben quedar al margen de toda consecuencia represiva o asegurativa, en virtud de haber realizado el hecho penalmente tipificado sin capacidad de juicio y decisión

La culpabilidad es otro de los elementos objetivos del delito, y se considera como la capacidad que tiene el sujeto para entender y querer en el campo del Derecho Penal; por lo tanto, se afirma que la imputabilidad funciona como presupuesto de la culpabilidad. Un sujeto será culpable, siempre y cuando se dé el nexo intelectual y emocional que ligue al sujeto con el acto que perpetró, de tal manera que dicho acto pueda serle reprochado jurídicamente. La culpabilidad reviste tres formas: el dolo, la culpa y la preterintencionalidad.

El factor negativo de la culpabilidad lo constituye la inculpabilidad. La inculpabilidad se da ante la ausencia del conocimiento y de la voluntad, que conforman los elementos esenciales de la culpabilidad; por lo tanto, toda causa eliminatoria de alguno de estos dos aspectos, es considerada como causa de inculpabilidad. Para muchos autores las causas de inculpabilidad son el error y la no exigibilidad de otra conducta; o dicho en otras palabras, el error esencial de hecho (que ataca el elemento intelectual) y la coacción sobre la voluntad (que afecta al elemento volitivo).

Por lo que respecta a la punibilidad como sexto elemento objetivo del delito, se dice que ésta consiste en la imposición de una pena en función de la realización del acto penalmente tipificado y sancionado por la ley. Es punible una conducta, cuando por su propia naturaleza amerita ser sancionada.

Cuando hay ausencia de punibilidad se dice que se está en presencia de las excusas absolutorias, las cuales como se puede apreciar, constituyen el factor negativo de la punibilidad. Al concurrir en el acto alguna excusa absolutoria, no es posible determinar la aplicación de una pena.

El autor Fernando Castellanos Tena, hace mención en su obra "Lineamientos Elementales de Derecho Penal", de las que a su juicio son consideradas como las principales excusas absolutorias y menciona como tales las siguientes: excusa en razón del arrepentimiento y mínima temibilidad del agente, excusa en razón de la maternidad consciente (en el caso de un aborto causado sólo por imprudencia de la mujer, o cuando el embarazo sea resultado de una violación), excusa por inexigibilidad de la conducta (como en el caso del encubrimiento de parientes y allegados , o de la falsa declaración de un encausado), excusa por graves consecuencias sufridas por el sujeto activo, en su persona, de tal manera que se hace notoriamente innecesario e irracional la imposición de una pena.

3.2. GENERALIDADES DE LOS DELITOS INFORMÁTICOS.

3.2.1. Orígenes.

Como ya se ha mencionado, la informática ha irrumpido en el mundo y ha ido penetrando en cada uno de los aspectos de la vida cotidiana, brindando múltiples beneficios a la sociedad; sin embargo, de la misma manera en como representa una herramienta muy favorable, también se ha convertido en un instrumento para la comisión de verdaderos actos ilícitos.

Este tipo de actitudes ilícitas encuentra sus orígenes en el propio surgimiento de la tecnología informática, ya que es imposible concebir al delito informático, sin la existencia de las computadoras.

Es así como en las últimas cuatro décadas, aparece un nuevo tipo de acto delincuencial, cuyo sujeto activo no usa herramientas típicas para cometerlo; sino que ahora maneja y tergiversa la información, valiéndose de los medios electrónicos a su alcance y en la más completa libertad, de ahí su peligrosidad.

La misma facilitación de actividades que trae aparejado consigo el uso de los medios informáticos, ha suscitado que el usuario de los mismos se encuentre en un momento dado en un estado de ocio, el cual canaliza a través de las computadoras, cometiendo en muchas ocasiones, una serie de ilícitos.

El delito informático o electrónico aumentó su número de acciones delictivas en un término muy corto. La popularidad que últimamente han tenido las computadoras personales, ha provocado un mayor número de usuarios y con ello, el potencial delictivo ha ido en aumento.

Hay una infinidad de ilícitos que se producen a través de las computadoras, y los delincuentes electrónicos proliferan día a día; es por tal motivo que se hace cada vez más necesaria, la existencia de una reglamentación jurídica adecuada a los nuevos tiempos, que trate de evitar en lo posible, la comisión del delito electrónico o informático y sus efectos.

3.2.2. Concepto.

Establecer un concepto sobre "delitos informáticos" es una labor difícil, en virtud de que para hablar del término "delitos informáticos", se requiere que éstos estén contemplados en los textos jurídicos-penales de los países.

En México, con excepción del Estado de Sinaloa, los delitos informáticos no existen, ya que los mismos no se encuentran regulados por disposición penal alguna; por tal motivo se considera que dicho tipo de ilícitos constituye una gran laguna en las leyes penales del país.

Algunas personas consideran que los delitos informáticos como tales no existen, argumentan que solo se trata de delitos normales cuya única diferencia estriba en el tipo de herramientas empleadas para cometer el ilícito o en los objetos sobre los cuales se produce. Sin embargo, esta es una visión muy limitada a la realidad.

No obstante a lo que muchas personas piensan, algunos tratadistas penales que han incursionado en el tema, se han dado a la tarea de conceptualizar el término "delitos informáticos o electrónicos".

Al respecto la Dra. Luz Ma. Del Pozo y Contreras considera que "delito electrónico es aquél que se comete con el uso de las computadoras o cualquier otro medio electrónico como pueden ser las telecomunicaciones"[32].

El autor Julio Téllez Valdés elabora un concepto típico y uno atípico para definir el término "delitos informáticos". De esta manera establece que "los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[33].

---

[32] http://www.cddhcu.gob.mx/camdip/foro/, "Foro de Consulta sobre Derecho e Informática (Memorias)", Ponencia: "Mecanismos existentes con ausencia de estructura , el Derecho Informático, el Delito Electrónico", Autor: Dra. Luz Ma. Del Pozo y Contreras, Poder Legislativo Federal, Biblioteca del H. Congreso de la Unión, Guadalajara, Jalisco., Septiembre, 1996.

[33] Téllez Valdés, Julio. Obra citada. Pág. 104.

En el mismo sentido, María de la Luz Lima define el delito por computadora como "cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o fin".[34]

El autor español Romeo Casabona se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual, "delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución"[35].

Para el autor Davara Rodríguez, resulta inadecuado hablar de "delito informático", ya que considera que como tal éste no existe, si se atiende a la necesidad de una tipificación en la legislación penal para que pueda existir un delito; y en virtud de que el Código Penal Español no introduce el delito informático, resulta inapropiado referirse a dicho término.

Sin embargo, admite la expresión por conveniencia y define como delito informático " la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[36].

Parker conceptualiza a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría de obtener un beneficio"[37].

---

[34] Ríos Estavillo, Juan José. Obra citada. Pág. 116.
[35] http://www.jose_cuervo.lettera.net, Página de José Cuervo Álvarez, "Delitos Informáticos: Protección Penal de la Intimidad", España , 29 de Mayo de 1997.
[36] Página de internet citada.
[37] Página de internet citada.

La definición que presenta la Organización para la Cooperación Económica y el Desarrollo señala que "cometerá delito informático la persona que maliciosamente 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, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red"[38].

Y finalmente, para el autor Ruiz Vadillo, que recoge la definición aportada por la Organización para la Cooperación Económica y el Desarrollo, "delito informático, es todo comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos"[39].

En virtud de lo anteriormente descrito, se puede concluir estableciendo que por "delito informático" se debe entender, toda conducta no ética, típica, antijurídica, culpable y punible cometida a través de cualquier sistema informático y/o telemático, ya sea que éste sea empleado como medio o como fin para llevar a cabo el delito.

3.2.3. Características.

Desde un punto de vista general, se han determinado ciertas características fundamentales de los delitos informáticos, entre las cuales se mencionan las siguientes:

- Son conductas criminógenas de cuello blanco, en virtud de que sólo un determinado número de personas con los conocimientos suficientes en el

[38] Ríos Estavillo, Juan José. Obra citada. Pág. 116.
[39] http://www.jose_cuervo.lettera.net.

ámbito de la informática puede llegar a cometerlos; sin embargo en la actualidad, el número de delincuentes informáticos se ha incrementado, debido a que los medios para cometer un delito de esta naturaleza están al alcance de casi todos los individuos.

- Son acciones que en múltiples ocasiones se llevan a cabo durante el desarrollo de las actividades profesionales del individuo, es decir, cuando el sujeto se encuentra laborando.

- Son acciones que se llevan a cabo aprovechando una ocasión, en la mayoría de las veces, creada por el propio sujeto, por lo que se les llama acciones de oportunidad.

- Son de consumación casi instantánea, ya que en milésimas de segundo y sin requerir necesariamente de una presencia física, pueden llegar a realizarse.

- Provocan grandes daños y pérdidas económicas a sus víctimas.

- Los casos de delitos informáticos son cada vez más, y las denuncias contra éstos son muy pocas, lo cual, ante la ausencia de disposiciones reguladoras al respecto, contribuye a que la delincuencia informática siga proliferando.

- Debido a su carácter técnico, son muy difíciles de comprobar; por lo que procuran a sus autores una probabilidad bastante alta de alcanzar sus objetivos sin ser descubiertos.

- Por estar los sistemas informáticos al alcance de todos los individuos; ofrecen grandes facilidades para su comisión, incluso a menores de edad.

- Carecen de regulación jurídica en las Legislaciones Penales del país, por lo que siguen considerándose como ilícitos impunes en México.

- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

De lo anterior, se advierte la peculiaridad que guardan los delitos informáticos frente a otro tipo de conductas criminales, lo que los distingue como una nueva modalidad de ilícitos cometidos a través de los medios informáticos.

3.2.4. Clasificación.

Para algunos autores, los delitos informáticos se pueden clasificar, atendiendo al provecho que producen para el autor del delito y el daño que provocan en los sistemas informáticos como entes físicos; o bien, en atención al agravio que le ocasionan a un individuo o grupos de individuos, en su integridad física.

Para otros, la clasificación de los delitos informáticos se realiza de acuerdo a los fines que se persiguen al cometer las conductas delictivas en los sistemas informáticos, desde esta perspectiva dichos delitos se clasifican atendiendo a dos puntos de vista:

- Delitos con medios informáticos, que son aquéllos en los cuales la computadora o sistemas informáticos son empleados como herramientas o medios de comisión del delito.

- Delitos contra medios informáticos, que son aquéllos en los cuales se provoca una lesión en el contenido de la información de un sistema, causando un perjuicio o afectación a los datos procesados o almacenados, o bien, a los propios programas del sistema.

Por su parte, el autor Juan Diego Castro Fernández establece que hay ciertos delitos informáticos que se adecuan a figuras tipificadas en el Código Penal, y en atención a los bienes jurídicamente afectados, realiza la siguiente clasificación de los delitos informáticos:

- Delitos contra las personas: Lo cual se puede dar desde el punto de vista de que la medicina moderna ya cuenta con sistemas informáticos como medios para diagnóstico clínico, por lo que es posible que se pueda dar un uso indebido de la computadora, por dolo o culpa del médico, ocasionando con ello un agravio en contra del paciente.

- Delitos contra el honor: Esto puede suceder en el caso de que se incluya información falsa de carácter injurioso en un archivo electrónico de un determinado individuo, lo cual al momento de darse a conocer cause un perjuicio al honor de la persona; o bien, que se conserve información falsa de alguna persona en registros electrónicos.

- Delitos contra la propiedad: La mayoría de los delitos informáticos encuadran dentro de esta subclasificación, en virtud de que en múltiples ocasiones el móvil de éste tipo de delitos es afectar un bien propiedad de alguien. En este sentido, los principales delitos contra la propiedad, según lo establecido por el autor Castro Fernández son los siguientes:

  - Manipulación (Fraude Informático): Existe manipulación en el programa o consola, lo cual puede afectar tanto a la fase de suministro o alimentación de datos, como a su salida o procesamiento.
  - Espionaje: Mediante esta actividad se obtienen datos o programas sin autorización de su propietario o titular, o bien, se divulgan aquéllos que han sido obtenidos legítimamente.
  - Sabotaje: Este tipo de conductas se propone la destrucción o incapacidad

de los sistemas informáticos o de algún elemento que las estructura (hardware o software).

- Hurto de tiempo: Es la utilización indebida de los sistemas informáticos por parte de los empleados o extraños, cuestión que puede provocar pérdidas considerables, especialmente en los sistemas de procesamiento de datos a distancia, en los cuales se emplean accesos con números de cuenta ajenos.

Para Julio Téllez Valdés , los delitos informáticos deben clasificarse en atención a dos criterios: como instrumentos o medio, o como fin u objetivo. De tal forma entre las principales conductas criminógenas que emplean a las computadoras como medio para la comisión del delito, se encuentran:

- Falsificación de documentos a través de los sistemas informáticos (tarjetas de crédito, cheques, etc).
- Variación de los activos y pasivos de la contabilidad de las empresas.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc).
- Robo de tiempo de computadora.
- Lectura, sustracción o copiado de información confidencial de la base de datos.
- Modificación de datos (en su entrada o salida).
- Aprovechamiento indebido o violación de un código para introducirse a un sistema con el fin de infiltrar instrucciones inapropiadas (esto es lo que se conoce con el nombre de Caballo de Troya).
- Variación en cuanto al destino de cantidades de dinero hacia cuentas bancarias apócrifas, método comúnmente conocido como "Técnica del Salami".
- Uso no autorizado de programas de acceso universal (Superzzaping o Llave Maestra).

- Puertas con trampa , es decir, utilización de interrupciones en la lógica de un programa en la fase de desarrollo para su depuración y uso posterior de éstas con fines lucrativos.
- Alteración del funcionamiento de los sistemas informáticos a través de los "virus informáticos".
- Obtención de información residual, obtenida a través de la impresión de trabajos o de la captura en cinta magnética en memoria después de la ejecución de un trabajo.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención de las líneas de comunicación para acceder o manipular los datos que son transmitidos.

Dentro de las conductas criminógenas que van dirigidas en contra de los sistemas informáticos como entidad física (clasificación de los delitos informáticos como fin u objetivo) se encuentran los siguientes:

- Programación de instrucciones que tienen como fin bloquear en forma total el sistema.
- Destrucción de programas.
- Daño a la memoria de los sistemas informáticos.
- Daños o atentados físicos contra la computadora y sus accesorios.
- Sabotaje político o terrorismo, en los cuales se destruye o haya un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos que contengan información valiosa con fines de chantaje (pago de rescate, etc.)

Para otros, a pesar de que el término delito informático engloba tanto a los delitos cometidos en contra de los sistemas informáticos, como a los cometidos mediante su uso, proponen realizar la siguiente clasificación:

- Delitos e infracciones tradicionalmente denominados informáticos: Dentro de los cuales se pueden destacar:

❖ El acceso no autorizado a sistemas informáticos, mediante el uso ilegítimo de passwords.

❖ Destrucción de datos (a través de los llamados "virus informáticos", bombas lógicas y demás actos de sabotaje informáticos.

❖ Infracción de los derechos de autor.

❖ Infracción del copyright de bases de datos.

❖ Interceptación de e-mail (violación de la correspondencia).

❖ Estafas electrónicas (a través de la proliferación de compraventas telemáticas).

❖ Transferencia de fondos.

