UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

DELITOS INFORMÁTICOS: NECESIDAD DE SU LEGISLACIÓN EN NUESTRO PAÍS

TESIS

QUE COMO PARTE DE LOS REQUISITOS PARA OBTENER EL TITULO DE LICENCIADO EN

DERECHO

PRESENTA

BERENICE MONSERRAT ALONSO CAMACHO

DIRIGIDA POR

LIC. ARSENIO DURÁN BECERRA

M. EN D. MARTHA SOTO OBREGÓN

CENTRO UNIVERSITARIO
QUERÉTARTO. QRO.- MÉXICO
2002

ÍNDICE

INTRODUCCIÓN

Las telecomunicaciones a nivel mundial, han registrado un notorio avance en los últimos años, es evidente el beneficio que para la vida diaria significan estos adelantos; su utilización va desde la información continúa a todo el mundo, hasta el manejo a gran escala de las transacciones de las principales bolsas comerciales y de valores, pasando naturalmente por las diversas opciones de entretenimiento, hasta los prácticos e individuales intercambios de correos electrónicos; ha sido tan impresionante el cambio, que algunos sociólogos han llegado a llamar a esta reciente etapa de la historia, como la sociedad de la información.

Simultáneamente, la aparición de Internet ha venido a revolucionar estos sucesos, sobre todo si consideramos, que hoy en día es reconocida como el más importante conjunto de redes computacionales entrelazadas gracias a los llamados proveedores de conectividad, lo que determina el sorprendente nivel de velocidad de muchas operaciones. Para entrar a Internet la gente puede accesar de distintas maneras, pero en la mayoría de los casos se hace tan fácilmente como tener una conexión llamada *dial-in*, un *modem* y una línea telefónica. Una de las características más importantes de estas redes es que funcionan las 24 horas, los 365 días del año, y sin las tradicionales fronteras físicas creadas entre los Países.

Podemos decir, con toda certeza, que no existe ningún otro medio de comunicación que tenga la fuerza y potencia que ofrece Internet, ya que permite la difusión de conocimientos a un precio muy bajo, y a nivel mundial.

Paralelamente se destaca, que a esta altura del desarrollo de la *sociedad de información*, y de las tecnologías computacionales, debemos abordar otro tipo de situaciones que deben regularse de manera necesaria en todo el mundo, toda vez, que pueden cambiar totalmente el sentido positivo de la expansión de la tecnología informática, y transformarla en una manera fácil de vulnerar los derechos de individualidad de las personas que accesan a este sistema.

Para ser más precisos, la red se maneja en un mundo virtual, pero los conflictos comienzan a ser muy reales. El hecho de que Internet sea virtual, no le ha impedido que arrastre todos los vicios del mundo real en el que vivimos. Internet puede ser portador de contenidos potencialmente nocivos o ilegales, o bien puede ser utilizado como vehículo para actividades criminales que pueden afectar a distintos ámbitos.

Los delitos que se cometen en la informática, no pueden convertirse en nuestro país en sinónimo de impunidad, de no tomar las medidas necesarias en este momento, corremos el riesgo de que un instrumento tecnológico maravilloso, se transforme en una herramienta de ilícitos, para evitar esta situación los culpables deben ser sancionados.

El delito informático implica actividades criminales que en determinado momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, perjuicios, sabotaje, etc. Sin embargo debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación.

Por otro lado, recordemos que las facilidades para la comisión de delitos en la red son cada vez mayores: por el hecho de que la red trasciende las fronteras nacionales, por la velocidad de las comunicaciones.

Ahora bien, podemos afirmar que la lucha contra el delito en la red es especialmente complicada, por que la legislación contra el delito en esta materia, no avanza a la misma velocidad que la tecnología de la que se sirven los delincuentes cibernautas, porque no existe una autoridad mundial que supervise la red, facilitándose de esta manera las complicidades.

Resulta necesario, una cooperación internacional para la lucha contra el delito en la red, ya que una legislación global, resultaría actualmente imposible.

Es por ellos que esta tesis esta encaminada a buscar, el respeto a la integridad humana en los espacios virtuales, evitando la intromisión de agentes externos no deseados, protección a los menores, evitando en la medida de lo posible que se comercie con la pornografía infantil, que lesionan los derechos humanos fundamentales de la niñez, impulsar la protección, independientemente de los sistemas particulares que para este fin se determinen, de la información confidencial generada por el estado así como la protección a entidades tanto físicas como morales, salvaguardar la propiedad intelectual, el derecho a la intimidad y protección a la información en general.

CAPÍTULO PRIMERO

ANTECEDENTES GENERALES DEL DELITO INFORMÁTICO

Hay personas que consideran que los delitos informáticos, como tales, no existen. Existen diversas opiniones acerca de la necesidad o no de legislar en materia de d*elitos informáticos*, ya que surge la duda de que si estas conductas antisociales informáticas no se encuentran reguladas ya en nuestra legislación penal actual, es decir, que los medios electrónicos son solo un medio o una herramienta para cometer el delito, pero que la realidad es que estas conductas antisociales ya se encuentran tipificadas como un delito tradicional en nuestra legislación.

El *delito informático* implica actividades criminales que, en un primer momento, los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como, robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades de delinquir, siendo el uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho en esta materia. Así las cosas, nos vemos ante la existencia de muchos otros delitos que difícilmente podemos encuadrar en algún tipo penal de los ya existentes en nuestras leyes penales vigentes, de tal manera, que no tenemos otra alternativa mejor, que la de ponernos a la vanguardia y lograr que nuestras leyes se adapten de la mejor manera posible, a la realidad tecnológica que vivimos hoy en día.

Un claro ejemplo de la necesidad que tenemos de legislar en esta materia, y de que en realidad se debe considerar la existencia de los *delitos informáticos,* no solo como un medio comisivo sino como la posibilidad de un nuevo tipo penal, es el siguiente:

"En noviembre de 1988 surgió el famoso *gusano* de Internet, que lanzó Robert Morris Jr. este virus bloqueó más de 6.000 ordenadores"[1]. De no existir en ese momento el Acta sobre Fraude y Abuso Informático en Estados Unidos, hubiese sido imposible que se le hubiera juzgado por la comisión de ese delito.

Hay que recordar también, que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido.

En este mismo sentido, encontramos que casi el 90% de los delitos informáticos que investiga el FBI tienen que ver con el Internet, lo cual nos transporta directamente a la problemática de la inexistencia de fronteras en materia de los delitos informáticos, es decir, no sabemos con exactitud la ley de qué país debemos aplicar, debido, a que en la mayoría de las veces, no se sabe a ciencia cierta en donde se cometió el ilícito, tema que trataremos más adelante.

---

[1] **GRIMES Brad;** "Nuevos equipos para la seguridad pública"; PC Computing 1998; Revista mensual; Editorial Palsa; número 43; México

En la lucha contra la comisión de este tipo de conductas encontramos que países como España, Chile, Venezuela, entre otros, se han visto en la necesidad de crear grupos de policía e investigación especiales, dedicados exclusivamente a la persecución de delitos informáticos.

Por todo lo anterior, nos podemos dar cuenta de la imperiosa necesidad que existe en nuestro país de crear una legislación que contemple y tipifique a todas aquellas conductas antisociales denominadas "*Delitos Informáticos*".

1.1 Antecedentes del delito informático en México.

Actualmente, aún no podemos hablar de delitos informáticos en México, debido a que jurídicamente, los delitos Informáticos en México no existen, sin embargo materialmente estas conductas se realizan día a día con mayor frecuencia cada vez, es decir, los Delitos informáticos en México no existen jurídicamente debido a que nuestra legislación penal federal, no estipula ninguna sanción para las conductas antisociales informáticas, o dicho de otra manera no se sanciona aún a los delincuentes informáticos.

Sin embargo, a continuación les mostraré la escasa legislación que, en materia de delincuencia informática he encontrado en nuestro país.

1.2 Legislación que regula administrativa y penalmente las conductas antisociales relacionadas con la informática en nuestro país

Para el desarrollo de este apartado, se analizará la legislación que regula administrativa y penalmente las conductas antisociales relacionadas con la informática, pero que aún, no contemplan en sí, los delitos informáticos. En este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte, en virtud de que nuestra Constitución en su artículo 133 establece que: "Esta Constitución, las leyes que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las constituciones o leyes de los Estados"[2], por tal motivo a continuación expondré el marco jurídico que existe en nuestro país en relación con los delitos informáticos.

1.2.1 Tratado de Libre Comercio

Este instrumento internacional, firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII, específicamente en el artículo 1701 se establece lo siguiente:

---

[2] **Constitución Política de los Estados Unidos Mexicanos;** D.F México; Editorial Alco; 2000; pagina 143.