- En un segundo término, clasifican a los delitos informáticos en "delitos convencionales", es decir, aquéllos que están plenamente tipificados por las legislaciones penales de los países, y en los cuales no se requiere el empleo de medios informáticos para su comisión, y son los siguientes:

❖ Espionaje. (se han dado casos de acceso no autorizados a sistemas informáticos gubernamentales, así como interceptación del correo electrónico del servicio secreto).

❖ Espionaje Industrial. (la existencia de hosts, que permiten guardar la identidad de los remitentes, ha sido aprovechada en muchas ocasiones por terroristas, para remitirse consignas y planear su actuación a nivel internacional.

❖ Narcotráfico: Es común el envío de mensajes encriptados entre narcotraficantes, para ponerse de acuerdo con los cárteles, por lo que el FBI y el Fiscal General de los Estados Unidos, han alertado sobre la necesidad de establecer medidas que permitan interceptar y descifrar dichos mensajes.

- Y en una tercera clasificación establecen los malos usos o también llamados cybertorts, entre los cuales se encuentran los siguientes:
  - ❖ Usos comerciales no éticos.
  - ❖ Actos parasitarios (como obstaculización de comunicaciones ajenas, mensajes con insultos personales, interrupciones en formas repetidas, etc).
  - ❖ Obscenidades: Entre los cuales se pueden encontrar los insultos; mensajes raciales, satánicos u otros; y el llamado terrorismo informático, que consiste en mostrar fotografías pornográficas e imágenes que muestran violencia, muerte y destrucción en páginas destinadas a niños y a adolescentes.

De acuerdo a lo reseñado con anterioridad, se puede concluir estableciendo que la clasificación general que se hace en torno a los delitos informáticos, atiende principalmente al fin que se persigue al momento de llevar a cabo la conducta ilícita que llega a afectar negativamente a un tercero.

Es así como finalmente se puede llegar a considerar que por cuanto hace a los delitos informáticos, existen tres tipos de comportamiento que se adecuan básicamente a su comisión:

1. El acceso no autorizado, que hace deliberadamente un usuario a una red, un servidor o un archivo.
2. Actos dañinos o circulación de material dañino, que se traduce en el robo o copia de archivos (piratería); introducción de información negativa o de virus informáticos; alteración, modificación o destrucción de datos o de software (sabotaje).
3. Interceptación no autorizada, en la cual el infractor obtiene información no dirigida a él, mediante la intrusión de comunicaciones relativas a sistemas informáticos o telemáticos.

El autor Olivier Hance cita en su obra "Leyes y Negocios en Internet" que las estadísticas más recientes sobre la comisión de delitos informáticos, indican alrededor de 72 mil intentos diarios por lograr acceso ilegal a algún sistema informático, además establece que "se estima que aparecen seis virus nuevos cada día y se han identificado más de mil virus informáticos"[40].

La cantidad de estas operaciones fraudulentas da una idea del daño informático y económico que se genera con la comisión de este tipo de ilícitos. Tan sólo en Estados Unidos, se calcula que se generan perjuicios económicos por los delitos informáticos que superan los 10.000 millones de dólares; en México la situación es menos impactante, sin embargo la necesidad de establecer una solución que frene tal problemática a la brevedad posible es algo de vital importancia.

3.2.5. Bien jurídico tutelado en los delitos informáticos.

El concepto de bien jurídico fue empleado por primera vez por Ihering para precisar el objeto de protección de las normas de derecho. Para algunos otros juristas como Nawiasky, se debe hablar de fin jurídico o interés jurídicamente protegido, pues el concepto positivista de derecho subjetivo cabe perfectamente en estos términos.

De acuerdo a la teoría positiva, el bien jurídico es arbitrariamente fijado por el legislador de acuerdo a su criterio. Según la misma, el legislador observa la realidad social, y de acuerdo a ésta y a su ideología, determina cuáles son los objetos a proteger. Puede determinar que sean la vida, la libertad, la propiedad, etc.; y la forma que se utiliza para proteger dichos bienes jurídicos determinados por el legislador, es mediante el uso de una sanción que puede ser civil o penal.

---

[40] Hance, Olivier. Suzan Dionne Balz. Leyes y Negocios en Internet. Traducción: Yasmín Juárez Parra. Revisión Técnica: Gabriela Barrios Garrido. Edit. Mc Graw Hill (Sociedad Internet de México). México, 1996. Traducido de la Primera Edición en Inglés de Business and Law on the Internet. , Pág. 101.

La Constitución Mexicana, consigna los bienes jurídicos que el legislador consideró que deberían estar protegidos. De esta forma, el Artículo 14 Constitucional indica que nadie puede ser privado de la vida, de la libertad, de sus propiedades, posesiones o derechos, sino como la propia Constitución prescribe.

El hablar de bienes jurídicos, es hablar de valores esenciales para la sociedad que, por su importancia, son protegidos por el derecho penal mediante la tipificación de delitos que atentan en su contra. Así, cada tipo delictivo consignado en el Código Penal protege un bien jurídico.

Sin embargo, por lo que se refiere a la materia que se analiza en este trabajo de investigación; existe una gran problemática, ya que no se ha llegado a identificar y justificar plenamente, desde la perspectiva normativa y doctrinal, el bien jurídicamente tutelado en los delitos informáticos; tal parece que los autores y legisladores de los países en donde dichos ilícitos ya se encuentran regulados aún no se ponen de acuerdo en cuál es el bien jurídico vulnerado al cometerse un delito de esta índole.

En su obra "Derecho e Informática en México", Juan José Ríos Estavillo, establece que se debe de identificar plenamente en un esquema primario, el bien jurídicamente tutelado en los delitos informáticos. Al respecto opina, "no podemos decir que lo que se tutela es la intimidad o la protección de la información personal, porque no sólo se protegen éstos, sino también aquellos que deriven de la seguridad nacional, o datos en materia de seguridad pública o en seguridad industrial, por lo cual no podemos tomar una parte como el todo, sino al todo con todas sus partes"[41].

[41] Ríos Estavillo, Juan José. Obra citada. Pág. 128.

Por lo tanto, según lo aseverado por este autor, se debe considerar que el bien jurídicamente tutelado en los ilícitos informáticos es la "información" en general, ya que, por las características de los delitos informáticos, lo que se protege es la información contenida en bancos y bases de datos, redes de computadoras o simples computadoras personales; comprendiendo dentro de dicha información, tanto la que se deriva de un lenguaje natural como del informático.

De allí que el término "información" deba ser entendido en este sentido, no solo como una simple acumulación de datos, sino como el proceso de "almacenamiento, tratamiento y transmisión de datos mediante los sistemas de procesamiento e interconexión"[42]. Dicho significado le ha concedido al término en cuestión un gran valor, al grado de considerarlo un interés social valioso, dotado de autonomía y objeto del tráfico, lo que justifica su tutela en el campo del derecho penal.

Ahora bien, una vez que se ha establecido que la "información" es el interés social digno de tutela penal en los delitos informáticos; hay que determinar si se está frente a un bien jurídico penal de carácter individual o colectivo.

Luis Miguel Reyna Alfaro sostiene que "el bien jurídico propuesto está dirigido a resguardar intereses colectivos, cercanamente relacionado al orden público económico, aunque pueden concurrir a su vez intereses individuales, que en éste específico caso serían los de los propietarios de la información contenida en los sistemas de tratamiento automatizado de datos"[43].

El carácter colectivo que se le atribuye al bien jurídico tutelado en los

---

[42] www.vlex.com , Perú: El Bien Jurídico en el Delito Informático , Luis Miguel Reyna Alfaro, Doctrina – Análisis y Artículos.
[43] Página de internet citada.

delitos informáticos, se da tomando en consideración que la información es un interés social vinculado a la actividad empresarial.

La valoración del merecimiento de protección que se le debe otorgar a aquellos intereses que, como la información, tienen un inminente carácter colectivo, debe abordarse en función de la trascendencia que dicho bien tenga para los individuos.

Mir Puig señala que "la valoración de la importancia de un determinado interés colectivo exigirá la comprobación del daño que cause a cada individuo su vulneración"[44], esto quiere decir, que no resulta suficiente que el interés social trascienda a la generalidad para que se compruebe el merecimiento de su protección, sino que precisa también que su lesión o puesta en peligro puedan provocar un daño a los individuos integrantes del grupo social.

En contraposición a lo anteriormente señalado; para otros autores como Luis Manuel C. Meján, el bien que se debe tutelar en los delitos informáticos es la "intimidad", y más específicamente la "intimidad informática".

Dicho autor establece que aunque el derecho vigente en el país contiene un buen número de disposiciones que regulan la materia de la intimidad y la información, es evidente que hay lagunas que han sido creadas por el avance tecnológico, las cuales deben ser colmadas con una adecuada legislación sobre la intimidad y en específico, sobre la intimidad informática, en la que se estipulen y regulen los derechos de los individuos a conocer, modificar, extraer las informaciones que sobre sí, obtienen tanto de los particulares, como el Estado, y el uso correcto que debe hacerse de dicha información.

[44] Mir Puig, S. Delincuencia Informática. Promociones y Publicaciones Universitarias. Librería Bárbara de Bragaza, 8. Oficinas y Revistas Tamayo y Baus, 728004. Barcelona, 1992, Pág. 98.

Asimismo afirma, que la inclusión de la intimidad informática como garantía fundamental en el texto de la Carta Magna, "sería un reconocimiento justo a la dignidad del ser humano en la problemática que nuestro tiempo pide"[45].

En efecto, tal como lo asevera Fabio Rubén Troncozo Auld, en su estudio titulado "México: El Derecho a la Intimidad y el Derecho a la Información ¿Garantías encontradas?", el hombre al nacer lo hace libre físicamente, y él mismo, tiene libertad para dar a conocer de sí ante los demás lo que su voluntad le sugiera; pero con la informatización de la sociedad, esto parece ser imposible. Con la gran inseguridad existente en el almacenamiento, ensayo, recopilación o transmisión de datos en las redes de las empresas públicas o privadas; así como con la manipulación de sistemas informáticos ajenos, la intimidad de las personas se ve quebrantada.

Si bien es cierto que la información es un elemento indispensable en la vida del hombre para la adecuada toma de decisiones, y que el hombre nace con el derecho a estar informado; también es cierto que el mismo tiene plena facultad para decidir qué información desea compartir con los demás individuos de su sociedad y cuál desea reservar para sí mismo.

En este sentido es posible apreciar que, "tanto el derecho a la información como el derecho a la intimidad, son derechos fundamentales en la vida del hombre de estos tiempos. No obstante la distancia que guardan ambos conceptos, se encuentran, hoy en día, estrechamente vinculados, esto debido al mal sentido que se le ha dado al derecho de ser informado, pues abusando de este último es como se transgrede el derecho a la intimidad"[46].

---

[45] Meján, Luis Manuel C. El Derecho a la Intimidad y la Informática. Editorial Porrúa. Segunda Edición. México, 1996, pág. 130.

[46] www.vlex.com.mx, México: El Derecho a la Intimidad y el Derecho a la Información: ¿Garantías encontradas?, Fabio Rubén Troncozo Auld, Doctrina – Análisis y Artículos.

Algunos otros estudiosos del derecho consideran que detrás del delito informático no existe un bien jurídico específico, y que sólo se tratan de formas de ejecución de delitos que afectan bienes jurídicos de protección penal ampliamente reconocida; pero quienes sostienen esto confunden a los delitos informáticos con ilícitos convencionales que ya están regulados en el Código Penal, sin entender que los delitos informáticos son conductas nuevas que por su peculiar naturaleza no se subsumen en la típica descripción de los delitos convencionales, por lo que se debe de admitir la existencia de un bien jurídico propio para esta nueva modalidad de delitos.

Se considera apropiado el criterio seguido por los autores que afirman que el bien jurídico a protegerse dentro de un análisis de delitos informáticos es la "información", ya que si bien es cierto que hasta hace unos años el merecimiento de protección penal en el interés social aquí abordado hubiese resultado cuestionable; hoy en día, el fenómeno informático en el que se halla inmersa la sociedad ubica al bien jurídico de la "información" en una posición de absoluto y comprensible merecimiento de resguardo en sede penal.

3.2.6. Perfil criminológico del sujeto activo de los delitos informáticos.

Con la informatización de la sociedad, la proliferación de centrales de cómputo y el aumento en el número de usuarios de éstas; ha surgido un nuevo tipo de acto delincuencial, y con él, un nuevo tipo de delincuente que para cometerlo no usa las herramientas típicas; sino que en su lugar maneja y tergiversa la información contenida en las bases de datos de los sistemas informáticos.

Los sujetos que cometen los "delitos informáticos", o mejor conocidos como "delincuentes informáticos", son personas que poseen ciertas características que no presentan el común denominador de los delincuentes.

Por lo regular, estos sujetos activos son individuos que tienen habilidades para el manejo de los sistemas informáticos y que por su situación laboral se encuentran en lugares estratégicos donde se maneja cierto tipo de información de carácter sensible; aunque no se puede generalizar en este sentido, ya que a pesar de que las estadísticas más recientes muestran que "el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada"[47]; otro estudio realizado en América del Norte y Europa indicó que "el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% de la actividad delictiva era externa"[48].

Esto demuestra que en muchos de los casos no necesariamente se requiere que el sujeto activo desarrolle actividades laborales que faciliten la comisión de este tipo de delitos, sino que basta tan sólo con que dicho sujeto sea diestro en el manejo de los sistemas informatizados.

El nivel de aptitud de los delincuentes informáticos, ha sido tema de controversia para diversos autores; ya que mientras que unos sostienen que el nivel de aptitudes no es indicador de delincuencia informática, otros aducen que los posibles delincuentes informáticos son personas sumamente inteligentes, decididas, motivadas y ansiosas de aceptar un reto tecnológico; aunque se puede afirmar que en la mayoría de los casos son personas carentes de principios.

Al respecto, la Dra. Luz María del Pozo y Contreras manifiesta: "casi la totalidad de este tipo de delincuentes no ven a las computadoras ni a los sistemas informáticos como algo asociado con las personas, las consideran solamente en su aspecto material"[49].

---

[47] www.vlex.com , España: "Legislación al respecto sobre Delitos Informáticos", (Doctrina – Artículos y Análisis), Marcelo Manson, 07/06/2001.
[48] Página de internet citada.
[49] http://www.cndhcu.gob.mx/camdip/foro/ .

Asimismo, explica que por lo general, estas personas tienden a ser solitarias, ya que prefieren trabajar con cosas y no con la gente. Otro factor que influye en el aislamiento de estos individuos del resto de la sociedad, es que pasan largas horas frente a las computadoras en busca de su objetivo, ya que sin trabajo no hay resultados.

La tendencia educacional que presenta la sociedad actual basada en una "racionalización hueca", hace pensar a los jóvenes en el delito informático como algo atrayente, lleno de audacia; y el cometerlo les produce en la mayoría de los casos una satisfacción visceral, de ahí parte el material humano que comete este tipo de ilícitos.

Hay otra situación preocupante en cuanto a los delincuentes informáticos; ya que debido a la gran disponibilidad de los sistemas informáticos, los cuales se encuentran fácilmente al alcance de cualquier persona sea ésta adolescente o adulto, se ha detectado que la edad de los delincuentes de esta naturaleza está ya entre los 13 a 15 años en adelante, de ahí que en cuanto más avanza la edad y la experiencia de impunidad, se desarrollan mayores capacidades para delinquir.

Como se puede apreciar de acuerdo a lo anteriormente reseñado, el sujeto activo del delito es una persona de cierto status socioeconómico, puede ser menor o mayor de edad, la comisión de este tipo de delitos no puede explicarse por pobreza del delincuente, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Más bien se trata de personas carentes de principios, que consideran sus desviaciones morales y éticas como algo audaz, y no como un conflicto.

Tomando en consideración las características de los sujetos activos en los delitos informáticos, los estudiosos en la materia los han catalogado como

"delitos de cuello blanco"; sin embargo, esta caracterización obedece no al interés protegido como sucede en los delitos convencionales, sino tomando en cuenta al sujeto activo que los comete.

3.2.7. El sujeto pasivo en los delitos informáticos.

En primer término se debe distinguir que el sujeto pasivo o víctima del delito es "el titular del derecho violado y jurídicamente protegido por la norma"[50], o "el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo"[51]; por lo que en el caso de los delitos informáticos, las víctimas o sujetos pasivos pueden ser personas físicas o morales, instituciones crediticias, entes gubernamentales, etc, que usan sistemas automatizados de información, generalmente conectados a otros.

Pero para poder ser considerado sujeto pasivo en los delitos informáticos, requiere ser cumplida una condición específica, que es la de ser titular de la información de carácter confidencial y privada, almacenada en formato digital, es decir, en un sistema informático, la cual es vulnerada por el delincuente informático al llevar a cabo la conducta ilícita. De tal forma, que no puede ser sujeto pasivo de un delito informático, quien no posea una información digital que revista cierto valor que requiera su confidencialidad; o quien detente dicha información pero ésta no se encuentre en formato digital, o sea registrada en un medio informático.

El sujeto pasivo es sumamente importante en el estudio de los delitos informáticos, ya que es a través de él como se pueden conocer las diversas conductas delictivas en las que incurren los sujetos que cometen este tipo de ilícitos y de esta forma tener la posibilidad de actuar en prevención de las acciones antes mencionadas.

---

[50] Castellanos Tena , Fernando. Obra citada. Pág.151.

[51] http://www.monografias.com/trabajos6/delin/delin.shtm, Delitos Informáticos y Computacionales cuyos efectos se producen en el extranjero. (Bolivia).

Sin embargo, en México e incluso en muchos de los países desarrollados resulta prácticamente imposible conocer la verdadera magnitud de los delitos informáticos, ya que gran parte de éstos no son descubiertos o lo que es peor, no son denunciados ante las autoridades, aunándole a ello la inexistencia de leyes que protejan a las víctimas de este tipo de delitos y la falta de preparación por parte de las autoridades para comprender, investigar y aplicar un tratamiento jurídico adecuado a esta problemática.

En muchos de los casos esta situación es provocada debido al temor de las empresas víctimas de delitos informáticos, de denunciar este tipo de ilícitos, por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes repercusiones económicas que ello traería aparejado consigo.

Para poder tener una prevención efectiva de la criminalidad informática se requiere entre otras cosas, educar a las víctimas potenciales (sujetos pasivos) de los delitos informáticos sobre las técnicas de manipulación y de encubrimiento utilizadas por los delincuentes informáticos para cometer sus ilícitos; así como estimular en ellos la confianza pública de denunciar esta clase de delitos ante las autoridades encargadas de detectar, investigar y prevenir los delitos informáticos, otorgándoles de esta manera protección penal.

3.3. CONDUCTAS DELICTIVAS TÍPICAS EN LOS DELITOS INFORMATICOS.

3.3.1. Tipos de conductas y sus características.

En el marco de los delitos informáticos existen ciertas conductas ilícitas que por su relevancia han sido de especial análisis por el derecho internacional público y privado; y que ya son reconocidas en la mayoría de los estados que cuentan con una legislación penal especializada en delitos de esta índole.

Dentro de la clasificación de conductas ilegítimas que comúnmente se llegan a dar en los delitos informáticos se encuentran las siguientes: a)Hacking, b)Cracking, c)Phreaking, d)Virucker y e)Carding.

a) *Hacking*: La palabra *"hacking"* proviene del inglés *"hack"* que significa "hachar" y es el término que se usaba hacia los años cincuenta en los Estados Unidos para describir la manera en que los técnicos telefónicos reparaban las cajas descompuestas, ya que éstos utilizaban como herramienta principal de reparación un golpe seco al artefacto con fallas, es decir un *"hack"*; de ahí que a estos individuos se les diera el nombre de *"hackers"*.

En la terminología informática un *"hacker"* es aquél individuo que "intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas"[52].

La actividad de *"hackear"* puede tener diferentes finalidades y alcances. Así, en la mayoría de los casos, los *"hackers"* acceden sin autorización a los sistemas informáticos con el objeto de satisfacer su curiosidad al husmear el contenido de la información protegida en los archivos o programas, o bien, para superar los controles, probar la vulnerabilidad del sistema para mejorar su seguridad, sustraer, modificar, dañar o eliminar información; y éstas motivaciones pueden deberse también a diversos intereses: ya sea que lo hagan con ánimo de lucro, por posturas ideológicas anarquistas, avidez de conocimientos, orgullo, propaganda política, etc.

Para algunos autores, el término *"hacker"* no significa más que intrusismo

[52] Barrios Garrido, Gabriela; Muñoz de Alba M., Marcia; Pérez Bustillo, Camilo. Obra citada. Pág. 103.

informático ilegítimo. Sin embargo, si bien todo intrusismo informático no autorizado resulta ilegítimo, ya que supone el acto de violentar las barreras de seguridad predispuestas por su titular para proteger la información para acceder al sistema, o bien, porque el ingreso se realiza en contra de la presunta voluntad de aquél; no es posible identificar, de acuerdo a circunstancias especiales, como es el caso de aquellos informáticos que desarrollan seguridad de redes; que todas estas conductas, en forma indiscriminada, deben ser objeto de sanción penal.

En efecto, el intrusismo informático, es la penetración por la fuerza a un sistema informático, pero el denominado "hacker ético" es aquel que posee autorización o consentimiento expreso del titular del sistema para verificar su seguridad. En este caso, es lógico pensar que en determinados ambientes como los empresariales por ejemplo; bajo los más estrictos controles y reglas básicas, así como en base a los pertinentes acuerdos contractuales, el intrusismo informático constituye una actividad lícita, y obviamente debe ser exenta de sanción penal, ya que no concurre el presupuesto de la antijuridicidad.

El jurista chileno Claudio Manzur, expresa en su artículo "Chile: Los Delitos de Hacking en sus diversas manifestaciones" publicado en la Revista Electrónica de Derecho Informático; que el *hacking* puede dividirse en directo e indirecto.

Este autor expresa que el *hacking* propiamente dicho "es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos o tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor"[53].

[53] www.vlex.com.mx , Argentina: "Presupuestos para la incriminación del Hacking", Autor: Hugo Daniel Carrión. Buenos Aires, Argentina.

Para Claudio Manzur, en el *hacking* directo, el *hacker* solo busca la intromisión a los sistemas informáticos por diversión. Entre las características propias de esta clase de *hacking* están las siguientes: el *hacker* es una persona experta en materias informáticas y sus edades fluctuarán comúnmente entre los 15 y 25 años, y su motivación no es la de causar un daño, sino que se trata más bien de obtener cierta satisfacción u orgullo, basándose para ello en la burla de los sistemas de seguridad dispuestos. Esta clase de *hacking* según el autor citado, no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

Contrario a lo anterior, el mismo autor considera que el *hacking* indirecto "es el medio para la comisión de otros delitos como fraude informático, sabotaje informático, piratería y espionaje"[54].

La característica principal en el *hacking* indirecto según lo aseverado por este autor, es que el ánimo del delincuente está determinado por su intención de accesar indebidamente a un sistema informático con el fin de dañar, de defraudar, de espiar, etc. Sin embargo, en este sentido, es menester hacer una distinción entre la conducta que desarrolla un *hacker* y la que desarrolla un *cracker*, ya que suele haber confusión entre ambas.

b) Cracking: Se les llama así, a las entradas ilegales a los sistemas informáticos, que tienen por objeto la destrucción de dichos sistemas; y a los sujetos que las realizan se les denomina *"crackers"*.

"Cracking" es una expresión idiomática derivada del inglés cuya traducción al español se puede entender como "quebrar, vencer las barreras de seguridad y romper lo que hay detrás de ellas"[55]. Según algunos estudiosos de la materia,

[54] www.vlex.com.mx, Argentina.
[55] http://www.monografias.com/trabajos6/delin/delin.shtm

en el supuesto del *cracking*; la intencionalidad del agente es accesar ilícitamente a un sistema informático con el fin de obstaculizar, dejar inoperante o dañar el funcionamiento de dicho sistema.

A simple vista, los términos *hacker* y *cracker* pudieran significar lo mismo; sin embargo, la diferencia radica en el elemento subjetivo que delimita la frontera de cada comportamiento; mientras que en el *cracking* la intencionalidad del agente es obstaculizar, dejar inoperante o dañar el funcionamiento de un sistema informático; en el *hacking*, el sujeto busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, pero sí vulnerando la confidencialidad y exclusividad de la misma, y la intimidad de su titular.

Aún cuando de lo anterior se pudiera desprender que la conducta que llevan a cabo los *hackers* al introducirse ilícitamente a los sistemas informáticos no genera daños, su actuar se encuentra dentro del plano de la ilegalidad y ellos lo asumen, de ahí que adopten muchas precauciones para evitar ser descubiertos.

Además, debe destacarse que desde el punto de vista técnico, el ingreso ilegítimo implica la utilización de los recursos del sistema y un riesgo concreto de dañar accidentalmente la información contenida en dicho sistema con la simple intrusión con fines aventureros, por lo que debe descartarse la hipótesis de que el mero acceso sin fines específicos de causar un daño determinado, no genera ninguna consecuencia sobre el sistema informático.

Por tal motivo existe disconformidad con la idea del Dr. Manzur, quien afirma que dicha conducta no representa un importante nivel de riesgo, toda vez que como se puede apreciar, el simple acceso genera consecuencias sobre los

sistemas, al mismo tiempo que priva a su titular de la confidencialidad y exclusividad de la información y vulnera el ámbito de su intimidad.

Retornando a la explicación de la figura del cracking, Claudio Manzur expone que "si el acceso ilegítimo al sistema informático es el medio para alterar, modificar o suprimir la información, no habrá *hacking* sino *cracking* que supone una acción concreta de daño sobre la información y el elemento subjetivo en el autor –dolo- constitutivo del conocimiento y voluntad de provocarlo"[56].

Entonces, en estricto apego a lo anterior, se puede considerar que el *hacking* es el presupuesto necesario para que se dé el *cracking*, sin embargo al consumarse la conducta del *cracking* se sobreentiende que para su consecución tuvo que haber un *hacking* previo, por lo que ésta conducta queda subsumida en la otra.

Lo que es un hecho en definitiva, es que en ambos casos, tanto en el *hacking* como en el *cracking*, hay una afectación al bien jurídico tutelado en los delitos informáticos, es decir, a la información, de ahí la peligrosidad de este tipo de conductas que hacen inminente la comisión de los delitos informáticos.

c) Phreaking: La actividad del *phreaking*, es una de las conductas ilícitas más comunes en el medio de los delitos informáticos; y se define con este término, a la actividad de obtener ventajas de las líneas telefónicas para los efectos de no pagar los costos de comunicación. Es decir, básicamente se trata de encontrar el medio para evitar el pago por el uso de la red telefónica, ya sea ésta pública o privada, digital o inalámbrica.

El *phreaking*, es considerado como un delito informático por la mayoría de los autores en la rama; no obstante lo anterior, esta conducta es generalmente

[56] www.vlex.com.mx , Argentina.

extra PC, es decir, raramente se realiza a través de las computadoras; su gestión se efectúa básicamente vía telefónica y se lleva a cabo por medio de la ingeniería en electrónica y no como en los delitos informáticos, los cuales se realizan propiamente a través de ingeniería en sistemas computacionales.

d) Virucker: Esta conducta consiste "en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus informáticos" y destruir, alterar y/o inutilizar la información contenida"[57].

Los virus informáticos son programas secuenciales que tienen como objetivo bloquear los sistemas informáticos, destruir los datos contenidos en dichos sistemas o causar un daño en la memoria de éstos, y que tienen una gran capacidad de reproducción en el ordenador y de expansión y contagio a otros sistemas informáticos. Su incidencia es similar a la que ejercen los virus propiamente dichos en el organismo humano, de ahí su denominación. El origen de los virus informáticos es desconocido, pero se tiene conocimiento de que Bulgaria es el país productor de la mayoría de ellos, seguido de Rusia y Estados Unidos. Entre los virus informáticos más conocidos están: el Data Crime, Alabama, Disk Killer, I love you y Melissa.

De acuerdo a lo expuesto en líneas anteriores, la conducta *"virucker"* se puede llegar a encuadrar dentro de la que se denomina *"cracking"*, ya que como se vio con anterioridad, el *cracking* supone el acceso ilegítimo a un sistema informático con el fin de obstaculizar, dejar inoperante o dañar el funcionamiento de dicho sistema; y como se aprecia en la definición de la conducta *"virucker"*, ésta se lleva a cabo de igual manera, a través del ingreso ilícito y doloso a un sistema informático con el objeto de destruir, alterar y/o inutilizar la información contenida en éste, mediante la introducción de un virus informático.

---

[57] Barrios Garrido, Gabriela; Muñoz de Alba ., Marcia; Pérez Bustillo, Camilo. Obra citada. pág. 103.

e) Carding: Se le llama *carding* a la actividad de cometer un fraude o estafa a través del uso ilegal de tarjetas de crédito. Pero no todo fraude cometido con una tarjeta de crédito supone que se esté realizado *carding*, ya que si una tarjeta de crédito es robada o encontrada y se usa por otra persona que no es su titular, ello no constituirá carding, sino un fraude convencional.

El *carding* consiste propiamente en el uso de un número de tarjeta de crédito (ya sea real o creado a través de procedimientos digitales), con el fin de realizar compras a distancia por internet y efectuar pagos.

El nivel de seguridad en Internet para realizar transacciones económicas no es bueno. A menudo existen fugas de información; ya que muchos usuarios de la red ponen su número de tarjeta de crédito para hacer compras y estos números son captados por otras personas que los reutilizan para hacer más compras sin ser los titulares de la tarjeta.

En otras ocasiones, los delincuentes informáticos que llevan a cabo este tipo de conducta, generan números válidos de tarjetas de crédito a través de procedimientos digitales para usarlos posteriormente en compras a distancia.

Otro inconveniente con que cuentan las tarjetas de crédito, es que las empresas que otorgan tarjetas numeradas a sus usuarios lo hacen a través de un sistema automatizado de creación de números aleatorios; dicho sistema es muy susceptible de ser vulnerado ya que cualquier persona con conocimientos en la materia puede hacer un sistema de cálculo de números aleatorios y por tanto, puede crear números válidos para efectuar transacciones fraudulentas.

Con el análisis realizado a las conductas delictivas típicas en los delitos informáticos, se puede apreciar la relevancia jurídica que dichas conductas han adquirido en la actualidad en virtud de la gran cantidad de delitos informáticos

que diariamente se realizan a través de las mismas, lo que hace cada vez más importante su tipificación y sanción a través de la creación de sistemas jurídicos aplicables a los mismos.