"*1. Cada una de las Partes otorgará en su territorio, a los nacionales de otra Parte, protección y defensa adecuada y eficaz para los derechos de propiedad intelectual, asegurándose a la vez de que las medidas destinadas a defender esos derechos no se conviertan en obstáculos al comercio legítimo.*

2. Con objeto de otorgar protección y defensa adecuada y eficaz a los derechos de propiedad intelectual, cada una de las Partes aplicará, cuando menos, este capítulo y las disposiciones sustantivas de:

a) Convenio de Ginebra 1971

b) Convenio de Berna 1971

c) Convenio de París 1967

Las Partes harán todo lo posible para adherirse a los textos citados de estos convenios si aún no son parte de ellos a la fecha de entrada en vigor de este Tratado"[3]

En términos generales, puede decirse que, este apartado del Tratado de Libre Comercio, se establecen como parte de las obligaciones de los estados signatarios en el área de propiedad intelectual, que deberán protegerse los programas de cómputo, es decir en el TLC, considera a los programas de cómputo como obras literarias así como a las bases de datos las considera compilaciones.

De esta forma, debe mencionarse que los tres estados parte de este tratado, también contemplaron la defensa de los derechos de propiedad intelectual, en virtud de su artículo 1714 se obligan a contener en su derecho interno, "... *Procedimientos de*

---

[3] **CALVO Nicolau Enrique y MONTES Suárez Eliseo;** "Tratados Internacionales en materia Tributaria"; México D.F; Themis; segunda Edición; 1998; Página 437

defensa de los derechos de propiedad intelectual, que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual. . ."[4]

En este orden, y con el objeto de que sirva para demostrar un antecedente para la propuesta que manejo en la presente tesis, es importante que señalemos el contenido del artículo 1717 titulado procedimientos y sanciones penales, el cual establece nuestro país se obliga con los estados signatarios del tratado que comento, que con la finalidad de proporcionar una seguridad jurídica a los nacionales de cada uno de los tres estados participantes en este tratado, se obligan a la creación de "*procedimientos y sanciones penales que se apliquen cuando menos en los casos de falsificación dolosa de marcas o de piratería de derechos de autor a escala comercial. . .*"[5] en este artículo se contempla de manera específica la figura de piratería de derechos de autor a escala comercial. Por lo que se refiere a los anexos de este capítulo, es decir el anexo 1718.14, el cual lleva por titulo *defensa de los derechos de propiedad intelectual,* se estableció lo siguiente: "*México hará su mayor esfuerzo por cumplir tan pronto como sea posible con las obligaciones del Artículo 1718, y lo hará en un plazo que no exceda tres años a partir de la fecha de firma de este Tratado*"[6].

Así mismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios el cual establece lo siguiente: "*Cada una de las Partes proveerá a cualquier persona los medios legales para impedir que los secretos industriales y de negocios se revelen, adquieran o usen por otras personas sin el consentimiento de la persona que legalmente*

---

[4] ***Idem*** página 438
[5] ***Ibidem***
[6] ***Idem;*** página 440.

tenga bajo control la información. . ."[7] hago referencia a este artículo, por que es precisamente en su apartado número dos, donde se habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos, es decir puedo entender que las penas y sanciones que se establecen el artículo 1717, se aplican para las violaciones a los secretos industriales, mediante el uso de medios electrónicos es decir el objeto de los *delitos informáticos*, es decir, aquí podemos ver claramente una causa más que justifica la necesidad de legislar en esta materia, debido a que los medios electrónicos que sirven para proteger el bien tutelado por este articulo del tratado, es decir, la propiedad intelectual, son vulnerables y de fácil violación por los delincuentes informáticos.

1.2.2 Ley Federal de Derechos de Autor

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997. Esta ley es de gran importancia para la elaboración de esta tesis, por tal motivo, considero importante hacer mención que el motor que impulsó a los legisladores para la creación de esta ley, fue el impacto que se estaba observando en materia de protección a los derechos de autor, ya que se habían estado presentado gran cantidad de ilícitos en esta materia, lo cual exigía una reforma con objeto de aclarar

[7] ***Idem;*** página 738.

las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión, con esta ley, se busca inhibir las conductas delictivas, y por otro lado, se usa como un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

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

En este sentido, el artículo 102[8] de esta Ley, protege los programas de computación, de la misma forma en que se protegen las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos ya sea

[8] **Ley Federal de Derechos de Autor**; sexta edición; D.F, México;Editorial Delma; 2002; pagina 43

en forma de código fuente o de código objeto. Se excluye de estas disposiciones de protección, todos aquellos programas de cómputo, que tengan por objeto causar efectos nocivos a otros programas o equipos, tales como virus gusanos etc., por otra parte, esta misma ley en su artículo 231 establece disposiciones legales en contre del comercio ilegal en tratándose de: "*...V. importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación...*"[9], a esta actividad se le conoce con el nombre de *hacking,* conducta que analizaremos más adelante, como una conducta antisocial informática, en este artículo indirectamente se esta refiriendo a un delito informático, sin embargo no esta prohibiendo la actividad de introducirse o violar un dispositivo de protección a un programa de computación, sino que a lo que se enfoca este artículo es única y exclusivamente a la comercialización de herramientas que permitan llevar a cabo esta actividad, con lo cual nos percatamos que el legislador, no tiene ni la menor idea de la capacidad e inteligencia tecnológica con la que gozan los delincuentes informáticos llámeseles ya sea *hackers* ó *crackers* como lo veremos en su oportunidad. Ahora bien, como lo mencionamos en el párrafo anterior, aún cuando la infracción se limita únicamente al área del comercio, permite la regulación administrativa de este tipo de conductas antisociales informáticas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, lo cual nos puede dar una idea de que, tal vez lentamente pero nuestros legisladores van poco a poco contemplando la posibilidad de la existencia material, aunque no jurídica, de los *delitos informáticos.*

---

[9] ***Ibidem***

Esta Ley en su artículo 231, fracciones II y VII trata de evitar la llamada piratería de programas en el área del comercio, prohibiendo, la producción, fabricación, almacenamiento, distribución, transportación es decir prohíbe cualquier forma de comercialización y uso de copias ilícitas de obras protegidas, considerando como obras protegidas un programa de computo. Aquí se permite la regulación administrativa de este tipo de conductas, como una posibilidad de proteger las conductas antisociales llevadas a cabo a través de medios electrónicos por la vía administrativa.

Otro punto de interés en esta ley, lo encontramos en su artículo 109, mismo que procederé a citar textualmente ya que me parece de importancia para esta investigación: "*El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el articulo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate*"[10] este artículo contenido en la ley de derechos de autor es de vital importancia debido a que gracias a este precepto legal, aunque aún de una manera muy vaga, entendemos que el bien jurídico tutelado en este precepto legal es de los más importantes para el hombre es decir el derecho a la Intimidad, ya que, se están protegiendo bases de datos de alta confidencialidad, información cuya propagación puede causar grandes daños tanto morales como materiales, por lo que en este artículo se trata de salvaguardar la intimidad personal, la cual es un aspecto de suma importancia. Un claro ejemplo de la importancia de la protección de estos

[10] ***Idem;*** página 45

tipos de base de datos, lo es el llamado correo electrónico (e – mail), el cual contiene información personal del usuario, así como la información necesaria para cometer un delito, utilizando los datos del usuario, en caso de que este medio sea violado, es por ello que insistimos en la pronta legislación para buscar la seguridad, y proteger la integridad de las personas que utilizan este medio, podemos decir que este es uno casos más comunes, sin embargo podemos mencionar varios ejemplos mas complejos en los que la violación de bases de datos que contengan información personal, pueden causar grandes daños, como lo podría ser, el caso de que un cyberdelincuente se introduzca en la base de datos de un hospital para tener acceso a las historias clínicas de los pacientes, y una vez obtenida la información, el cyberdelincuente la divulgue o publique los pacientes infectados con el virus del SIDA, con la única intención de, provocarles más problemas sociales de rechazo, mismos que con juntarían n un daño moral irreparable.

Después de haberme dado a la tarea de analizar los artículos de esta ley, en los cuales se habla de medios electrónicos y sistemas de computo, puedo percatarme que, al considerar éstos únicamente como una obra literaria, sigue dejando una enorme laguna jurídica a favor de los cyberdelincuentes, mismos que se aprovechan de esta situación de ilegalidad para cometer sus fechorías y que estas queden impunes.