CAPÍTULO 4
MARCO JURÍDICO APLICABLE A LOS DELITOS INFORMÁTICOS

4.1. REGULACIÓN JURÍDICA DE LOS DELITOS INFORMÁTICOS.

4.1.1. Análisis Logislativo en la Unión Europea.

Como ya se ha explicado con anterioridad, el nuevo fenómeno científico tecnológico que ha traído aparejado consigo la informatización de la sociedad, configura un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde el derecho se hace necesario para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

El gran auge que ha obtenido la tecnología informática, ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. El aumento de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una gran amenaza para la economía de un país y para la sociedad en general; ya que no sólo la cuantía de los perjuicios ocasionados de esta manera es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que estos ilícitos no se lleguen a descubrir. Por tal razón, se afirma que la informática reúne muchas características que la convierten en un medio idóneo para la comisión de nuevas modalidades delictivas, como lo son los delitos informáticos.

De ahí la necesidad que han tenido varios países en donde esta clase de delitos ya ha dejado sentir sus consecuencias, de implantar en sus cuerpos normativos, legislaciones sobre protección de los sistemas informáticos.

La protección de los sistemas informáticos se puede abordar tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Pero para que estas medidas de protección alcancen su objetivo primordial deben estar estrechamente vinculadas unas a otras.

"Dadas las características de esta problemática, solo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una eficacia en la defensa de los ataques a los sistemas informáticos"[58].

Para iniciar el análisis de las diversas legislaciones que se han dado en torno a los delitos informáticos a través del mundo, se debe definir en primer término lo que se entiende por legislación informática.

En palabras de Julio Téllez Valdés la legislación informática es el "conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática..."[59].

Para dicho autor, la reglamentación jurídica al respecto deberá contemplar las siguientes problemáticas: regulación de los bienes informacionales, protección de datos personales, flujo de datos transfronterizos, protección de los programas informáticos , contratos informáticos , ergonomía informática , valor probatorio de los soportes modernos de información y lo que en este trabajo de investigación se analiza, codificación de los delitos informáticos.

---

[58] www.vlex.com (España).
[59] Téllez Valdés, Julio. Obra citada. Pág.59.

Un análisis de las diversas legislaciones que se ha promulgado en varios países al respecto, arroja que las disposiciones jurídicas que se han puesto en vigor están dirigidas primordialmente a proteger la utilización abusiva de la información reunida y procesada mediante el uso de las computadoras, e incluso algunas de ellas han previsto la creación de órganos especializados encargados de proteger los derechos de los ciudadanos amenazados por los ordenadores.

Desde hace aproximadamente diez años, la mayoría de los países europeos han hecho todo lo posible por incluir dentro de sus leyes, la conducta punible penalmente, como el acceso ilegal a los sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos, entre otros.

De igual forma, en muchos de los países occidentales se han creado normas similares a las de los países europeos. Todos estos enfoques coinciden en la misma preocupación de contar con legislaciones vigentes que les permitan tener comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

A continuación se aborda en detalle la situación que guarda el marco legislativo y normativo de los delitos informáticos en los países de la Unión Europea:

- **Francia:**

Desde la década de los setenta, surgió en Francia la gran inquietud de que los sistemas informáticos podían llegar a ser instrumentos para vulnerar o para agredir los derechos fundamentales de los ciudadanos, entre ellos, el derecho a la información. Fue así como se creó en aquél país la Comisión Nacional de Informática y Libertades cuya función era evitar que el mal uso o aun la simple obsolescencia de los sistemas informáticos, vulneraran los

derechos de los ciudadanos. Esta comisión sigue constituyendo a la fecha, uno de los pilares en la defensa de las libertades individuales y sociales de los franceses.

Más recientemente, el 5 de enero de 1988; se agregó al código penal francés un capítulo sobre crímenes de cómputo, el cual penaliza entre otras cosas, el acceso fraudulento a los sistemas informáticos y el mantenimiento de dichos accesos fraudulentos a los sistemas (fraude informático), y estipula penas alternativas por tales delitos, previendo así una pena de dos meses a dos años de prisión y multa de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos de los sistemas informáticos.

Asimismo, esa ley tipifica aquéllas conductas que de forma intencional y a sabiendas de estar vulnerando los derechos de terceros hayan impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos, o aquélla que de igual manera, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos contenidos en éste o sus modos de procesamiento o de transmisión (introducción de virus informáticos).

También se prevé en la legislación francesa el delito de (sabotaje), cuando de manera dolosa se acceda a un sistema informático, agravando la penalidad de dicho ilícito en el caso de que del mero acceso resultare la supresión o modificación de datos contenidos en el sistema, o bien la alteración del funcionamiento del sistema.

A pesar de la regulación anterior, debe destacarse que la adición al código francés en 1988, no contempla todos los problemas, ni ciertas conductas delictivas; por lo que resulta incompleta.

- **Gran Bretaña:**

Los primeros indicios de legislación aplicable a los delitos informáticos se dieron en Inglaterra a partir de la creación de una Comisión Parlamentaria presidida por Sir Kenneth Younger, la cual, a pesar de que llegó a la conclusión de que la vida privada no se encontraba amenazada por las computadoras en aquél país, recomendó algunas reglas de seguridad entre las cuales se pueden citar, la obligación que tienen los bancos de solicitar autorización de sus clientes para suministrar información acerca de sus cuentas, así como el derecho de acceso de los ciudadanos a las agencias que manejan electrónicamente datos relativos a su persona.

Sin embargo, a raíz de un caso de hacking que se dio en este país en 1991, comenzó a regir en la legislación inglesa la Computer Misuse Act (Ley de Abusos Informáticos), la cual castiga el deliberado acceso sin autorización a un sistema de cómputo con una fianza y un periodo de encarcelamiento que puede llegar a ser hasta de cinco años, si el acceso se realiza con el fin de cometer delitos graves, como amenazas y chantaje.

Dicha ley cuenta con un apartado en el que se prevé la introducción de virus a un sistema de cómputo, así como cualquier acto deliberado que dé como resultado una modificación no autorizada de los datos contenidos en dicho sistema y lo castiga con fianza y un periodo de encarcelamiento de hasta cinco años, dependiendo del daño que cause el virus. La noción de modificación contempla toda alteración, adición o eliminación de datos y se considera ilegal, si la persona que comete el acto no estaba autorizada para efectuarlo o no tenía la aprobación de alguien que pudiera otorgarla.

De igual forma, la intercepción deliberada de comunicaciones telefónicas o de comunicaciones efectuadas por medio de un sistema de

telecomunicaciones público será sancionado con fianzas y un lapso de encarcelamiento de no más de dos años.

- **Holanda:**

El 1° de Marzo de 1993, entró en vigor en este país la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el phreacking, la ingeniería social (entendiendo por ésta el arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus a los sistemas informáticos.

La penalización de la distribución de virus a los sistemas informáticos, está en función de la forma en que se hizo la distribución, ya sea si se escaparon por error, caso en el cual existe una atenuante en la sanción, motivo por el cual la pena no excederá de un mes en prisión; o si fueron liberados deliberadamente para causar un daño, caso en que existe una agravante del delito, por lo que su penalización podrá llegar hasta los cuatro años de prisión.

- **Alemania:**

Se tiene nociones de que en este país se creó la Ley contra la Criminalidad Económica en 1986, ordenamiento jurídico que contempla los siguientes delitos informáticos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

- **Austria:**

En Austria, la Ley de reforma del Código Penal, promulgada el 22 de diciembre de 1987, sanciona en su artículo 148, a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una

elaboración de datos automática a través de la confección de un programa; por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

Asimismo, dicha Ley contempla sanciones para quienes cometen este hecho haciendo uso de su profesión de especialistas en sistemas, situación donde existe agravante del delito.

- **España:**

Sin duda alguna, la ley más importante en torno a la materia en este país, es la Ley Orgánica 10/1995, del Código Penal, promulgada el 23 de noviembre del mismo año. En efecto, el Código Penal Español de 1995 alude en varios de sus artículos a los delitos informáticos y a sus penas, en concreto los Arts. 197 y subsecuentes, 270 y subsecuentes, y Art.400 y subsecuentes del Código Penal.

En el artículo 197 del Código Penal Español y subsecuentes, se habla en torno al descubrimiento y revelación de secretos; en tales circunstancias dicho numeral penaliza la interceptación de correo electrónico ajeno o cualquier documento de carácter personal imponiendo una sanción que va de uno a cuatro años de prisión y multa de doce a veinticuatro meses.

La misma pena será atribuida al que utilice, se apodere o modifique datos de carácter personal registrados en soportes informáticos o ficheros automatizados.

Esta Ley impondrá también una pena de hasta cinco años, al que difúnda, revele o ceda a terceros los datos o hechos descubiertos o imágenes captadas en la forma anteriormente mencionada.

El artículo 263 del Código Penal y sus subsecuentes, trata el delito de daños provocados mediante hacking o por introducción de virus; y en este sentido estipula que el que causare daños en la propiedad ajena destruyendo, inutilizando o por cualquier otro medio provocando daños en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, será sancionado con una pena de prisión de uno a tres años y multa de veinticuatro meses.

En el artículo 270 del Código Penal Español, se prevén los delitos contra la propiedad intelectual e industrial o también llamados (werez), y los sanciona con una pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses. Esta sanción será aplicada, para aquellos que con ánimo de lucro y en perjuicio de un tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La exposición de motivos del Código Penal Español de 1995, considera como uno de sus principales logros innovadores " el haber afrontado la antinomia existente entre el principio de intervención mínima y las crecientes necesidades tutela en una sociedad cada vez más compleja, dando prudente acogida a nuevas formas de delincuencia, pero eliminando, a la vez, figuras delictivas que ha perdido su razón de ser"[60].

4.1.2. Análisis Legislativo en Latinoamérica.

En algunos de los países latinoamericanos, la tipificación de los delitos informáticos y su consecuente penalización ya es una realidad , tal y como

[60] http://www.jose_cuervo.lettera.net .

sucede en Argentina, Chile y Bolivia; a continuación se analizan las legislaciones existentes en torno a la materia en dichos países.

- **Argentina:**

En Buenos Aires, Argentina; los primeros indicios de legislación relativa a la Informática se produce con la adopción de la Declaración de Salamanca, en la cual se reconoce la importancia de la ciencia y de la tecnología como instrumentos fundamentales para garantizar el desarrollo de los pueblos y de sus sistemas democráticos.

Este país, reforzó la Declaración de Salamanca y estipuló que el tránsito entre el subdesarrollo y el desarrollo de los países, entre la injusticia y la justicia social, entre la absurda distribución de la riqueza que priva en América Latina y una distribución justa, depende en gran medida del uso adecuado que se le dé a los instrumentos científicos y tecnológicos y principalmente a la informática.

Sin embargo, en cuanto a la materia que atañe en el presente capítulo, en Argentina aún no existe legislación específica sobre los llamados delitos informáticos. Solo existe la Ley 11.723 de Propiedad Intelectual promulgada en virtud del Decreto N°165/94 del 8 de febrero de 1994, en la cual se protegen las obras de bases de datos y de software.

En este Decreto se define lo que son las obras de software para efectos de su protección, y se contempla dentro de éstas los diseños, tanto generales como detallados del flujo lógico de datos en un sistema de computación; los programas de computadoras y la documentación técnica para el desarrollo, uso o mantenimiento del software.

Asimismo y para los mismos efectos se registra lo que son las obras de bases de datos, en las que incluye las obras literarias.

Sin embargo, esta Ley 11.723 resulta insuficiente a efectos de proteger los programas de computación, los sistemas o la información en ellos contenidos, de ciertas conductas delictivas tales como el ingreso no autorizado, la violación de secretos, el espionaje, el uso indebido, el sabotaje, entre otros; ya que no existen disposiciones específicas para los casos concretos.

No obstante, existen en el Congreso Nacional de este país diversos proyectos de ley que contemplan la temática de los delitos informáticos, aunque sólo dos de ellos cuentan en la actualidad con estado parlamentario. Estos proyectos son los presentados por los Senadores Nacionales Eduardo Bauza y Antonio Berhongaray.

- **Proyecto de Ley Penal y de Protección de la Informática presentado por el Senador Eduardo Bauza.**

El Proyecto de "Ley Penal y de Protección de la Informática" presentado por el Senador Eduardo Bauza, señala en su artículo 24 que la alteración, daño o destrucción de datos en una computadora, base de datos o sistema de redes, se realiza exclusivamente mediante el uso de virus informáticos y otros programas destinadas a tal modalidad delictiva.

Por lo que respecta al tipo penal de violación de secretos y divulgación indebida, se circunscribe al correo electrónico, dejando a un lado la figura de la información obtenida de cualquier computadora o sistema de redes. Asimismo, este autor incluye la apología del delito y agrava la conducta en caso de que el ilícito se cometa contra la seguridad de la nación.

El Proyecto del Senador Bauza, prevé en su artículo 20 el delito de acceso no autorizado, y estipula que para que se configure el tipo penal se requiere que la conducta vulnere la confianza depositada en él por un tercero (ingreso indebido), o que mediante maquinaciones maliciosas (dolo) ingresare a un

sistema informático o computadora utilizando un password ajeno. Este artículo prevé una agravante para el caso de que el ilícito sea cometido por profesionales de la informática.

En materia de uso indebido, este proyecto incluye este tipo penal en su artículo 21, sancionando a aquél que vulnerando la confianza depositada en él por un tercero (abuso de confianza), o bien por maquinaciones maliciosas (dolo), ingresare a un sistema o computadora, utilizando un password ajeno, con la finalidad de apoderarse, usar o conocer indebidamente la información contenida en sistema informático ajeno.

En tanto que el artículo 38 pena la manipulación de datos realizada por cualquier persona física o jurídica, de carácter privado, que manipule datos de un tercero con el fin de obtener información personal acerca de esa persona, vulnerando de esta manera el honor y la intimidad personal o familiar del mismo.

Este Proyecto también prevé lo relativo al sabotaje informático y daños; y sanciona con prisión de uno a tres años a aquél que en forma maliciosa, destruya o inutilice una computadora o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Contempla una agravante en caso de afectarse datos contenidos e la computadora o en el sistema de redes. Para que se configure este tipo penal se requiere actuar con malicia (dolo).

Para el tipo penal de interceptación ilegal (apoderamiento), este proyecto aplica penas de prisión.

En materia de violación de secretos (Espionaje o Divulgación), se contempla gradualismo en la aplicación de la pena, agravamiento por cargo e inhabilitación para funcionarios públicos. Además impone como sanción multas en el caso del delito de divulgación.

Por lo que se refiere a la Estafa y Defraudación se impone pena de prisión al responsable de una estafa cometida mediante el uso de un sistema informático.

- **Proyecto de Ley Régimen Penal del Uso Indebido de la Computación presentado por el Senador Antonio Berhongaray.**

En este proyecto de ley se abarcan diversas modalidades delictivas , agravando las penas especialmente en los casos de que la destrucción datos fuera cometida en contra de datos pertenecientes a organismos de la defensa nacional, seguridad interior o inteligencia, contemplando especificamente el delito de Espionaje.

En lo que se refiere a los delitos de Espionaje y Divulgación (Violación de Secretos), este proyecto penaliza la s violaciones a la defensa nacional, seguridad interior y a la inteligencia extranjera, y agrava la penalidad en caso de que ocurriera un conflicto internacional y para el caso de espionaje.

De igual manera, el Proyecto Berhongaray sanciona la imprudencia, negligencia, impericia o inobservancia de los reglamentos en la comisión de delitos por parte de terceros.

Dicho proyecto también contempla los delitos de Sabotaje y Daños e introduce agravamiento en la pena cuando se afecte organismos de la defensa nacional, seguridad interior e inteligencia. Estos delitos se sancionan con pena de prisión.