Tal y como he venido sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas antisociales informáticas, día a día podemos darnos cuenta por diversos medios de comunicación, sobre las

pérdidas anuales que sufren las compañías fabricantes de programas informáticos, perdidas cuyas cantidades pueden llegar a ser estratosféricas por concepto de piratería de estos programas.

En este entendido, considero que por la gravedad de las conductas antisociales que se han generado y que se seguirán generando en nuestro país, y las implicaciones que traen aparejadas estas conductas, justifica la necesidad de su regulación penal.

Por lo anterior, el breve análisis de esta ley, en la materia que nos ocupa, corrobora la posición que hemos sostenido respecto a que, en las conductas antisociales realizadas a través de medios electrónicos, el bien jurídico a tutelar no es únicamente la propiedad intelectual, sino también otros derechos como lo es el derecho a la intimidad que he comentado, por lo que las conductas antisociales informáticas debería formar parte solamente de una Ley de derechos de autor, sino también deberían de ser materia de nuestro código penal federal, tal y como se ha hecho en otros países.

1.2.3 Código Penal para el Distrito Federal en materia de Fuero común y para toda la República en materia de Fuero Federal

Los *delitos informáticos* en México, poco a poco han ido llamando la atención de nuestros legisladores, de tal manera que se han logrado algunos avances en la creación de disposiciones legales que sancionen las conductas antisociales

informáticas, es decir los delitos informáticos, en este sentido, nuestro Código penal federal Vigente en su título noveno, denominado *Revelación de secretos y acceso ilícito sistemas y equipos de informática,* contiene normas que sancionan a estas actividades ilícitas informáticas, sin embargo aún no las contempla ni les da el carácter de *delitos informáticos,* como proponemos en esta tesis. A continuación me daré a la tarea de realizar un análisis de los artículos contenidos en el título del Código penal federal que comento.

La conducta ilícita regulada en el artículo 211[11] BIS, se trata de la actividad desarrollada por los Crackers, actividad que es conocida por la ciencia informática como el *Cracking.*

El *cracking,* es un delito informático mismo que analizaremos en su oportunidad, sin embargo, cabe comentar respecto a este artículo, que es demasiado limitativo, debido a que la actividad que están describiendo y castigando, solo es la de *modificar o bien destruir*, la información que se encuentre contenida en algún sistema o equipo de informática estableciendo una pena que asciende de seis meses a dos años de prisión y de cien a trescientos días multa, y en la segunda parte de este precepto legal y estableciendo una pena de de tres meses a un año de prisión o bien de cien a trescientos días multas a quién "*...sin autorización conozca o copie información contenida en un equipo o sistema de computo...*"[12], considero que es

---

[11] **Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de fuero Federal;** México D.F; Editorial Delma; 2002;página 143;

[12] ***Ibidem***

limitativo este precepto legal, ya que solo es aplicable la sanción si esta conducta se ejerce sistemas o equipos de informática que se encuentren *protegidos por algún mecanismo de seguridad,* esto restringe la aplicación de la pena establecida para aquellos que se introducen en sistemas informáticos de los particulares, somos presa fácil de los cyberdelincuentes, es decir el común de la sociedad como Ustedes o como yo, que contamos con equipos de computo no tan sofisticados tal vez, pero que de igual manera, podemos colocarnos en la posición del sujeto pasivo de la conducta ilícita.

Mi comentario respecto al articulo 211 BIS 2 es, que la conducta que se esta regulando y sancionando es la misma que en el anterior artículo, a diferencia de que en este el legislador se avoca a la protección exclusiva de la información contenida en sistemas o equipos de informática que estén protegidos por algún mecanismo de seguridad la variante es, que se aplicará la pena, siempre y cuando estos equipos o sistemas informáticos pertenezcan al estado, motivo por el cual la pena se incrementa a uno a cuatro años de prisión y de doscientos a seiscientos días multa, como se puede observar se sigue dejando si protección a los particulares ante este tipo de actividades delictivas informáticas.

Respecto al artículo 211[13] bis 3, al igual que los dos anteriores artículos se regula la intromisión ilegal a sistemas de computo, con la salvedad que este precepto esta directamente enfocado a aquellas personas que están autorizados para ingresar a dichos sistemas pero que indebidamente los modifique, destruya de cualquier otra

[13] ***Idem;*** página 144

forma provoque la pérdida de la información contenida en estos sistemas, este artículo, se encuentra protegiendo solamente la información del estado.

Por su parte en el artículo 211 bis 4, se regulan las mismas conductas ilícitas, la modificación, destrucción de la información que se contiene en sistemas o equipos de informática sin embargo aquí se intenta acertadamente, proteger todas las instituciones financieras.

Por lo que se refiere al artículo 211 bis 5 la diferencia existente entre el articulo anterior sería solamente que la conducta típica sea realizada por personas que si están autorizadas para ingresar a estos equipos o sistemas de computo de las instituciones financieras de nuestro país.

Estableciendo penas mas altas en tratándose de funcionarios o empleados de las instituciones que integran el sistema financiero.

De lo anterior podemos deducir que nuestros legisladores han hecho un gran esfuerzo por introducir en este código protección para los usuarios de sistemas informáticos, sin embargo únicamente se están limitando a legislar en materia de un solo delito informático, el *hacking*, por lo cual, el título noveno de el Código penal federal, no acaba de raíz con la problemática que nos ocupa en esta tesis, ya que el legislador olvida o tal vez lo que es peor, desconoce que los delitos que se pueden cometer a través de medios electrónicos o en contra de estos, van mucho más allá de la sola afectación de la información. Por lo tanto sigue siendo insuficiente la legislación existente.

1.3 Derecho Comparado de Legislaciones Extranjeras y la Legislación de nuestro País, en materia de delitos informáticos

Frente al avance de la tecnología, y a la importancia de la informática en el mundo entero, se hace necesaria a nivel mundial una reforma legislativa y la creación de tipos penales adecuados, por lo tanto considero de gran importancia hacer un breve análisis comparativo, de los países qué han decidido adoptar en sus legislaciones la penalización de las conductas antisociales que se llevan a cabo por a través de medios electrónicos es decir "delitos Informáticos"

El Comité de Informática de la UNESCO hizo público, en la XIV Conferencia de Autoridades Iberoamericanas de Informática, celebrada en La Habana, en noviembre de 1995, un llamamiento acerca de los virus informáticos, en el que se exhortó a los gobiernos a tomar las medidas legales para la creación y la distribución de virus informáticos fueran considerados delitos y penados por la ley; asimismo, se acordó que la ONU propusiera la implementación de una solución legal a este problema.

La Legislación Comparada muestra que aún son pocos los países que han legislado sobre el tema; en este aspecto la Legislación que ha llegado más lejos en el tema es la Legislación Estadounidense.

• **Estados Unidos de Norteamérica**[14].- Constituye el acercamiento más responsable y claro frente a este grave problema; generalmente no los define, se limita a describir el acto a fin de no constituir una valla para que en el futuro puedan incluirse ataques tecnológicos a los sistemas informáticos en cualquier modo que se realicen.

El Acta Federal de Abuso Computacional de 1994, que modificó al Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es, que no es y en que difieren de los virus, proscribe la transmisión de un programa, información, códigos o comandos que causan daños al ordenador, al sistema informático, a las redes, información, datos o programas. La ley constituyó un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994, diferencio el tratamiento, a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El Acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa; y para aquellos que lo transmiten por medio de una conducta imprudente la sanción fluctúa entre una multa y un año en prisión. El Acta de 1994 aclara que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un

[14] **BIERCE, William**; "El delito de violencia tecnológica en la legislación de Nueva York"; Derecho de la Alta Tecnología; Febrero 1994; Revista bimestral; No. 66; Estados Unidos; Página 20

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

El objetivo de los legisladores al realizar estas enmiendas, era el de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas, es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos. Sin embargo, considero que los legisladores estadounidenses, se han avocado únicamente a legislar en materia de virus y su transmisión, lo relevante de ésta, es que se distingue la voluntad del sujeto activo del delito es decir si la conducta la realiza de manera culposa o bien dolosa, lo cuál se verá reflejado, en las penas que se imponen a estos delitos.

- **Inglaterra.-** Este país, ha establecido sanciones para los creadores y distribuidores de virus, de hasta cinco años de privación de libertad.

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

- Espionaje de datos
- Estafa informática
- Falsificación de datos probatorios, junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos, conductas que se encuentran contenidas en los artículos 270, 271, 273
- Alteración de datos, es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático, destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal, el hallar un equivalente análogo al triple requisito de

---

[15] **http://www.buesa.net/en laces/hacking.htm**; Responsable de la Página Carlos Busón Buesa; fecha de consulta 21 de Septiembre de 2002.

acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita. Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue adoptada en los países escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática, el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una

nueva dimensión, pero que en realidad tan sólo constituyen un nuevo *modus operandi*, que no ofrece problemas para la aplicación de determinados tipos.

Sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos.

En un artículo publicado en la revista "Criminalità e tecnologia" Carlo Sarzana en Computers Crime. Rassagna Penitenziaria e Criminologia. 1-2 Año 1. Roma, Italia. página 53, nos proporciona una clara idea de lo que naciones europeas están haciendo actualmente para combatir el cybercrimen, mismas que a continuación describiré.

Francia.-

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- Acceso fraudulento a un sistema de elaboración de datos, en este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y

aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

- Sabotaje informático, en este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos, en este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados en este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos en este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Se puede decir que la tendencia legislativa actual en este país, es la de reconocer la destrucción de datos y programas informáticos como una conducta merecedora de sanción penal.

- **México.** En nuestro país solo la legislación penal del Estado de Sinaloa existe la figura jurídica del Delito informático, se creó dentro del Código penal de este

estado, dentro del título dedicado a delitos contra el patrimonio, en su capitulo V, reconoce y adopta esta figura jurídica de los delitos informáticos, considero importante su análisis debido a que, a diferencia del Código penal para el Distrito Federal en materia de fuero común y para toda la república en ,materia de fuero federal, el Código penal de Sinaloa, contempla los delitos informáticos de manera extensiva y no limitativa, al referirse a que cometerá este tipo de delitos en su artículo 217, como aquel que "*...use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información,*"[16]

En la fracción segunda de este mismo artículo, se establece que cometerá el delito informático aquella persona que: "*...Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora...*"[17]

Lo que se debe destacar en esta ley es que se castigará solo aquel que cometa la conducta con ánimo de dolo, con lo cual yo difiero, ya que, considero de gran importancia que se admita la forma culposa del delito, sobre todo, en su fracción segunda por que si puede darse el caso de ingresar circunstancialmente a un sistema sin la intención de generar un daño.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa, desde mi muy particular punto de vista, considero que la sanción pecuniaria que se estipula para este delito, debido

---

[16] **Código Penal para el Estado de Sinaloa;** México D.F; Editorial Delma; página 89; 2001
[17] ***Ibidem***

a que los daños materiales que se pueden causar con la comisión de estos delitos son incuantificables.

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

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

1.4 Propuestas legislativas en diversos Estados de la República en materia de delitos informáticos

Como ya lo he mencionado con anterioridad, nuestro país se encuentra muy lejos de poder contar con una legislación suficiente, para poder luchar con este tipo de conductas antisociales realizadas a través de medios electrónicos, Sinaloa es el único estado de nuestra República que ha logrado implementar en su legislación penal la existencia de los delitos informáticos, sin embargo, ya en nuestro Distrito Federal se han realizada varias propuestas para legislar en Materia de Delitos

informáticos desgraciadamente ninguna de estas ha tenido éxito. La última iniciativa de reformas y adiciones sobre diversas disposiciones del Código Penal para el Distrito Federal en materia de fuero común, y para toda la República en materia de fuero federal fue la realizada en la sesión del miércoles 22 de marzo del 2000, por el Diputado Francisco Suárez Tánori, dicha propuesta legislativa contiene lo siguiente:

En su artículo 167, el legislador, intenta regular en materia de delitos informáticos que tienen por objeto entorpecer una comunicación de una red pública, Al que interrumpiere la comunicación de un equipo de cómputo, imponiendo una sanción de uno a cinco años de prisión y multa de quinientos a cincuenta mil pesos.

Respecto a la violación de correspondencia, esta propuesta legislativa, en su artículo 173, sanciona la conducta encaminada a acceder a través de medios electrónicos, a la comunicación escrita dirigida a un tercero, estableciendo para esta conducta una sanción pecuniaria de tres a ciento ochenta jornadas de trabajo a favor de la comunidad, a lo cual yo considero, que la pena propuesta, no proporcional al daño que se causaría, realizando esta conducta.

Dentro del titulo de los Delitos en contra de las personas en su patrimonio, esta propuesta establece la posibilidad, de la existencia del Fraude en su artículo 389, el establece lo siguiente:

". . . al que actuando en calidad de usuario, intermediario, empresa proveedora de información, banco, o cualquier empresa comercializadora, ***utilice el intercambio electrónico de datos*** *para obtener con engaños*

ganancias indebidas, como dinero, valores, o cualquier otra cosa, ***aprovechándose de su acceso a los sistemas de redes computacionales,*** *adquiriendo, enajenando, transfiriendo, depositando, o dando en garantía productos y servicios de toda índole".*[18]

En materia de delitos informáticos, esta propuesta hace una directa referencia a lo que se conoce en la ciencia informática como, manipulación de programas, en su art castigando a aquél que sin autorización se apodere utilice o modifique información de carácter personal, familiar o bien de negocios, que estén contenidos en un sistema de computo ya sea público o privado, artículo en el que el bien jurídico tutelado es la información.

En la fracción segunda de este mismo artículo, se establece, que se castigará además, a todo aquél que difunda, revele, o ceda, imágenes o la información obtenida de manera ilícita.

En la fracción cuarta, se estipula una pena mayor para quien realice las conductas contenida en las fracciones anteriores, cuando se tenga acceso a dicha información por razón del trabajo o actividad que desempeñan.

Encontré, en la fracción VII de este articulo una obligación para todos los proveedores de Internet, es decir, se obliga a estos proveedores, a publicar la leyenda siguiente: "estas páginas contienen materiales aptos solo para adultos, si usted tiene menos de 18 años, deberá salir de esta página, si usted es un adulto que está interesado en evitar que menores de edad que manejan su equipo de cómputo,

---

[18] **http://info4.juridicas.unam.mx/ijure/fed/8/** ; Responsable de la Página UNAM, fecha de consulta 18 de mayo 2002.

tengan acceso a estas páginas, póngase en contacto con el proveedor de la información para su cancelación"[19]

De todo lo anterior, considero necesario llevar a cabo una distinción, respecto del uso de los medios informáticos como un simple medio para la comisión de un delito, y respecto de aquellas conductas en las que si es necesario crear un nuevo tipo penal, es por ellos que la propuesta realizada por el Diputado Francisco Suárez Tánori, ya que muy acertadamente, adhiere una fracción más al delito de fraude, en tratándose de su comisión por el uso de medios electrónicos, este en si no es un delito especial sino que puede ajustarse al tipo penal tradicional y existente ya en nuestro código penal federal, pero con una pena diferente, debido a los medios empleados para su comisión. Así también, en otras conductas como la manipulación de programas si será necesario crear un tipo penal ya que este tipo de conductas, no se ajusta a ninguno de los delitos que nuestro Código penal Federal contiene actualmente.

Sin embargo, cabe hacer mención que a pesar de que el Diputado, hace diversas reformas y adiciones debidamente acertadas en materia de delitos informáticos, también es cierto que hizo a un lado la problemática de los virus, omitió gravemente la legislación en la creación y distribución de los virus informáticos, olvidando que estos son una fuente principal para la comisión de delitos informáticos, si esta iniciativa fuese aprobada, entendemos que sufriría de una laguna en materia de virus con lo cual posiblemente resultaría poco eficaz su aplicación.

---

[19] ***Ibidem***

CAPITULO SEGUNDO

2. PROBLEMAS JURIDICOS DERIVADOS DE LAS NUEVAS TECNOLOGÍAS

La informática hoy en día, es una herramienta de desarrollo del hombre, se ha convertido en una necesidad, nos encontramos inmersos en un mundo donde la Informática ocupa el lugar número uno, en las actividades diarias de la sociedad entera, esto es una realidad y no podemos cerrar nuestras puertas al desarrollo. Está en casi todos los aspectos de la vida del hombre, desde los más triviales hasta los más sofisticados, pero también debemos reconocer que sociedades enteras seríamos un caos sin la existencia de la Informática, desgraciadamente la tecnología nos ha alcanzado y es el momento en que ninguna sociedad actual puede conducirse sin apoyarse de los sistemas electrónicos, por tal motivo podemos decir que existe una *dependencia computacional.*

El hombre interactúa en la sociedad valiéndose de medios electrónicos, y como en otras ramas del derecho es necesaria la creación de normas de conducta para hacer posible la vida en sociedad, ante esa nueva era de la tecnología.

El Derecho es un elemento regulador de las relaciones humanas, cuyo objetivo primordial es preservar el orden social. Desgraciadamente, las instituciones jurídicas con las que nuestro país cuenta actualmente, son obsoletas, nos encontramos ante la imposibilidad de hacer frente a las necesidades de nuestra sociedad.

El avance tecnológico de los medios electrónicos, en la actualidad se está utilizando como un medio o como una herramienta para perpetrar y facilitar diversas

actividades delictivas. La informática avanzada en manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, convierten a la tecnología en instrumentos para realizar actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público. Estas nuevas herramientas son usadas por personas, que por naturaleza humana, nos hacen enfrentar situaciones que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para sí nuevas técnicas de criminalidad es decir el uso de los sistemas electrónicos para el cometido de sus acciones perturbadoras en perjuicio de otros. Estas acciones perturbadoras de la convivencia social han surgido como una consecuencia de las nuevas herramientas tecnológicas, y desgraciadamente, nuestro país no se encuentra en condiciones de hacer frente en la lucha contra la cyberdelincuencia. En el ámbito mundial, se ha generado la búsqueda por regular de alguna manera las conductas ilícitas que se comenten dentro del mundo de la informática, sin embargo estos esfuerzos han sido insuficientes para proporcionar una verdadera seguridad informática, ya que esta búsqueda de medios jurídicos para dar solución a esta problemática, se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados delitos informáticos, pero ha provocado que los organismos de control social a nivel mundial comiencen a realizar acciones claras y evidentes ante la necesidad de controlar y detener la delincuencia informática.

Esta situación de inseguridad informática a la que nos estamos enfrentando, en el área de la protección legal de los derechos de las personas ya sean físicas o

morales, no ha detenido el avance de otros medios, provenientes de la misma área tecnológica, para los resguardos de nuestros bienes jurídicos, tales como la privacidad, bienestar, derechos de autor y tantos otros; como son la aparición en el ámbito privado de servicios que mediante el uso de nuevas tecnologías o metodologías permiten un ambiente de tranquilidad relativa, especialmente en el desarrollo del comercio electrónico.

En nuestro país es casi nula la legislación que regule las novedosas relaciones y realidades que se vinculan con la computación, a pesar del creciente número de computadoras que son adquiridas día con día. Si se toma en cuenta que en México, a pesar de no ser un país desarrollado, se han comenzado a depositar enormes cantidades de datos en sistemas de cómputo, algo urgente o eficaz debe ser realizado para prevenir y sancionar las conductas que lesionen tanto los bienes jurídicos tradicionales como los bienes jurídicos recientes, basados en la computación. La problemática de los delitos informáticos, requiere un estudio especial para determinar la medida en que la legislación penal deba prever la manifestación de delitos computacionales.

Nuestros legisladores han cerrado los ojos a la delincuencia informática, en consecuencia, tampoco se han dado a la tarea de llevar a cabo ningún acuerdo internacional, para enfrentar los nuevos retos de la seguridad de la red y la delincuencia informática, restándole la importancia y la urgencia con la que

requerimos de una nueva legislación que realmente conserve la seguridad social que es el objetivo del derecho.

En otros países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención. Hoy en día la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de Norteamérica, se han dirigido hacia la creación de los organismos necesarios para determinar que el problema de los delitos informáticos y sus consecuencias en la seguridad de las personas y en sus respectivas economías, son hechos graves y que requieren de urgentes medidas de todo tipo, tanto en el ámbito legislativo, de tecnologías y de socialización.

Desgraciadamente y a pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos.

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto.

Todas estas acciones internacionales no han sido suficientes para desafiar los hechos que acontecen en nuestra realidad informática y lograr cambiar la nula percepción de inseguridad que sentimos frente a estos nuevos hechos.

En este orden de ideas podemos formularnos las siguientes interrogantes:
¿Es necesaria la creación de nuevas normas que regulen la conducta del hombre en el uso de sistemas electrónicos?
¿Cuál es el bien jurídico que la ley debe tutelar en tratándose de delitos informáticos?
¿Es necesario el desarrollo de una nueva rama Autónoma del Derecho?

Para poder dar respuesta a algunas de las infinitas interrogantes que nos podemos formular dentro del tema que nos atañe, es necesario buscar mecanismos efectivos para solucionar los problemas que arrastran el uso y la difusión de las nuevas tecnologías.

2.1 Autonomía del Derecho Informático

Es necesario explicar, el porqué consideramos que en la actualidad ya podemos hablar de una verdadera Autonomía en materia de Derecho Informático, en lo que atañe al desarrollo y evolución del derecho informático, cabe mencionar que en aquellos países donde el fenómeno de la informática se encuentra masificado, es decir, donde la mayoría de la población tiene acceso real a los sistemas de

información, se habla del comienzo de una verdadera autonomía en ésta área. No es posible desconocer, por otra parte, que, tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero sí existe en el ámbito del derecho informático, en el orden mundial, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos y leyes especiales que promueven los entes legislativos con la finalidad de proveer a la sociedad de una seguridad informática que sea realmente efectiva al controlar y encuadrar todas aquéllas conductas antisociales llevadas a cabo a través de medios electrónicos. Sin embargo, aceptando la necesidad del desarrollo del derecho informático como rama autónoma, nuestro país se encuentra en la actualidad bastante lejos de lograr tal autonomía, habida cuenta que, en concordancia con la doctrina mayoritaria, es necesario que concurran cuatro aspectos: autonomía legislativa, autonomía jurisprudencial, autonomía académica y autonomía científica, aspectos con los que México no puede contar aún.

2.2 La informática en el Derecho Penal

Si bien hemos aludido a las inmensas posibilidades de la informática como instrumento de desarrollo económico-social y cultural, y a su vez, nos hemos percatado de sus consecuencias negativas, no me he detenido, aún, al análisis de cómo es que el mal uso de las nuevas tecnologías de la información, requiere, en lo relacionado con las nuevas conductas antisociales llevadas a cabo a través de estos medios electrónicos, la urgente intervención del Derecho penal.

Naturalmente que, frente a un fenómeno de tal magnitud como el que se está tratando aquí, es imposible que la criminalidad quedara exenta del impacto de la tecnología informática. Algunos autores consideran que "La informática abre nuevos horizontes al delincuente, incita su imaginación, favorece su impunidad y potencía los efectos del delito convencional"[20]. Y a ello contribuye la facilidad para la comisión y encubrimiento de estas conductas antisociales y la dificultad para su descubrimiento, prueba y persecución. Como era de suponerse, resultaría imposible, que los delincuentes dejaran pasar la oportunidad de poder abusar de esas óptimas condiciones para delinquir ante el impacto que la tecnología informática ha arrojado al mundo, es por ello que el derecho penal se esta imponiendo de dicha situación para buscar la mejor forma de combatir este tipo de nuevas conductas.

2.3 Aproximación al Delito Informático

Entre el Derecho y la Informática se podrían apreciar dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la informática jurídica. Pero al considerar a la informática como objeto del Derecho, se hace alusión al Derecho de la Informática o simplemente Derecho Informático. La cibernética juega un papel bastante importante en estas relaciones establecidas. Por cuanto sabemos que la cibernética es actualmente, una de las ciencias más importantes en la vida del ser humano, y surge como necesidad de

---

[20] **MOLINA García** Pablo; "Informática y Derecho Penal, en Implicaciones socio-jurídicas de las tecnologías de la información"; Madrid España; Editorial Citema; 1984; página 39

obtener una ciencia general que estudie y trate la relación de las demás ciencias. De esta manera, tenemos a la ciencia informática y por otro lado a la ciencia del derecho; amabas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el derecho en su aplicación, es ayudado por la informática; pero resulta que ésta debe estar estructurada por ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas informáticas; así pues, nace el derecho informático como una ciencia que surge a raíz de la cibernética, como una ciencia que trata la relación derecho e informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer, regular las acciones, procesos, aplicaciones, relaciones jurídicas, en su complejidad, de la informática. Pero del otro lado encontramos a la informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.

En efecto, la informática no puede juzgarse en su simple exterioridad, como utilización de aparatos o elementos físicos o electrónicos, pura y llanamente; sino que, en el modo de proceder se crean unas relaciones ínter subjetivas de las personas físicas o morales y de entidades del Estado, y surgen entonces un conjunto de reglas técnicas conectadas con el Derecho, que vienen a constituir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la Ciencia Informática, con autonomía propia. Esos principios conforman las directrices propias de la institución informática, y viene a constituir las pautas de la interrelación nacional-universal, con otras normas mundiales supranacionales y cuyo objeto será necesario recoger mediante tratados públicos que hagan posible el proceso comunicacional en sus propios.