En su artículo 5° este proyecto pena a quien a través del acceso no autorizado o de cualquier otro modo, voluntariamente o por cualquier otro medio, destruyere, alterare en cualquier forma, hiciere inutilizables o inaccesibles o produjera o diera lugar a la pérdida de datos informáticos.

Igualmente, en su artículo 6°, pena la destrucción o inutilización intencional de los equipos de computación donde se encontraban los datos afectados. Agravando la sanción, cuando la destrucción, alteración o pérdida de datos trajera aparejadas pérdidas económicas, o cuando fuera cometida contra datos pertenecientes a organismos de la defensa nacional, seguridad interior o intelígencia.

En su artículo 11, propone como tipo legal el acceso no autorizado y el uso indebido, incorporando un móvil que es la ventaja económica.

- **Chile:**

Chile fue el primer país latinoamericano en contemplar una Ley contra los Delitos Informáticos, la cual fue promulgada el 28 de mayo de 1993 y entró en vigor el 7 de junio del mismo año. Se trata de una ley muy concisa, pues solo consta de 4 artículos.

Esta Ley relativa a Delitos Informáticos, o mejor conocida en Chile bajo el rubro "Ley 19.223", prevé en su artículo 1° como delitos informáticos el daño de los soportes físicos, de los fierros o hardware, de las partes o componentes del sistema, lo cual en ningún otro país donde existe legislación al respecto ha sido contemplado como delito informático, ya que se trata simplemente de un delito convencional de daños.

De acuerdo a lo estipulado por esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es sancionada con penas que van desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones contempla la introducción de virus a los sistemas informáticos.

Por su parte, el artículo 3°, tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

- **Bolivia:**

En Bolivia, la introducción de los delitos informáticos se hizo posible con la modificación del Código Penal Boliviano a través de la Ley 1766, y su tipificación quedó contemplada dentro del título referido a los Delitos contra la Propiedad en el Capítulo XI cuyo epígrafe es "Delitos Informáticos" (artículos 363 bis y 363 ter).

Únicamente se trata de dos delitos; el primer delito informático reconocido por esta legislación es el denominado "manipulación informática" el cual estipula que el que con la intención de obtener una beneficio indebido para sí o un tercero , manipulara un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Otro de los delitos informáticos contemplado por esta ley es el acceso y uso indebido de datos informáticos, previsto en el artículo 363 ter del Código Penal Boliviano, el cual a la letra dice "el que sin estar autorizado se apoderare, acceda, utilice, modifique, suprima o inutilice datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días".

Se considera que la inclusión de los delitos informáticos dentro del título relativo a los Delitos contra la Propiedad en la presente ley es incorrecta, toda vez que los delitos informáticos son pluriofensivos, es decir afectan la intimidad, la propiedad intelectual, el patrimonio, la seguridad, etc., y no solo la propiedad como lo ha previsto dicha legislación.

A pesar de que la inclusión de estos delitos en la ley en cuestión encuadra perfectamente dentro de la clasificación realizada por las Naciones Unidas sobre los delitos cometidos a través de las computadoras, algunos autores consideran que dicha inserción es limitada ya que no se contemplan delitos tan relevantes jurídicamente como es el caso del carding y el phreaking.

4.1.3. Análisis Legislativo en Estados Unidos y Canadá.

En Estados Unidos, la preocupación por proteger la vida privada de las personas ante los grandes avances de las tecnologías informáticas no es algo nuevo.

En 1974, el Congreso de Estados Unidos de América aprobó una Ley Federal de Privacidad en cuya exposición de motivos señalaba que el uso creciente de las computadoras y tecnologías de información sofisticada en ese país, a pesar de ser esencial para la eficiente operación del gobierno, había magnificado la posibilidad de causar daños a la privacidad individual mediante la recolección, mantenimiento, uso o diseminación de información personal.

Asimismo, externaba que el mal uso que se le daba a ciertos sistemas de información, ponía cada vez más en peligro las oportunidades de los individuos a conseguir un empleo, seguros y créditos, así como su derecho a un juicio justo y otras protecciones legales. De ahí que dicha ley creó obligaciones para el Estado norteamericano con respecto a la protección de la vida privada de sus ciudadanos; pero como esta ley no era vinculante para particulares, dejaba a las empresas y demás entes privados en libertad de acceder y utilizar la información confidencial de los particulares.

En 1986, se aprueba el Acta de Fraude y Abuso Computacional (Computer Fraud and Abuse Act), la cual contemplaba a nivel federal aquellos delitos destinados a afectar los sistemas de cómputo del gobierno federal y los que

necesitaban usar computadoras localizadas en más de un estado de los Estados Unidos.

De igual manera, el acceso no autorizado a un sistema de cómputo fue uno de los asuntos principales que fueron considerados en la citada acta, lo mismo que el acceso que excedía de la autorización limitada. En estos casos, era necesario probar que el intruso tenía la intención de transgredir las barreras del sistema.

Dicha acta también consideraba otros dos delitos con el fin de restringir la propagación de virus y otros programas dañinos, lo mismo que el sabotaje. Al respecto, un estudiante universitario que hizo circular un gusano en internet fue sentenciado bajo los efectos de esta ley.

Pero ante la latente desprotección de los usuarios frente a las empresas y demás entes privados; se aprueba más tarde el Acta de Comunicaciones Electrónicas Privadas o Ley de Privacidad de las Comunicaciones Electrónicas (Electric Communications Privacy Act) , la cual como su nombre lo indica, sanciona el acceso a las comunicaciones electrónicas privadas o la intercepción no autorizada a las mismas. Esta Ley si creaba obligaciones para particulares y regulaba todo tipo de comunicación electrónica, incluyendo la transmisión de datos e imágenes. Entre las disposiciones más relevantes de la misma se encuentran, la prohibición de la intervención no autorizada a toda persona o empresa, la prohibición de acceso no autorizado a mensajes almacenados en sistemas computarizados, y la prohibición de interceptar mensajes durante su transmisión sin la debida autorización.

En 1994, este país adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030), la cual modificó el Acta de Fraude y Abuso Computacional de 1986.

Esta nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas; ello con el fin de eliminar argumentos muy técnicos acerca de lo que es un virus, un gusano, un caballo de Troya y en qué difieren los tipos de virus existentes. Esta Ley está directamente en contra de los actos de transmisión de virus informáticos.

Igualmente, la citada ley diferencia el tratamiento de aquellos que de manera temeraria lanzan ataques de virus y de aquellos que lo realizan con la intención de causar estragos en el sistema informático. De esta manera, define dos niveles para el tratamiento de quienes crean virus y los sanciona con distinta penalidad:

a) Para los que intencionalmente causan un daño por la transmisión de un virus, los sanciona con una pena de hasta 10 años en prisión federal más una multa.
b) Para los que lo transmiten solo de manera imprudencial, la sanción fluctúa entre una multa y un año de prisión federal.

Esta ley anticipa los distintos niveles de delitos en materia informática y contempla qué se debe entender por acto delictivo en términos de delitos informáticos.

Asimismo, prevé penas de prisión federal y multa para delitos relacionados con estafas electrónicas, defraudaciones y otros actos dolosos relacionados con dispositivos de acceso a sistemas informáticos.

En 1995, se adoptan los "Computer Crime Statutes" (Estatutos para los delitos computacionales), que contemplan delitos contra equipo y suplementos de las computadoras; delitos contra la propiedad intelectual; uso criminal de la

computadora, crimen organizado y fraude; intrusión computacional; fraude computacional, etc.

En el año 2000, a través de la "Computer Security Enhancement Act", se incita a las compañías privadas a colaborar con el Gobierno, entregándole a éste información delicada que aquéllas tuvieran acerca de posibles incumplimientos en materia de ciber-seguridad, para investigar ciber-crímenes.

En ese mismo año, se publica la "Computer Crime Enforcement Act", cuya finalidad fue simplemente la de expandir la lista de delitos computacionales, contemplándose a partir de ese momento como tales: el *hacking* (acceso no autorizado a un sistema computacional con la intención de causar un daño); el *spam* (correo electrónico no solicitado), *cybersmearing* (calumnias por internet), *telecommunications fraud* (fraude telecomunicacional), *illegal breaking to computers* (daños ilegales a sistemas computacionales), *trade secrets stealling* (robo de secretos de estado), *piracy* (piratería), *trademark infringement* (copia o robo de una marca registrada), *patent infringement* (copia o robo de una patente), *copyright infringement* (reproducción del original).

Gracias a la existencia de estos ordenamientos ha sido posible que en este país, la comisión de los delitos informáticos no quede impune.

De acuerdo a un boletín publicado por la Revista Electrónica de Derecho Informático el 7 de mayo del 2001; dos jóvenes adolescentes de Estados Unidos fueron condenados por la comisión de sendos delitos informáticos.

En el primer caso, un joven de 16 años fue condenado a seis meses de prisión por un Tribunal de Miami por haber penetrado en las redes informáticas del Departamento de Defensa del país, en la NASA y en un servidor privado. Esta situación ocurrió en el mes de junio de 1999, fecha en la que el menor lanzó

un ataque contra trece ordenadores del Centro de Vuelo Espacial Marshall de la NASA en Hunstville, Alabama. A consecuencia de esta acción, dichos sistemas informáticos quedaron fuera de servicio durante 21 días, produciendo enormes pérdidas. Sin embargo, en agosto del mismo año, el mismo adolescente consiguió penetrar en la Red de Agencia de Reducción de Amenazas Militares y descifrar algunos códigos, así como también logró penetrar en un servidor situado en Virginia, en donde interceptó miles de correos electrónicos.

Por otro lado, un adolescente de 15 años, fue acusado por las autoridades reguladoras del Mercado de Valores Estadounidense de estafa bursátil por internet. El joven mediante el internet compraba acciones de compañías a precio muy bajo para más tarde inflar su valor con informes y noticias falsas, introduciéndolas en foros financieros on-line. Dicho individuo fue obligado por las autoridades a devolver las ganancias obtenidas a través de la realización de dicho acto ilícito.

Por lo que respecta a Canadá, el uso no autorizado (o abuso) de una computadora encabeza la lista de comportamientos penados por el derecho canadiense. Este delito se comete cuando un usuario obtiene en forma ilegal servicios o funciones desde una computadora, o la utiliza para cometer un delito informático. Tales actos deben cometerse sin ninguna leve sospecha de que el usuario es cómplice.

Esta situación demuestra el gran interés que tienen los operadores de los sistemas informáticos, en adoptar medidas de seguridad destinadas a proteger a los sectores privados de un sitio y limitar su acceso a los usuarios.

En virtud de que este delito implica el uso no autorizado de un sistema informático, en lugar del acceso no autorizado al mismo; es posible reprimir a un usuario que sobrepase los límites establecidos por un servicio. Asimismo, como

el delito abarca el uso de funciones, también permite indirectamente la supresión de datos apropiados ilegalmente a través de internet. En este sentido, se entiende que los intrusos que intenten apropiarse en forma ilegal de datos tendrán, necesariamente, que allegarse de ellos primero a través de un sistema de cómputo, de ahí que al hacerlo, utilizarán servicios informáticos no autorizados.

De igual forma, el uso mal intencionado de computadoras no solo abarca la destrucción o modificación de datos sino también, todos aquellos actos que reduzcan el rendimiento de esos datos o que interrumpan en forma temporal o permanente el acceso a ellos. Este delito permite castigar tanto a los autores directos de ataques dañinos en internet, como a los autores de virus informáticos y gusanos.

Como se ha podido apreciar, las leyes estadounidenses y canadienses, lo mismo que los sistemas legales de la mayoría de los países europeos y algunos de Sudamérica, han tipificado y penalizado dentro de sus textos legales los principales tipos de comportamiento ilícito cometidos a través de los sistemas informáticos, entre los que se pueden destacar: el acceso no autorizado, actos dañinos o circulación de material dañino e interceptación no autorizada.

Esto advierte, tal y como lo señala Pérez- Luño que " En una sociedad como la que nos toca vivir en que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario"[61].

[61] Pérez-Luño, Antonio Enrique. Las Generaciones de los Derechos Humanos, en: Dialogo con la Jurisprudencia. N° 1, Gaceta Jurídica Editores. Lima, Perú. 1995.

4.1.4. Problemas que rodean a la cooperación internacional en el área de los delitos informáticos.

En cuestiones de jurisdicción y competencia, por lo que a delitos informáticos se refiere; surgen varias interrogantes para el Derecho Penal Internacional, sobre quién deberá resolver las complejas situaciones que se generan a partir de la comisión de dichos ilícitos, teniendo en cuenta, que en la mayoría de los casos son delitos que se generan a distancia.

Un ejemplo podría ser el caso de que un país contemple dentro de su legislación penal como delito, el acceso no autorizado a los sistemas informáticos. Luego, un Banco de ese país sufre un acceso no autorizado a su sistema tendiente a obtener una transferencia indebida; pero al investigar, se descubre que el violador del sistema es un alemán que vive en Nueva Zelanda y que penetró en el sistema a través de un servidor que se encuentra en los Estados Unidos. Surge la pregunta inevitable de si pudiese el país en cuestión apropiarse la potestad de persecución del delito.

En respuesta a dicha interrogante, hay autores que consideran que el Juez penal de ese país puede intervenir por la sola circunstancia de que la infracción fue cometida en el territorio de su país, por lo que de acuerdo a ello, se aplicaría la ley del domicilio.

Como ya se ha reseñado con anterioridad dentro del cuerpo del presente trabajo de investigación , los delitos informáticos por sus características , son delitos que en su mayoría carecen de un espacio físico, y por tanto, de nacionalidad. Es decir, pueden ser cometidos por nacionales o extranjeros y sus efectos pueden o no darse dentro del Estado en donde fueron cometidos; de ahí la importancia de determinar qué jurisdicción tendría competencia para juzgarlos.

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

En un claro esfuerzo por lograr una homologación internacional en materia de delitos informáticos, en la celebración de la "Draft International Cybercrime Convention", se propuso la creación de una legislación internacional uniforme para prevenir y combatir los delitos informáticos a nivel internacional; y en la misma se acordó otorgarle amplios poderes a Estados Unidos y la Unión Europea para la consecución de dichos objetivos.

Sin embargo, la cooperación internacional en el área de los delitos informáticos, está rodeada de ciertos problemas que a continuación se mencionan:

a. Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
b. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e. Carácter transnacional de muchos delitos cometidos mediante el uso de las computadoras.
f. Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados, que permitan la puesta en vigor de la cooperación internacional.

De acuerdo a informes brindados por la ONU, estos son los mayores problemas que afectan la cooperación internacional, para lograr una adecuada investigación y sanción de los delitos informáticos. De ahí que exista una gran impunidad en cuanto a delitos informáticos con efectos transfronterizos se refiere.

4.1.5. Perspectiva global del Derecho Mexicano ante el fenómeno informático.

En esta nueva era en la vida del hombre en la que las tecnologías de la información han adquirido un carácter estratégico es necesario analizar, reflexionar, profundizar y proponer los tiempos y formas que deben dar cuerpo a la singular relación del derecho y la informática, con la finalidad de contar con un adecuado marco jurídico relativo al uso y desarrollo de esta tecnología, que permita la aplicación de disposiciones jurídicas que aseguren las condiciones requeridas para su mejor aprovechamiento.

En México, la realidad que propone el movimiento globalizador que se ha acelerado a partir de las tecnologías de la información, plantea, al igual que en los demás países, nuevas formas de organización en los negocios, en el mundo de la academia, en los gobiernos, en las actividades habituales y en general, nuevos problemas jurídicos que requieren una solución práctica y eficiente lo antes posible.