CAPITULO TERCERO

3. PROBLEMAS DE VALIDEZ DE LOS DELITOS INFORMÁTICOS

En este apartado, se llevara a cabo un estudio, de los límites y alcances de la ley penal, específicamente en materia de las conductas antisociales informáticas, ya que como se observará a continuación uno de los fundamentales problemas para la persecución de este tipo de conductas, lo es en el ámbito territorial, ya que, una conducta antisocial informática se puede llevar a cabo en un país y surtir efectos o causar su resultado en otro, problemática que analizaré en su oportunidad más adelante.

3.1 Validez Material de la Ley Penal

La validez material de la ley penal se refiere a la competencia legislativa, en el artículo 124[21] de nuestra Ley Suprema se establece que "Las facultades que no estén expresamente concedidas por esta Constitución a los funcionarios federales, se entienden reservadas a los Estados", este artículo nos da dos opciones de competencia, materia Federal, y materia del fuero común, del mismo precepto se deduce también que las facultades que se le confieren al poder federal, son de carácter limitativo, puesto que solo pueden actuar en lo que se les esta expresamente permitido.

---

[21] **Constitución Política**; *op. cit*; página 60.

De igual manera el artículo 73 fracción XXI de la misma Ley, establece que "El Congreso de la Unión tiene facultad... fracción XXI para establecer los delitos y faltas contra la Federación y fijar los castigos que por ellos deban imponerse..."[22]

En Materia de fuero Común, cada uno de las 31 Entidades Federativas tienen la facultad de dictar a través de su poder legislativo local, las leyes que se consideren pertinentes para el buen gobierno de dicha entidad obviamente siempre y cuando no sean contrarias a nuestra Ley Suprema.

Nuestra carta magna también confiere facultades legislativas al Congreso de la Unión, que realiza la actividad legislativa para el D.F, mismas leyes que serán aplicables a toda la republica cuando se traten de afectaciones a la Federación.

En este orden de ideas podemos decir que cada entidad Federativa tiene la capacidad de llevar a cabo actividad legislativa en materia de delitos informáticos, como lo realizó en su momento el Estado de Sinaloa, Sin embargo en esta trabajo estamos sustentando que los delitos Informáticos sean considerados como delitos Federales ya que de acuerdo a lo asentado líneas arriba la afectación es directamente a la federación.

Por ultimo, en este mismo apartado de la Validez material de la ley penal encontramos a aquéllos delitos que son competencia del Derecho penal Militar, tema que , ya que en esta materia cuenta con una reglamentación especial solamente de aquellos delitos que se cometen en contra de la disciplina militar, de tal manera que estas leyes solo podrán ser aplicadas a los miembros del ejercito, pero no tacaremos

---

[22] ***Ibidem***

a detalle este punto por que no es materia de estudio en el presente trabajo de investigación.

3.2 Validez espacial de la Ley Penal

Este apartado se refiere exclusivamente a la aplicabilidad de la ley, como ya lo dijimos en el punto anterior, la ley es creada por cada Entidad Federativa, y por la Federación, por tanto, la validez espacial, hace referencia a que la ley deberá ser aplicada única y exclusivamente dentro del territorio para el cual fue creada, y no en ningún otro. Sin embargo, en muchas ocasiones aparecen diversos problemas para determinar cual es la norma aplicable, sobre todo, en tratándose de delitos que tuvieron lugar fuera del territorio nacional, que es justamente lo que pasa en materia de *delitos Informáticos*, ya que pueden cometerse desde cualquier lugar del mundo y surtir efectos dentro del territorio Mexicano o Viceversa, de aquí deriva la importancia de explicar los mas ampliamente posible este apartado.

En el ámbito de validez espacial de la ley penal, encontramos diversos principios que nos ayudaran a obtener una mayor comprensión de este tema.

- Principio de Territorialidad.- Se refiere (como ya lo expliqué en el párrafo anterior) a que las leyes se aplicaran solamente en el territorio para el cual fueron creadas, y nunca fuera de este, de la misma forma en que no podrán ser aplicadas fuera del territorio mexicano, de acuerdo a este principio la norma jurídica solo se aplicara dentro del territorio para el cual fue creado, a los ciudadanos o extranjeros que infrinjan dicha norma.

En el artículo Primero del Código Penal Federal, en su artículo 1°, establece expresamente el Ámbito de Validez especial de la Ley Penal señalando que: *"Este Código se aplicara en toda la Republica para los delitos del orden Federal"*[23].

- Principio de Extraterritorialidad.- Este principio es el que más nos interesa en el estudio de esta investigación, debido a la problemática que se presenta para llevara a cabo la aplicación de la ley en materia de delitos informáticos, es por ello que considero importante detenernos en este principio para analizarlo más a fondo.

A lo largo del desarrollo de este trabajo de investigación hemos manifestado que los medios electrónicos, los sistemas informáticos, el Internet etc., son un vehículo de comunicación multimedia, mundial, vertiginoso, asequible a casi todas las economías, difícil de controlar por gobiernos y particulares, ya que todos estos medios tienen albergando textos, sonidos, imágenes con o sin movimiento, difundiéndolas instantáneamente, sin embargo el común denominador, de esta problemática lo es el Internet .

El Internet, algunas veces llamado simplemente "La Red", "es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, contando o no con el permiso de quien deba darlo, accesar información de otra computadora y

[23] **Código Penal para el Distrito Federal;** *Op. Cit;* página 3

poder tener inclusive comunicación directa con otros usuarios en otras computadoras"[24].

Hoy en día, el Internet es un medio de comunicación público, cooperativo y autosuficiente, en términos económicos, accesible a cientos de millones de gentes en el mundo entero, razón por la que red o Internet, añade una mayor facilidad, difusión, y especialmente ***una internacionalización del delito*** que aún no tiene una respuesta jurídica clara. Los efectos transfronterizos de los daños producidos por ejemplo, por los virus informáticos, obligan a determinar cuál debe ser la jurisdicción competente para enjuiciar los delitos que tienen origen en un país y causan sus efectos en otro, cobrando gran importancia los Convenios de Reciprocidad.

En México encontramos que para determinar cual es la jurisdicción competente para conocer de un delito perpetrado en un lugar y cuyos resultados fueron en otro lugar fuera del territorio Nacional como puede suceder con los delitos de los llamados Informáticos, nos tenemos que remitir a l Código Penal Federal ya que se encontramos una posible solución a esta problemática en los artículos siguientes:

En su artículo tercero, esta ley hace referencia a que todos aquellos delitos continuados que se inicien en país extranjero y que se sigan cometiendo en nuestro país serán castigados de acuerdo a las leyes mexicanas independientemente de la nacionalidad del sujeto activo

---

[24] **http://www.informaticamilenium.com.mx**; Responsable de la página Jorge Marcelo Torres Lipe; fecha de consulta 13 de Abril del 2002.

En el artículo cuarto, el legislador consideró importante que aquellos delitos que se lleven a cabo en países extranjeros ya sean cometidos por mexicanos contra extranjeros, mexicanos contra mexicanos, o de un extranjero en contra de un mexicano, siempre y cuando el sujeto activo del delito se encuentre en territorio mexicano, no haya sido juzgado por ese delito en el territorio en el que se cometió el delio, y que el delito este contemplado como tal, en ambas legislaciones, es decir en el lugar donde tuvo origen el delito y en México.

El código penal federal hace una aclaración pertinente en su artículo sexto, estableciendo de que en caso de que el delito que se cometió en país extranjero, no está contemplado de la misma forma en nuestro país, se aplicara la ley Mexicana, siempre y cuando, la conducta realizada, se encuentre contemplada en una ley especial o en un tratado internacional en el que México se estado signatario,

A pesar de la existencia de estos preceptos que han ayudado a la aplicación de la ley en materia de extraterritorialidad, nos encontramos con ciertos obstáculos en el momento de la persecución de esta clase de delitos Informáticos tales como:

- La escasez de medios técnicos dedicados a la actividad investigadora de estos delitos, es decir falta de la Tecnología necesaria por parte de nuestras autoridades para la persecución de estos.
- Ventaja tecnológica de los delincuentes cibernéticos.
- Exceso de tiempo entre la solicitud de intervención judicial y su concesión y trámite.

► Principio Personal.- Este principio establece que la ley que se deberá aplicar dependerá de la Nación a la que pertenezca el delincuente sin necesidad de tomar en cuanta en que lugar se perpetro el delito o bien en que lugar surtió sus efectos, este principio lo vemos reflejado en el artículo 4° del Código Penal mismo que analizamos líneas arriba, y que determina las situaciones en las cuales aplicará este principio.

► Principio Real.- Por lo que concierne a este principio, éste hace alusión únicamente a los bienes jurídicos tutelados, una vez analizado cual es el bien que la ley esta protegiendo, entonces en base a ello se procederá a determinar cual será le ley aplicable a ese caso.