Si bien es cierto el nivel de informatización nacional no es tan pronunciado como en otros países (estadísticas muestran que el nivel de informatización en México es de un 5% a comparación de Canadá y Estados Unidos que muestran niveles superiores a un 70%), al menos es suficiente para la realización de un adecuado análisis y tratamiento por la vía del Derecho, ya que los hechos demuestran que tanto el uso de las computadoras como la evolución de la cultura informática, son dos fenómenos crecientes e irreversibles en el país.

En México, la historia de la normativa en torno al fenómeno informático se inicia en 1984. En septiembre de este año, la Gran Comisión del Senado de la República encomendó a su Comisión Especial de Informática, identificar las necesidades de legislación en esa materia, y en su caso, proponer los criterios y bases generales para establecer un adecuado marco normativo. Entre otros asuntos, la Comisión debía formular los proyectos de iniciativa correspondientes y estudiar la conveniencia de establecer un Centro de Informática Legislativa, como órgano dependiente del Senado de la República.

En 1985, el Senador José Antonio Padilla Segura, en su calidad de Presidente de la Comisión Especial de Informática, rindió ante el Pleno del Senado un informe en virtud del cual se originó el acuerdo de creación del Centro de Informática Legislativa del Senado (CILSEN), organismo que entró en vigor a partir del 7 de octubre de 1986.

Una vez instaurado dicho órgano, la Comisión encomendó al CILSEN profundizar en torno a los estudios relativos al establecimiento de un marco normativo aplicable a la informática acorde a las necesidades del país. Esto trajo como consecuencia el documento titulado "Marco Normativo de la Informática en México", cuyo contenido se encuentra configurado de la siguiente manera:

1. Estado actual de la normatividad sobre informática en México.
2. Proyecto de exposición de motivos sobre la necesidad de establecer un marco normativo en materia de informática, y
3. Proyecto por el que se adiciona la palabra "informática" a la fracción X del Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

El primer punto se encuentra dividido en dos áreas de estudio: la primera aborda la problemática relativa a la "Legislación relacionada con la informática" en la cual se estudian aquellas normas (leyes, reglamentos, acuerdos y tratados

internacionales) que no obstante no mencionar expresamente el término informática, son aplicables en las múltiples circunstancias en que esta tecnología está presente; y la segunda, la concerniente a la "Legislación específica sobre informática", que está integrada por aquéllas normas que de manera expresa mencionan dicho término.

El análisis partió del documento base del sistema jurídico mexicano, la Constitución; y siguiendo en orden jerárquico continuó con las leyes reglamentarias, las ordinarias, los reglamentos del Ejecutivo y los Convenios Internacionales.

De este estudio, se desprendió una conclusión sustancial al referir la imperiosa necesidad de legislar en torno a esta materia a nivel constitucional, toda vez que no existe disposición especifica sobre informática en la Constitución Política del país. De manera indirecta, solo hay algunas disposiciones constitucionales aplicables a ciertas situaciones derivadas del uso de las tecnologías informáticas; tal es el caso de los Artículos 28 y 134 Constitucionales, preceptos relacionados con la tecnología en cuestión, en cuanto a que en éstos se considera como actividad estratégica la comunicación vía satélite (dentro de la cual se puede considerar encuadra la comunicación vía internet) y se establecen también ciertos principios generales para la administración de recursos económicos del Estado, dentro de los que pueden incluirse los informáticos.

Por otro lado, la Constitución no otorga facultad expresa al Congreso de la Unión para legislar en materia informática, de tal forma que en atención al régimen de competencias instaurado por el Artículo 124 de la Constitución General de la República, la facultad para legislar en torno a esta materia debería entenderse reservada a los Estados; sin embargo, ante la magnitud que plantea la problemática derivada del uso de las tecnologías de la información,

se considera que dicho aspecto debe ser tratado y legislado a nivel federal por la importancia que su aplicación reviste y por ser una materia de observancia especial.

En el marco de la legislación ordinaria, se analizaron aquellas leyes que influyen en áreas que regulan aspectos de la informática relacionados con las telecomunicaciones o respecto de su propio desarrollo como tecnología, ya sea que se trate a la informática como instrumento, como medio de producción de bienes y servicios o bien como producto tecnológico, o que regulen la propiedad industrial del soporte lógico. De ahí que entre las legislaciones estudiadas en este rubro se encuentren: la Ley de Vías Generales de Comunicación, Ley para Coordinar y Promover el Desarrollo Científico y Tecnológico, Ley Orgánica para la Administración Pública Federal, Ley para promover la Inversión Mexicana y regular la Inversión Extranjera, entre otras.

En cuanto a los Convenios Internacionales, se incluyeron sólo aquellos que vinculan a la informática con las telecomunicaciones.

Ante la carencia de un marco jurídico suficiente, el Ejecutivo ha tenido que recurrir a la facultad reglamentaria a fin de regular y resolver una serie de situaciones concretas que se han creado a partir del uso y aplicación de las tecnologías de la información.

Existen también ciertos ordenamientos jurídico-administrativos que de alguna manera vienen a cubrir las lagunas jurídicas existentes en nuestro sistema jurídico en torno a la materia en cuestión, y que permiten que por lo pronto, se desarrollen planes, proyectos y programas que puedan ser empleados en la acertada regulación de los sistemas informáticos.

De igual manera, y tal como se explicó con anterioridad, en atención al régimen de distribución de competencias establecido en la Constitución en su Artículo 124; hay entidades federativas que ya han expedido en algunos casos, normas reglamentarias con el fin de regular algunos aspectos de la aplicación de la informática y de esta forma dar solución a algunos problemas inmediatos que la implantación y uso de esta nueva tecnología ha originado.

De lo anteriormente expuesto se desprende que existe un gran vacío legislativo en el país en lo que a regulación de la materia informática concierne, y aún más, a nivel federal no se contempla disposición alguna respecto a este factor tan importante y que tantas consecuencias tanto positivas como negativas ha generado con su uso y aplicación.

Lo ideal sería tal y como lo sugieren algunos autores, adicionar a la fracción X del Artículo 73 Constitucional, la facultad al Congreso de la Unión para legislar en torno a la materia "informática", y una vez promulgada la adición que se indica; establecer en la Ley Reglamentaria a dicho precepto constitucional, las áreas específicas sobre las cuales el Congreso de la Unión habrá de legislar.

A propósito de lo anterior, el autor José Antonio Padilla Segura en su libro "Informática Jurídica", enumera las áreas en las que considera prioritario legislar al respecto:

- Garantías individuales, sociales y políticas.
- Seguridad nacional.
- Soberana nacional.
- Flujo de datos transfronterizos.
- Delitos Informáticos.
- Protección a la propiedad intelectual sobre programas de computadoras.
- Promoción del desarrollo científico.

- Promoción de la enseñanza de la informática en los niveles de educación básica y formación de profesionistas e investigadores.
- Defensa de los valores culturales.

Lo cierto es que es evidente que a pesar de los índices de crecimiento del uso de las computadoras y del internet, en México se vive un problema social al que algunos autores han denominado "analfabetismo informático", del cual el Poder Legislativo no está exento; prueba de ello es el retraso considerable que se advierte en las leyes del país en lo referente a las tecnologías de la información. La mayoría de las autoridades integrantes de los Poderes Ejecutivo, Legislativo y Judicial aún no entienden el concepto y estructura del fenómeno informático; por tal razón, en México se está ante un gran reto no sólo legislativo sino de carácter social, que permita el mejor aprovechamiento del empleo de las tecnologías de la información.

4.1.6. Situación actual de México ante la ausencia de Legislación en materia de Delitos Informáticos.

En la Legislación Penal de México, la tipificación de los delitos informáticos es casi inexistente. Un análisis documental legislativo demuestra que con excepción del Estado de Sinaloa, en México, ya sea a nivel federal o local, los delitos informáticos como tales, no existen, ya que dichas conductas no se encuentran contempladas en los textos jurídicos; por lo tanto, al no actualizarse los presupuestos básicos para la tipificación de un delito como tal, que son: " 1) que la conducta constitutiva del mismo esté tipificada por la ley; y 2) que medie una sentencia condenatoria en la cual èl juez penal haya declarado probada la existencia concreta de una conducta típica, antijuridica y culpable constitutiva de delito informático"[62], es posible afirmar que tales ilícitos dentro del contexto legal del país son inexistentes.

[62] www.vlex.com.mx , México.

Tal y como se enunció en líneas anteriores, en el caso de México, el tratamiento de los denominados delitos informáticos es muy precario. El único Código Penal que tipifica como "delito informático" una conducta ilicita derivada del uso de los sistemas informáticos, es el del Estado de Sinaloa (Octubre 1992), el cual en su artículo 217 establece que:

" 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, bienes o información; o

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

Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa."[63]

En palabras del autor Juan José Ríos Estavillo, este numeral representa una copia del Proyecto de Ley Informática del Ministerio de Justicia de Chile. Además, su inclusión dentro del Código Penal es limitada toda vez que se encuentra clasificado dentro del título correspondiente a los delitos patrimoniales, lo que advierte que en este caso únicamente se protege el patrimonio de las personas, cuando que en realidad la tipificación de este tipo de delitos protege no sólo el aspecto patrimonial, sino primordialmente el bien jurídico informacional y el derecho a la intimidad.

Además, en dicho ordenamiento punitivo se comete un error al contemplar que quien comete un delito informático siempre tendrá el propósito de obtener un lucro, lo cual resulta totalmente falso, ya que en muchas ocasiones tales

[63] Ríos Estavillo, Juan José. Obra citada. Pág. 126.

conductas se realizan por placer o como reto intelectual, cuestión que no es prevista por el numeral en cuestión.

Este precepto tampoco delimita contextualmente lo que implica el hecho de "diseñar, ejecutar o alterar esquemas", por lo que su apreciación resulta un tanto escueta.

Por tales razones, es conveniente resaltar que aún y cuando dicha conducta esté contemplada en el texto del Código Penal del Estado de Sinaloa bajo el rubro de "delito informático", no es en sí un delito informático, ya que si bien es cierto cumple con el requisito de tipicidad al haber encuadramiento de la conducta con la descripción hecha en la ley, también es cierto que no satisface el resto de los elementos formales y materiales que caracterizan a este tipo de ilícitos. Por lo tanto, se puede decir que desde el punto de vista técnico-penal sí representa un delito para el Estado de Sinaloa, pero desde la perspectiva técnica-informática no llega a satisfacer plenamente su descripción.

Cabe hacer mención que paralelamente a esta disposición jurídica cuya supuesta intención es la de prevenir y sancionar el manejo ilícito de los sistemas informáticos, existen en el país otros dos ordenamientos jurídicos que contemplan en forma superflua la protección de la información contenida en los sistemas de cómputo.

Se trata de los Códigos Penales de los Estados de Morelos y Tabasco, cuyos artículos 150 y 163 respectivamente, establecen que se sancionará a quien sin consentimiento de otro o sin autorización judicial y para conocer asuntos relacionados con la intimidad de una persona, entre otros supuestos, utilice medios técnicos para escuchar, observar, transmitir, grabar o reproducir la imagen o el sonido. El bien jurídicamente protegido en estos casos es la "privacidad" y la "propiedad" de la información contenida en los equipos o

sistemas de cómputo. Sin embargo, no se puede decir que en ambas legislaciones se prevea dicha conducta como si se tratare de un delito informático, puesto que no está contemplado como tal; además de que resulta erróneo aseverar que lo que se tutela en el supuesto del uso indebido de los sistemas informáticos sea la privacidad o la propiedad de la información contenida en los mismos, ya que como se reseñó con anterioridad, el bien jurídico tutelado en esta nueva modalidad de ilícitos derivados del uso ilegal de los sistemas informáticos es la "información" en su máxima expresión, y no solo la privacidad o la propiedad de la misma.

Como se puede inferir, el tratamiento que la legislación del país le ha otorgado a los ilícitos derivados del uso de las tecnologías de la información es casi arcaico. En el Código Penal Federal, con la reforma publicada en el Diario Oficial de la Federación el 17 de mayo de 1999; se adicionó dentro del Título Noveno, cuyo contenido trataba exclusivamente lo relativo al delito de "Revelación de secretos", el Capítulo II intitulado "Acceso ilícito a sistemas y equipos de informática", conformado por los artículos 211 bis 1, 211 bis 2, 211 bis 3,211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7, en cuyos textos se contempla en forma muy precaria, algunas acciones delictivas provocadas por el acceso no autorizado a los sistemas informáticos.

Así por ejemplo, el Artículo 211 bis 1, establece que se impondrán de seis meses a dos años de prisión, y de cien a trescientos días multa, al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad. Para el caso del que accese en la forma antes mencionada a algún sistema o equipo de informática, con la intención de conocer o copiar la información contenida en dichos sistemas, se le impondrá de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

El artículo 211 bis 2, se refiere a la misma situación que el artículo anterior, con la única variante de que el acceso ilícito se efectúe sobre sistemas o equipos de cómputo pertenecientes al Estado, en cuyo caso la multa se eleva de uno a cuatro años de prisión y de doscientos a seiscientos días multa; y si la intención es conocer o copiar la información contenida en dichos sistemas, la sanción que corresponderá será de seis meses a dos años de prisión y de cien a trescientos días multa.

Por su parte, el Artículo 211 bis 3, especifica la sanción para aquellos que estando autorizados para acceder a un sistema y equipo de informática perteneciente al Estado, indebidamente modifiquen, destruyan o provoquen pérdida de la información contenida en los mismos. En este caso la penalidad se agrava de dos a ocho años de prisión y de trescientos a novecientos días multa. Y si el caso es que el que está autorizado para accesar a dichos sistemas o equipos de informática del Estado, lo hace con la intención de copiar indebidamente la información que en ellos se contenga, la sanción será de uno a cuatro años de prisión y multa de ciento cincuenta a cuatrocientos cincuenta días.

El Artículo 211 bis 4, se refiere a la misma situación que el artículo anterior, pero para el caso de que el acceso ilícito se perpetre en los sistemas o equipos de informática de las instituciones que integran el sistema financiero, en cuyo caso se impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Y para el caso de que la intención sea conocer o copiar la información contenida en éstos, se impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

El Artículo 211 bis 5, contempla el caso de que el acceso ilícito a los sistemas o equipos de informática de las instituciones que integran el sistema financiero, lo haga alguien que esté autorizado para ello, pero con la intención de

modificar, destruir o provocar indebidamente, pérdida de la información que en dichos sistemas se contemple; para esta situación, la pena que se impondrá será de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Si la intención del que está autorizado para acceder a los sistemas o equipos de informática que se especificaron con anterioridad, es copiar indebidamente la información que éstos contienen, la sanción que se le impondrá será de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Este artículo contempla una agravante, en el caso de que las conductas que el mismo prevé, sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero; y para tal modalidad, las penas estipuladas en dicho artículo se incrementarán en una mitad.

Por lo que hace al Artículo 211 bis 6, estipula qué se entiende por instituciones que integran el sistema financiero, para los efectos de los artículos 211 bis 4 y 211 bis 5.

Y por último, el Artículo 211 bis 7, contempla otra agravante, para el caso de que la información obtenida a través del acceso ilícito o no autorizado a los sistemas informáticos sean públicos o privados, se utilice en provecho propio o ajeno, es decir con ánimo de lucro; por lo que en dicha situación, todas las penalidades contempladas en este capitulo se incrementarán hasta en una mitad, siempre y cuando se actualice la agravante que contempla este numeral.

Como se puede apreciar, la intención que tuvo el legislador con la reforma del 17 de mayo de 1999, al incluir dentro del contexto del Código Penal Federal, una cuestión que pudiera darle solución a la problemática derivada del inminente uso y aplicación de los sistemas informáticos en la sociedad, fue buena; sin

embargo, el problema se abordó desde una perspectiva errónea, ya que el considerar a este tipo de ilícitos como si se tratare de figuras típicas de carácter tradicional, puede provocar enormes errores de apreciación, y por ende, de punitividad, puesto que se corre el riesgo de alterar de manera flagrante el principio de legalidad de las penas.

Como se ha venido explicando a lo largo de la presente tesis; el empleo de las técnicas informáticas, ha creado nuevas modalidades de conductas ilícitas provocadas por el uso indebido de los sistemas informáticos, lo que ha propiciado a su vez la necesidad de regulación. Sin embargo, este nuevo tipo de delitos, denominados "delitos informáticos", merecen un tratamiento especial, con disposiciones jurídicas específicas en torno a la materia, que sean contempladas en los códigos penales sustantivos, para efectos de un adecuado control preventivo y correctivo de dichas conductas ilícitas, que tanto daño causan a los intereses individuales y sociales.

El Código Penal Federal, comete el error de otorgarle un tratamiento convencional a este tipo de ilícitos, al no considerarlos un nuevo tipo de modalidad delictiva; y por ende, al no ser contemplados como delitos informáticos dentro del texto de dicho ordenamiento penal, se debe considerar entonces que los delitos informáticos como tales, no existen dentro de la Ley Penal Federal del país. Además, el tema se aborda en forma escueta, lo que da lugar a que queden innumerables interrogantes en torno a situaciones susceptibles de ser sancionadas por el Derecho Penal, que no son previstas en el cuerpo de dicha codificación y que por tanto, han generado un ambiente de impunidad al respecto.

Con la intención de remediar la situación que se vive en México, ante la ausencia de legislación en materia de delitos informáticos; el 22 de marzo del 2000, se presentó ante el Honorable Congreso de la Unión del país, un

"Proyecto de Iniciativa de Ley que Reforma y Adiciona diversas disposiciones del Código Penal para el Distrito Federal en materia del Fuero Común y para toda la República en materia de Fuero Federal (ahora Código Penal Federal), con el objeto de penalizar lo referente a Delitos Informáticos".

Dicha iniciativa, fue sometida por los Diputados Federales, Francisco Suárez Tanori, Adalberto Balderrama Fernández y algunos otros diputados de varios grupos parlamentarios de la LVII Legislatura del Honorable Congreso de la Unión, lo anterior con fundamento en lo dispuesto por la fracción II del Artículo 71 de la Constitución Política de los Estados Unidos Mexicanos.

En su exposición de motivos, dicho proyecto reconoce el impacto que las telecomunicaciones han generado a nivel mundial. Incluso, no duda en afirmar que en México ya se está viviendo la "sociedad de la información", como muchos sociólogos han llegado a llamar a esta reciente etapa de la historia.

Asimismo, advierte que el Internet es en la actualidad el medio de comunicación con más fuerza y potencia, ya que permite la difusión de conocimientos a un precio muy bajo y a nivel mundial.

Pero en la misma forma en que destaca el sentido positivo de la expansión de la tecnología informática; también puntualiza que se debe de abordar otro tipo de situaciones que deben de regularse de manera necesaria en todo el mundo, toda vez que el mal empleo que se haga de dicha tecnología, puede llegar a convertirla en un medio idóneo para vulnerar los derechos de individualidad de las personas que accesan a estos sistemas.

En dicho proyecto también se menciona que los delitos que se cometen en materia informática, no pueden convertirse en México en sinónimo de impunidad, por lo que deben tomarse inmediatamente las medidas necesarias al respecto.

Para efectos de esta iniciativa de ley, por "delitos informáticos" deben entenderse, todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen referencia al uso indebido de cualquier medio informático.

Los Diputados Federales que elaboraron esta iniciativa, afirman que la lucha contra el delito informático es complicada, porque la legislación contra el delito en esta materia no avanza a la misma velocidad que la tecnología de la que se sirven los delincuentes informáticos, ya que al no existir una autoridad mundial que supervise la red se facilita la propagación de las conductas ilícitas. También sugieren, que independientemente de la penalización que se propone en materia de delitos informáticos en el país, resulta necesaria una cooperación internacional para la lucha contra los delitos en materia informática.

En dicha iniciativa de ley, se contemplan las siguientes reformas y adiciones al Código Penal para el Distrito Federal en materia del Fuero Común y para toda la República en materia del Fuero Federal:

Se propone reformar el Título Quinto, Capítulo I, Artículo 167 fracción VI, en el cual se prevé que se impondrá de uno a cinco años de prisión y multa de quinientos a cincuenta mil pesos, a aquél que interrumpiere la comunicación de una red pública de telecomunicaciones, de un espectro radioeléctrico, telegráfica o telefónica, alámbrica o inalámbrica, o el servicio de producción, transmisión de alumbrado, gas o energía eléctrica, destruyendo o deteriorando uno o más postes o aisladores, el alambre, un equipo de cómputo, una máquina o aparato de un telégrafo, de un teléfono, de una instalación de producción, o de una línea de transmisión de energía eléctrica.

Igualmente, se propone reformar el Capítulo II del mismo título relativo a la "violación de correspondencia", en específico los artículos 173 y174, en los

cuales se sanciona únicamente con pena de multa de tres a ciento ochenta jornadas de trabajo a favor de la comunidad, al que abra indebidamente una comunicación escrita, o la accese a través de medios electrónicos, electromagnéticos u ópticos, que no esté dirigida a él. Asimismo, estipula que para el caso de que quienes abran o intercepten las comunicaciones escritas, a través de medios manuales, electrónicos, electromagnéticos u ópticos, sean los padres respecto de las comunicaciones dirigidas a sus hijos menores de edad, o los tutores respecto de las personas que se hallen bajo su dependencia; no se considerará que obren delictuosamente. En este mismo sentido, se propone la adición del Art. 174 bis.

En esta iniciativa, se adiciona al Título Vigésimo segundo que contempla los "Delitos en contra de las personas en su patrimonio", el Capítulo Tercero, con el Artículo 389 ter; este artículo advierte una nueva modalidad de fraude derivada del uso ilícito a los sistemas informáticos; y así especifica que se sancionará con prisión de tres meses a doce años y multa de cincuenta a quinientos días, al que actuando en calidad de usuario, intermediario, empresa proveedora de información, banco, o cualquier empresa comercializadora, utilice el intercambio de datos para obtener con engaños ganancias indebidas, aprovechándose de su acceso a los sistemas de redes computacionales.

De igual forma, se propone adicionar dentro del mismo título, el Capítulo Séptimo referente a "Delitos Informáticos", con el Artículo 399 ter, párrafos I al VIII, en cuyo texto se estipulan sanciones para aquellos que sin estar autorizados, se apoderen, alteren, utilicen o modifiquen, en perjuicio de terceros, datos reservados de carácter personal, familiar o de negocios que se hallen registrados en ficheros, programas, códigos, soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de registro público o privado.

También sanciona al que difunda, revele o ceda a terceros los datos o hechos descubiertos en la forma anterior. En el mismo sentido, impone la misma penalidad para el que con conocimiento de su origen ilícito y sin haber tomado parte en el descubrimiento, realice la conducta estipulada en el párrafo anterior. Este precepto advierte penalidad agravada, para el caso de que quien cometa la conducta descrita con anterioridad, sean los encargados o responsables de los ficheros, programas, códigos, comandos o soportes informáticos, electrónicos o telemáticos.

De igual manera, hay agravante para el caso de que con la conducta descrita anteriormente, se afecten datos de carácter personal, que revelen la ideología, religión, creencias, salud, origen racial o vida sexual de las personas, o la víctima fuere un menor de edad o persona con discapacidad.

La fracción VII del precepto en cuestión, contempla otra agravante para el caso de que la realización de los hechos descritos en las fracciones I a la III de dicho artículo, se hagan con la intención de obtener un lucro de las mismas.

También se sanciona a los proveedores de acceso a internet, que proporcione servicios informativos que contengan material apto solo para mayores de edad, o que puedan afectar la integridad de la familia, o herir la sensibilidad de algún sector de la población, y que omita identificarse totalmente; o al que siendo proveedor de acceso a internet, solicite a los usuarios el derecho de uso de sus datos personales, con el fin de obtener un servicio, o comprar o vender un producto, o bien los utilice con diversos fines pero sin su autorización.

Y por último, esta iniciativa de ley, propone reformar el título Vigésimo Sexto, que contempla lo relativo a los "Delitos en materia de derechos de autor", en específico el Artículo 424, cuyo texto estipula que se impondrá una pena de seis meses a seis años de prisión y de

trescientos a quinientos días multa, a quien en forma dolosa, a escala comercial y sin autorización, produzca, reproduzca, importe, almacene, transporte, distribuya, ceda o arriende copias de obras, fonogramas, videogramas, programas computacionales, o libros protegidos por la Ley Federal de los Derechos de Autor.

Como se puede apreciar, del análisis realizado al Proyecto de Iniciativa de Ley que en Materia de Delitos Informáticos sometieron el 22 de marzo del 2000, los Diputados Federales mencionados con anterioridad; se desprende que a pesar de que dicha iniciativa aborda con más claridad y precisión la temática en torno a los delitos informáticos, adolece de la misma imperfección que muchas de las legislaciones existentes en torno a esta materia, ya que se continúa encuadrando y adaptando esta nueva modalidad de conductas ilícitas derivadas del uso indebido de los sistemas informáticos, dentro de los llamados delitos convencionales, lo cual como ya se ha venido recalcando en páginas anteriores, es anacrónico, toda vez, que los delitos informáticos son una nueva forma de delitos que merecen ser tratados como tales, y por ende, deben ser contemplados en un título específico, con penalidades adecuadas al daño económico y social, que éstos ocasionan.

México, tiene la ventaja de poder tomar como marco de referencia las experiencias que en el ámbito internacional se han dado en materia de delitos informáticos, así como de observar elementos valiosos que el derecho comparado le ofrece; sin embargo, también requiere de juristas con conocimientos en la materia, que tengan la capacidad de influir en la adaptación de estos esquemas internacionales a la realidad nacional, en su entorno histórico, social y jurídico.

4.1.7. Perspectiva de inclusión de los delitos informáticos en la Legislación Penal del país.

Como se puede inferir del análisis legislativo que se ha plasmado en páginas anteriores, en México los delitos informáticos carecen de un adecuado entorno jurídico.

Su función preventiva ha tenido que manifestarse a través de diversas formas de carácter administrativo, normativo y técnico, tales como: elaboración de exámenes psicométricos previos al ingreso de trabajadores al área de sistemas informáticos en las empresas, introducción de cláusulas especiales en los contratos de trabajo del personal informático, establecimiento de códigos de ética de carácter interno en las empresas, adopción de medidas en el acceso y control de las áreas informáticas de trabajo, capacitación adecuada del personal informático a fin de evitar actitudes negligentes, rotación en el uso de claves de acceso al sistema (passwords), entre otras.

Pero el adecuado control preventivo y correctivo de este tipo de ilícitos, solo podrá lograrse en la medida en que se introduzcan las disposiciones jurídicas específicas en los códigos penales sustantivos del país.

En términos generales, se requiere reglamentación jurídica en los siguientes rubros:

- Tipificación del delito informático.
- Caracterización del delito informático.
- Determinación técnica del grado de delictuosidad.
- Fijación de responsabilidades.
- Determinación de negligencia.
- Fijación de indemnizaciones por daños.
- Establecimiento de medidas preventivas.

- Capacitación (en torno a la materia informática) de las autoridades penales encargadas de sancionar este tipo de conductas.
- Establecimiento de la obligación de reportar esta clase de ilícitos.

Lo que se pretende lograr con la adecuada regulación jurídica de esta nueva modalidad de delitos propiciados por el uso indebido de los sistemas informáticos es:

1.- Protección de la información confidencial (bien jurídico informacional) contenida en los sistemas informáticos, respecto de la vulneración que frecuentemente sufre por la introducción ilícita de agentes delictivos a los sistemas informáticos.
2.- Respeto a la integridad humana (derecho a la intimidad) en los espacios virtuales; evitando la intromisión de agentes externos no deseados (como el abuso de publicidad o correos electrónicos no deseados).
3.- Protección al patrimonio de las personas, evitando en todo lo posible la manipulación de datos informáticos con fines lucrativos en beneficio de terceros ajenos a la titularidad de dicha información (fraudes informáticos).
4.- Fomentar la protección, independientemente de los sistemas particulares, de la información confidencial generada por el Gobierno Federal, las fuerzas armadas, la marina, etc., para evitar practicas delictivas como el (sabotaje y el espionaje informático).
5.- Protección a los menores, evitando en la medida de lo posible que se comercie con la pornografía infantil, así como evitando la libre circulación de programas no aptos para menores, la violencia, formas abusivas de mercadeo, etc., en la red y en general de toda actividad que lesione los derechos humanos fundamentales.
6.- Salvaguardar la propiedad intelectual, evitando la distribución no autorizada de trabajos protegidos mediante derechos reservados (piratería, etc.).

De esta manera, queda justificada en forma general, la gran necesidad de estructurar dentro de la Legislación Penal del país, una normatividad relativa a los "Delitos Informáticos", con el fin de establecer un marco jurídico con carácter positivo y vigente, que permita una adecuada aplicación y aprovechamiento de las tecnologías de la información en el país.

4.1.7.1. Propuesta de incorporación de los delitos informáticos en el Código Penal Federal del país.

Debido a la situación actual que enfrenta México, ante la ausencia de tipificación de los "delitos informáticos", estimo la conveniencia de su inclusión dentro del Código Penal Federal del país.

Se estima que el planteamiento de tales conductas ilícitas debe ser del a nivel del fuero federal, toda vez que por su complejidad no encuadran en ningún tipo penal existente. Asimismo, su tratamiento debe mantener cierta homogeneidad con el tratamiento que se le ha dado a esta clase de delitos a nivel internacional, con el fin de lograr una uniformidad regulatoria en torno a los mismos.

Sin embargo, sería ilógico pensar que la sistematización legal que se pretende hacer en materia de delitos informáticos, sea tarea única y exclusivamente de los legisladores, juristas y en general de los estudiosos del Derecho. Esta tarea requiere un esfuerzo conjunto de expertos tanto en la materia del Derecho, como en el área de la Informática, con el fin de contar con las técnicas y el personal adecuados para su consecución.

Además, no hay que olvidar que el Derecho se sirve de diversas disciplinas auxiliares para el logro de sus objetivos, con el fin de brindar "certeza y seguridad jurídica".

De tal forma que paralela a la tipificación de esta nueva modalidad de delitos, se requiere vislumbrar una instrumentación adecuada de las medidas tecnológicas y legales adjetivas indispensables para su completa operatividad.

Así por ejemplo, el método a seguir para investigar un delito de esta índole y lograr la identificación y persecución de su autor, así como para reunir los indicios y elementos suficientes para acreditar el cuerpo del delito y la probable responsabilidad del inculpado, será el mismo procedimiento que el planteado por la Criminalística, pero coadyuvado por la Informática Forense, que en este caso interviene como disciplina auxiliar del Derecho.