► Principio Universal.- Por ultimo, este principio refiere que todas las Naciones independientemente del lugar en que se cometió el delito, el lugar en donde tuvo sus efectos o bien independientemente de la nacionalidad del delincuente, podrán sancionar al delincuente.

Para concluir con este apartado de la Validez Espacial de la ley penal es importante estudiar un conceptos que van a coadyuvar para la solución de la problemática de la aplicación de ley penal en materia de los delitos informáticas los cuales son materia de estudio en esta investigación, el cual es la Extradición.

La Extradición es una figura jurídica, en la cual un Estado hace entrega a otro Estado de un delincuente que se refugió en aquel, para evadir la ley penal, ya que como es bien sabido, aquel que comete un delito debe ser enjuiciado y castigado en el lugar en donde el delito tuvo lugar. Al respecto el maestro Jiménez de Asúa define la

extradición como "...la entrega del acusado o del condenado, para juzgarlo o ejecutar la pena, mediante petición del Estado donde el delito perpetróse, hecha por aquel país en que buscó refugio"[25].

La extradición se puede clasificar de la siguiente forma:

a) Activa.- es la extradición que ejerce el estado que la solicita es decir, el estado quien pide la remisión del delincuente para ser juzgado en el país solicitante.

b) Pasiva.- este tipo, es la realizada por el país del que se solicitó la extradición, es decir del país quién entrega el delincuente a otro.

c) Espontánea.- Es cuando el País en donde se encuentra refugiado el agente que cometió el delito, lo envía al país en donde se perpetró el delito, sin que este lo solicite.

d) Voluntaria.- en este caso, es cuando el delincuente por su propia voluntad, se entrega a su país de origen.

e) De paso o tránsito.- Es la posibilidad que un Estado da a un delincuente para que transite por éste mientras se está llevando a cabo su traslado al país en donde se cometió el delito.

De todo lo anterior no me queda más que decir que, el unificar criterios a nivel internacional es fundamental, puesto que el fenómeno de las nuevas tecnologías de información, no ocurre dentro de ninguna frontera, sino fuera de todas. Si se llama internacional al derecho de las relaciones entre estados, nada ha surgido con tanta

---

[25] **JIMÉNEZ DE ASÚA** Luis; "La ley y el Delito"; principios del derecho penal; 10° edición; Buenos Aires Argentina; 1980; página 215

claridad, como la realidad del ciberespacio y los nombres de dominio como merecedores del título de "internacionales", en la medida que todo lo que ocurre es en la esfera transfronteriza. Considero que la simple regulación en materia de *delitos informáticos*, no acaba por completo o de raíz con esta problemática, sino que estas deberán ser complementadas con la existencia de tratados a nivel internacional, y la creación de organizaciones internacionales que se formen con el objetivo de combatir el cybercrimen.

3.3 Validez temporal de la Ley Penal

Este aspecto de la Validez de la ley penal, tiene que ver directamente con la vigencia de la ley, ya que es imposible que el Estado exija el cumplimiento de la ley cuando esta no ha entrado en vigencia de acuerdo a las formalidades de ley o bien cuando esta ha sido derogada, en otros términos, la ley únicamente podrá ser aplicada mientras ésta se encuentre en vigor. De lo anterior se desprende una problemática denominada *retroactividad,* ésta figura está reconocida por nuestra Constitución en su artículo 14 párrafo primero "A ninguna ley se le dará efecto retroactivo, en perjuicio de persona alguna."[26] Esto quiere decir que ninguna Ley se podrá aplicar respecto de un hecho que se suscitó con anterioridad a la existencia de la ley, sin embargo este mismo precepto Constitucional en su parte final aclara nunca será en perjuicio de persona alguna, lo cual lleva implícito que la retroactividad si se podrá

---

[26] **Constitución Política**; *op. cit;* página 33

efectuar siempre y cuando sea en beneficio de la persona. Esta última parte lo encontramos reforzado en el artículo 56 del Código penal Federal en el cual el legislador establece que "*Cuando entre la comisión de un delito y la extinción de la pena o medida de seguridad entrare en vigor una nueva ley, se estará a lo dispuesto en la mas favorable al inculpado o sentenciado. La autoridad que este conociendo del asunto o ejecutando la sanción aplicara de oficio la ley mas favorable...*"[27].

3.4 Validez personal de la Ley Penal

El ámbito personal de la ley penal, atiende a la siguiente interrogante ¿a quién va dirigida la ley?, no hay que confundir es aspecto de validez de la ley penal con la igualdad de los Ciudadanos ante la Ley, la Garantía de igualdad consagrada en nuestra Constitución, sin embargo, es importante hacer referencia a las excepciones que existen a este principio de Igualdad ante la ley.

Básicamente son dos áreas en las que caben las excepciones al principio de igualdad, el primero de ellos es en lo concerniente a nuestro derecho interno, en cual existen consideraciones especiales a algunos servidores cuando estos cometen un delito, lo cual es a través del juicio político.

Y por otro lado encontramos al derecho Internacional, el cual es el que nos interesa en razón del tema que estamos analizando, aquí aparece la figura de la inmunidad, derecho que se concede a los diplomáticos de países extranjeros, que

---

[27] **Código Penal para el Distrito Federal;** *op. cit;* página 47

encontrándose en ejercicio de sus funciones, infringen la ley dentro de nuestro territorio se encuentran en territorio nacional.

En ambos casos, este tratamiento especial se justifica en la intención de proporcionar y proteger, ya sea al servidor público o al diplomático extranjero, del pleno ejercicio de sus actividades, sin que puedan ser objeto de falsas acusaciones que les impidan desarrollar sus actividades laborales.

CAPITULO CUARTO

4. DEFINICIÓN DE DELITO INFORMÁTICO.

Muchos estudiosos del Derecho Penal, han intentado formular una noción del delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible, que la definición del delito general, debido a la diversidad de culturas y sistemas jurídicos de cada pueblo y de cada siglo.

Por su parte, Eugenio Cuello Calón establece que el delito "es la acción humana antijurídica, típica, culpable y punible"[28] de esta definición podemos deducir que los elementos integrantes del delito para Cuello Calón son los siguientes:

El delito es una conducta humano, es una acción u omisión.

Dicha conducta humana debe ser antijurídica, es decir debe lesionar o poner en peligro un interés jurídicamente protegido.

Debe corresponder a un tipo legal establecido por La Ley, es decir debe estar tipificado.

Así mismo esta conducta debe ser culpable, dolosa (dañina intención de cometer la afectación) y solamente una acción puede ser imputable cuando se le atribuye una determinada persona.

---

[28] **CASTELLANOS Fernando;** "Lineamientos elementales de Derecho Penal"; trigésima sexta edición; México D.F; Porrúa; 1996; página 129

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Podríamos llevar a cabo una lista de las diversas definiciones que, a lo largo de la historia de la ciencia del derecho, innumerables autores nos han proporcionado. Sin embargo, para efectos del tema de *delitos informáticos* que nos ocupa, prefiero a pegarme a la establecida por el artículo séptimo del Código penal para el Distrito Federal en materia de fuero común y para toda la República en materia de fuero federal "Delito es el acto u omisión que sancionan las leyes penales"[29]

En la actualidad no contamos con una definición clara de lo que son los delitos informáticos, el mismo tratadista Pedro Zamora Sánchez, establece que "Aún no existe una definición reconocida internacionalmente que precise lo que constituye un ilícito"[30]. Sin embargo, ciertos autores y especialistas coinciden en que no podemos negarnos a la existencia del fenómeno de la cyberdelincuencia, y por tal motivo, se han proporcionado diversidad de definiciones, intentando llegar a la definición más acertada, desafortunadamente, no han tenido éxito en esta tarea, debido a que la doctrina no se apoya en un parámetro claro y común desde el cual comenzar los intentos de definición.

Una de las definiciones más aceptadas, es la proporcionada por el Profesor Alemán Urich Sieber, quien establece lo siguiente "Delitos informáticos son todas las lesiones

---

[29] **Código penal para el Distrito Federal**; *op. cit.*; página 3

[30] **ZAMORA Sánchez** Pedro; "Marco Jurídico del Lavado de Dinero"; México; Oxford University prees México; 1999; Pagina 53

dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente"[31]. Así mismo, el autor mexicano Julio Téllez Valdez, señala 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)"[32]

Por mi parte, podría definir los *delitos informáticos* como, toda acción u omisión, realizada en el entorno informático, que cause un perjuicio a otro, existiendo o no ánimo de lucro, o bien, que por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique a la víctima, tipificado por La Ley, y sancionado con una pena.