El autor Hugo Leal Neri, en su artículo "México: ¿Es factible la identificación y persecución del autor de un evento antisocial relacionado con la informática?, publicado en la Revista Electrónica de Derecho Informático; establece la conveniencia de crear una "Unidad Especializada en la investigación y persecución de Delitos Informáticos", organismo que halla su justificación en el Artículo 14, tercer párrafo de la Ley Orgánica de la Procuraduría General de la República, en cuyo texto se advierte que las "unidades especializadas son las idóneas para la persecución de un determinado género de delitos que requieren especialización" [64] .

Se considera acertada la opinión referida por este autor, toda vez que como ya se ha explicado, México se encuentra aún ante una etapa de "analfabetismo informático" en lo que a leyes se refiere, por lo que en tanto se imparte capacitación en torno a la materia al personal encargado de impartir justicia en el país, para lograr un adecuado seguimiento de esta nueva clase de ilícitos; se requiere de los conocimientos de especialistas en el ámbito de la informática que coadyuven junto con las autoridades penales del país en la persecución de estos delitos, y una "Unidad Especializada en la investigación y

[64] www.vlex.com.mx , México.

persecución de los Delitos Informáticos", sería el medio idóneo para su actuación. Este órgano operaría a nivel federal y sería un órgano dependiente de la Procuraduría General de la República.

Como ya se explicó, lo concerniente a la capacitación del personal que imparte justicia en el país es primordial para poder lograr una adecuada investigación y persecución de los delitos en cuestión. Por tal motivo, es imprescindible que se impartan cursos sobre la materia, orientados no solo a los responsables directos de administrar e impartir justicia en el país (Jueces, Agentes del Ministerio Público del Fuero Federal, Policía Judicial Federal, Peritos Especializados en el Área Informática), sino en general, a todas aquellas autoridades integrantes de los Poderes Ejecutivo, Legislativo y Federal, que son los encargados de establecer y hacer prevalecer el Estado de Derecho en el país.

Retomando la idea expuesta con anterioridad, sobre la propuesta de inclusión de los delitos informáticos dentro del Código Penal Federal del país, se reitera la propuesta de plasmar esta clase de delitos dentro del ordenamiento jurídico citado, con el fin de hacer factible y eficiente la investigación, persecución y sanción de los delitos informáticos, así como la identificación y procesamiento de su autor.

Se aprecia en base a las razones expuestas en el curso de la presente investigación, y en virtud de las características especiales que diferencian a este tipo de ilícitos del resto de las figuras típicas dèlictivas contempladas por la Legislación Penal del país, que es necesaria la inclusión de un Título exclusivamente reservado para el tratamiento y penalización de esta clase de conductas, que prevea todas las situaciones que puedan llegar a actualizarse con el uso indebido de los sistemas informáticos, a fin de no dejar impune cuestión alguna en torno a la materia.

Cabe hacer mención, que la regulación jurídica de esta clase de delitos en el Código Penal Federal, traería aparejada consecuentemente, la reforma y adición de algunas disposiciones en las legislaciones adjetivas del país, tal es el caso del Código Federal de Procedimientos Penales, en cuyo articulado se deberán contemplar, las reglas específicas para el tratamiento y resolución de las problemáticas suscitadas con motivo de los delitos informáticos, así como lo conducente a la adopción de técnicas pertinentes en materia de Informática Forense. La normatividad penal adjetiva es la idónea para hacer aplicables en la práctica forense, los tipos penales relacionados con la informática, para operativizarlos y guiar a las autoridades por el camino adecuado para la eficaz persecución y sanción de los mismos, y para lograr la captura y procesamiento de esta nueva clase de delincuentes surgidos con la era de la "sociedad de la información" y la creciente aplicación de las tecnologías informáticas.

CONCLUSIONES

PRIMERA. La irrupción de la Informática en la vida del hombre ha tenido un impacto de tal magnitud al grado de que en estos días es casi imposible concebir la globalización en que se vive sin la incidencia de la Informática en la Sociedad.

SEGUNDA. La ausencia de disposiciones jurídicas en torno a la materia informática, propicia la proliferación de acciones delictivas que vulneran los derechos de individualidad de aquellas personas que hacen uso de esta innovadora tecnología causándoles importantes perjuicios, tanto económicos como morales.

TERCERA. Por lo tanto, surge la necesidad de analizar nuevas modalidades de conductas delictivas derivadas del uso de las tecnologías de la información, con la finalidad de contar con elementos de juicio para su adecuada sanción y prevención.

CUARTA. Es un hecho que la comisión de conductas delictivas derivadas del uso indebido de las tecnologías de la información, se ha hecho cada vez más frecuente ante la inexistencia de estructuras jurídicas que fijen las pertinentes responsabilidades legales.

QUINTA. En virtud del inadecuado empleo del que han sido objeto las tecnologías informáticas, es que resulta inevitable la aplicación del Derecho, como un elemento disciplinador del proceso, capaz de brindar la protección necesaria para el adecuado desarrollo y evolución de dichas tecnologías , y al

mismo tiempo de proveer a la sociedad de los dos grandes valores que el Derecho persigue: Seguridad jurídica y Justicia.

SEXTA. Luego entonces, surge una nueva disciplina del Derecho denominada "Derecho Informático", cuyo objeto esencial es establecer una normatividad jurídica aplicable al fenómeno informático.

SÉPTIMA. Otro factor importante para el conveniente desarrollo de la Informática es proveer al país de una adecuada Política Informática que consienta realizar una planificación específica, a través de normas y objetivos que permitan orientarla y aprovecharla de la mejor forma para beneficio del país.

OCTAVA. A pesar de los índices de crecimiento en el uso de las tecnologías de la información, México enfrenta un gran problema social radicado en lo que se denomina " analfabetismo informático".

NOVENA. Los delitos informáticos surgen como una nueva modalidad de ilícitos cometidos a través del uso indebido de los medios informáticos, por lo tanto, es conveniente advertir la peculiaridad que guardan estos delitos frente al común denominador de conductas ilícitas contempladas en los textos legales.

DÉCIMA. Se afirma que los delitos informáticos como tales no existen en la Legislación Penal del país, ya que dichas conductas no se encuentran contempladas en los textos jurídicos; por lo tanto, al no actualizarse los presupuestos básicos para la tipificación de un delito como tal, es posible aseverar que tales ilícitos dentro del contexto legal del país son inexistentes.

DÉCIMO PRIMERA. El carente entorno jurídico que existe en México en materia de delitos informáticos es inadecuado, toda vez que encuadra y adapta esta clase de ilícitos, dentro de los llamados delitos convencionales, lo cual resulta

anacrónico, ya que los delitos informáticos son una nueva forma de delitos y por tanto merecen ser tratados como tales.

DÉCIMO SEGUNDA. En el aspecto legislativo, México tiene la ventaja de poder tomar como marco de referencia las experiencias que en el ámbito internacional se han dado en materia de delitos informáticos, así como de observar elementos valiosos que el derecho comparado le ofrece.

DÉCIMO TERCERA. Luego entonces, se justifica en forma general, la gran necesidad de estructurar dentro de la Legislación Penal del país, una normatividad relativa a los "Delitos Informáticos", con el fin de establecer un marco jurídico aplicable, que permita un adecuado aprovechamiento de las tecnologías de la información en el país.

PROPUESTA

ÚNICA.- Ante la inminente situación de impunidad e incertidumbre jurídica que se vive en México debido a la ausencia de disposiciones jurídicas que regulen la materia relativa a los Delitos Informáticos; se recomienda la inclusión de dichas conductas delictivas dentro del Código Penal Federal del país, en un capítulo especial, donde se aborde la tipificación de las mismas, a fin de establecer un marco jurídico con carácter positivo y vigente, que permita una adecuada aplicación y aprovechamiento de las tecnologías de la información.

Asimismo, existe la imperiosa necesidad de legislar en torno a la materia informática a nivel constitucional, toda vez que no existe disposición específica sobre ésta en la Constitución Política del país. Por tal motivo, se sugiere adicionar a la fracción X del Artículo 73 Constitucional, la facultad al Congreso de la Unión para legislar en torno a la materia "informática", y una vez promulgada la adición que se indica; establecer en la Ley Reglamentaria a dicho precepto constitucional, las áreas específicas sobre las cuales el Congreso de la Unión habrá de legislar.

De igual forma, se plantea la conveniencia de crear una "Unidad Especializada en la investigación y persecución de Delitos Informáticos", como órgano dependiente de la Procuraduría General de la República; organismo que deberá estar integrado por profesionales expertos en la materia Informática y en el Derecho, a fin de que coadyuven mutuamente para lograr una adecuada investigación y persecución de los delitos en cuestión.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

BARRAGÁN, JULIA. Informática y decisión jurídica. Biblioteca de Ética, Filosofía del Derecho y Política. Distribuidora Fontamara, S.A. Primera Edición. México, D.F. 1994.

BARRIOS GARRIDO, GABRIELA; MUÑOZ DE ALBA M., MARCIA; PÉREZ BUSTILLO, CAMILO. Internet y Derecho en México. Editorial McGraw Hill. Sociedad Internet de México. Primera Edición. México, 1998.

CASTELLANOS TENA, FERNANDO. Lineamientos Elementales de Derecho Penal (Parte General). Trigésima Cuarta Edición. Editorial Porrúa., México, D.F., 1994.

DICCIONARIO JURÍDICO 2000. Desarrollo Jurídico copyright 2000. Todos los derechos reservados DJ2K – 332.

DICCIONARIO JURÍDICO MEXICANO. Tomo V. Editorial Porrúa. México, 1985. pág.98.

HANCE, OLIVIER. SUZAN DIONNE BALZ. Leyes y Negocios en Internet. Traducción: Yasmín Juárez Parra. Revisión Técnica: Gabriela Barrios Garrido. Edit. Mc Graw Hill (Sociedad Internet de México). México, 1996. Traducido de la Primera Edición en Inglés de Business and Law on the Internet.

MEJÁN, LUIS MANUEL C. El Derecho a la Intimidad y la Informática. Editorial Porrúa. Segunda Edición. México, 1996.

MIR PUIG, S. Delincuencia Informática. Promociones y Publicaciones Universitarias. Librería Bárbara de Bragaza, 8. Oficinas y Revistas Tamayo y Bauś, 728004. Barcelona, 1992.

PADILLA SEGURA, JOSÉ ANTONIO. Informática Jurídica. Editorial SITESA (Sistemas Técnicos de Edición, S.A. de C.V.), IPN (Instituto Politécnico Nacional), Primera Edición, México, 1991.

PÉREZ-LUÑO, ANTONIO ENRIQUE. Ensayos de Informática Jurídica. Biblioteca de Ética, Filosofía del Derecho y Política. Distribuciones Fontamara, S.A. Primera Edición. México, D.F. 1996.

PÉREZ-LUÑO, ANTONIO ENRIQUE. Las Generaciones de los Derechos Humanos, en: Dialogo con la Jurisprudencia. N° 1, Gaceta Jurídica Editores. Lima, Perú. 1995.

POZO, LUZ MARÍA DEL; HERNÁNDEZ, RICARDO. Informática en Derecho. Biblioteca de Informática para profesionistas. Editorial Trillas. Primera Edición. México, D.F. Enero, 1992.

RÍOS ESTAVILLO, JUAN JOSÉ. Derecho e Informática en México. Universidad Nacional Autónoma de México (Instituto de Investigaciones Jurídicas). Serie E: Varios. Primera Edición. Número 83. México, 1997.

TÉLLEZ VALDÉS, JULIO. Derecho Informático. Editorial Mc Graw Hill/Interamericana de México, S.A. de C.V. Segunda Edición. México, 1996.

LEGISGRAFÍA

CÓDIGO PENAL FEDERAL (3ra. Versión). Interpretación por el Poder Judicial de la Federación. Coordinación General de Compilación y Sistematización de Tesis de la Suprema corte de Justicia de la Nación. México, 2000.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Anaya Editores S.A. Colección Leyes y Códigos. Enero, 2001.

OTROS MEDIOS DE INFORMACIÓN

PERIÓDICO UNIVERSITARIO "EL UNIVERSO" (El periódico de los Universitarios), Universidad Veracruzana, Dirección de Comunicación Social (Departamento de Prensa), Año 1, No. 31, Julio 16 de 2001, Xalapa, Veracruz, México. Pág. 23. (Título del artículo publicado: ¿Sabes lo que es un hacker?, Autor: Alejandro Rulfo Méndez, Sección Interfase).

http://www.arachnis.net/forolex, "Foro sobre delitos informáticos". Página de la Lic. Ivonne Muñoz. México, 2000.

http://www.bma.org.mx/ponencias1/comercio.html, ¿Debe México aprobar la Ley modelo de la CNUDMI sobre el Comercio Electrónico?. Barra Mexicana, Colegio de Abogados, A.C. Varsovia Número 1. Colonia Juárez. C.P. 06600. México, 1998.

http://www.cddhcu.gob.mx/camdip/foro/ , "Foro de Consulta sobre Derecho e Informática (Memorias)". Poder Legislativo Federal. Biblioteca del H. Congreso de la Unión, Ponencia: "Mecanismos existentes con ausencia de estructura, el Derecho Informático, el Delito Electrónico", Autor: Dra. Luz Ma. Del Pozo y Contreras, Guadalajara, Jal., Septiembre, 1996.

http://www.cddhcu.gob.mx/camdip/foro/, "Foro de Consulta sobre Derecho e Informática (Memorias)". Poder Legislativo Federal. Biblioteca del H. Congreso de la Unión.

http://www.ciberderecho.com.ar/, Página de Gustavo Daniel Tanús. Argentina.

http://www.informatica_jurídica.com.mx. "Legislación de Derecho Informático en México". Página de Odra Zúñiga. México.

http://www.jose_cuervo.lettera.net, Página de José Cuervo Álvarez. "Delitos Informáticos: Protección Penal de la Intimidad". España, 29 de Mayo de 1997.

http://www.monografias.com/trabajos6/delin/delin.shtm , Delitos Informáticos y Computacionales cuyos efectos se producen en el extranjero. (Bolivia).

http://www.uncitral.org/spanish/texts/electrcom/ml-ec.htm, Ley Modelo de la CNUDMI sobre Comercio Electrónico con la guía para su incorporación al Derecho Interno.

http://www.vlex.com/mx/c/Derecho_Inform@tico, Página de Derecho Informático, México.

www.vlex.com (España). Delitos Informáticos: Tipos, Legislación aplicable y Penas. 21 de Agosto del 2001. Doctrina – Artículos y Análisis.

www.vlex.com (España). Legislación sobre delitos informáticos. 21 de Agosto del 2001. Doctrina – Artículos y Análisis. Autor: Marcelo Manson.

www.vlex.com , (Argentina), "Presupuestos para la incriminación del Hacking", Autor: Hugo Daniel Carrión, Buenos Aires, Argentina.

www.vlex.com , México: ¿Es factible la identificación y persecución del autor de un evento antisocial relacionado con la informática?. Autor: Hugo Leal Neri. Doctrina - Artículos y Análisis.

www.vlex.com.mx, México: El Derecho a la Intimidad y el Derecho a la Información: ¿Garantías encontradas?, Fabio Rubén Troncozo Auld, Doctrina – Análisis y Artículos.

www.vlex.com.mx, Perú: El Bien Jurídico en el Delito Informático, Luis Miguel Reyna Alfaro. Doctrina - Artículos y Análisis.