4.1 Enfoque del delito informático en la teoría del delito

De la definición de *delitos informáticos* que di en el párrafo anterior, podemos deducir que los elementos que integran al delito informático son:

Conducta.- es decir la acción u omisión.

Tipicidad.- que se encuentre tipificado por una ley.

La teoría del delito, nos menciona otros elementos que integran al delito, como lo pueden ser, la antijuridicidad, la voluntad, la culpabilidad etc., sin embargo, yo me avocaré solamente al estudio de los elementos que integran el delito de acuerdo a la

---

[31] **SIEBER, Urich;** "Criminología Cibernética"; München Deutschland; Mc. Graw Hill; D.F, México;1995; página 83

[32] **CASTELLANOS;** *op. cit;* página 129

definición que proporciono, misma que se encuentra apegada a la definición de delito proporcionada por el artículo séptimo del Código penal Federal vigente.

4.2 Conducta como elemento del delito informático

"La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito"[33]

No cabe duda que el *delito informático,* antes que otra cosa, es una conducta, refiriéndose esta, ya sea a un acto positivo, o ya sea a un acto negativo, es decir una acción u omisión, un hacer o un dejar de hacer. Podemos encontrar este elemento manifestándose de diversas formas como una *acción, omisión o comisión por omisión.* Por acción debemos entender la ejecución de un acto volitivo del hombre, por otra parte, la omisión y la comisión por omisión serán entonces una inactividad, un dejar de hacer.

La diferencia que podemos encontrar entre la omisión y la comisión por omisión será que en la primera de ellas se esta llevando a cabo una trasgresión a un deber jurídico establecido es decir se deja de hacer algo que jurídicamente se esta obligado a hacer, en la segunda de ellas es decir en lo referente a la comisión por omisión se quebrantan dos deberes jurídicos uno de ellos será el hacer y otro lo será el dejar de hacer.

---

[33] ***Idem***; página 149

Hablamos de que la conducta puede manifestarse de diversas formas entre las cuales mencionamos la Acción considero pertinente desglosar los elementos de esta de la siguiente manera:

a) Voluntad.- esta se refiere a la persecución de un fin, es decir a lo "que podemos denominar el "querer humano" de cometer el delito en otras palabras en la intención de querer el resultado.

b) Actividad.- es precisamente el Hacer, lo que el ser humano Hace para cometer el delito.

c) Resultado.- es la consecuencia de la conducta, es el efecto buscado *por el* hombre y contenido en una ley penal como delito.

d) Nexo de Causalidad.- es la relación próxima existente entre la conducta y el resultado, es el elemento que une la causa con el resultad, de no existir este lazo entre la causa y el efecto, jamás se podrá atribuir este a la causa.

En este orden de ideas también considero prudente esclarecer, que los elementos de la omisión y de comisión por omisión son, al igual que la acción, la Voluntad, la actividad, el resultado y el nexo causal, ya que como lo he explicado líneas arriba, la acción implica un Hacer, en cuanto a que la Omisión es un no hacer o dejar de hacer.

4.3 Tipicidad como elemento del delito informático

Para lograr un buen entendimiento de lo que es la tipicidad, antes que nada es necesario determinar lo que es para el derecho penal el ***TIPO,*** ya que en diversas ocasiones suele haber innumerables confusiones entre el *Tipo* y la *Tipicidad,* por un lado concebimos que "El tipo es la descripción legal de un delito, o bien la abstracción plasmada en la ley de la figura delictiva"[34], es cuando el legislador plasma o describe en la ley penal la conducta que debe ser considerada delito. Por el contrario, la *Tipicidad* es "la adecuación de una conducta concreta con la descripción legal formulada en abstracto"[35], por lo anterior deducimos que la tipicidad es el momento en que el juzgador encuadra la conducta en el tipo penal para de esta forma decidir si una determinada conducta podrá ser considerada delito o no, una vez que la conducta embone perfectamente y contenga en si misma todos y cada uno de los elementos tipo. De tal forma nuestra Carta Magna en su artículo 14 tercer párrafo establece que "en los Juicios del orden criminal queda prohibido imponer por simple analogía o por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata."[36], en tal virtud jurídicamente no podrá existir un delito si no existe la tipicidad.

Irma Amuchategui en su libro titulado "Derecho penal", nos proporciona una lista de los principios generales de la tipicidad mismos que a continuación describo:

- *Nullum crimen sine lege.-* No hay delito sin ley.

---

[34] **AMUCHATEGUI Requena** Irma; "Derecho Penal"; D.F, México; Harla; 1993 página 56
[35] **CASTELLANOS Fernando;** *op cit;* página 167
[36] **Constitución Política;** *op. cit.;* página 33

- *Nullum crimen sine tipo.*- No hay delito sin tipo.
- *Nulla poena sine tipo.*- No hay pena sin tipo.
- *Nulla poena sine crimen.*- No hay pena sin crimen.
- *Nulla poena sine lege.*- No hay pena sin ley.

Nuestra Constitución en su artículo 14 último párrafo reconoce y da validez a estos principios generales. En estos preceptos constitucionales, se fundamenta la necesidad de que exista una ley que se pueda aplicar en materia de *delitos informáticos,* ya que si bien es cierto, como lo he comentado, los sistemas informáticos pueden se utilizados solo como una herramienta o medio para cometer delitos de los existentes actualmente en nuestra legislación penal, también lo es que muchas otras actividades ilícitas en esta materia, ya se encuentran fuera del marco legal, por lo cual insisto que nos encontramos ante una situación de impunidad en tratándose de delitos informáticos.

4.4 Necesidad legal de los delitos informáticos

En la actualidad, la informatización se ha implantado en casi todos los países, tanto en la organización y administración de empresas tanto públicas como privadas, en la investigación científica, en la producción industrial, en el estudio o bien el simple esparcimiento, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, lo cuales es justamente el objeto de estudio de este trabajo, es decir la *criminalidad informática.*

El espectacular desarrollo de la tecnología informática, ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o base de datos, y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, mediante los cuales, es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales, haciendo análisis comparativo entre los delitos comunes, con los nuevos delitos informáticos, nos damos cuenta de que la cuantía de los perjuicios ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, además de que también existen posibilidades mucho más elevadas de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o bien, el medio para cometer otros delitos. La informática reúne características que la convierten en un medio idóneo para la comisión de diversas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su necesidad en la producción de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material

de los objetos destruidos. A ello se une, que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores, una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Ahora bien, la legislación sobre protección de los sistemas informáticos, ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación, sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Otra razón por la cual es imprescindible la legislación en materia de Delitos Informáticos, lo es, que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas tanto físicas como morales, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, de identificación de las personas etc. y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que nuestra misma Constitución protege.

El problema fundamental en esta materia, no lo es la amenaza potencial de la computadora sobre el individuo, esto no es lo que debe provocar preocupación a los

legisladores, sino la utilización real por el hombre de los sistemas de información con fines de delictivos.

De igual manera, no son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen y los infringen con fines delictivos.

La humanidad no esta frente al peligro de la informática, sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder, que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas y su patrimonio. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos, puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas para combatir en contra de la cyberdelincuencia.

Es por ello que, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos

4.6 Efectos de la inexistencia de la legislatura informática

La inexistencia de una ley informática, imposibilita que la persecución y castigo de los autores de delitos informáticos sea efectiva. Aunado a esto, el órgano encargado de perseguir los delitos, no poseen el nivel de experiencia requerida en estas áreas, ni la capacidad tecnológica para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas, es por ellos que si logramos una legislación basta para la persecución de los delitos informáticos, a la par, lograremos impulsar el desarrollo tecnológico tanto del equipo como del personal para hacer efectivo el cumplimiento de la ley.

4.7 Características de los Delitos Informáticos

Según el mexicano Julio Téllez Valdez[37], en su obra "Derecho Informático", considera que los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

---

[37] **TELLEZ Valdez** Julio; "Derecho Informático"; México; Mc Graw Hill; 2a. edición; 1996; Páginas 103-104

- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos no sancionados por nuestra ley penal.

CAPÍTULO QUINTO

DELINCUENCIA CYBERESPACIAL: Aspectos criminológicos del sujeto activo del delito informático

Las personas que cometen este tipo de delitos, son generalmente aquellas que tienen habilidades para el manejo de sistemas informáticos, y que, gracias a su situación laboral, los sitúa en lugares estratégicos donde se maneja información de carácter prioritario, o bien, son hábiles en el uso de los sistemas, aún cuando en muchos de los casos, no desempeñen labores que faciliten el cometer este tipo de delitos.

Los autores de este tipo de conductas antisociales son muy distintos uno de otros, por lo que la única manera de distinguirlos es gracias a la naturaleza de los delitos que cometen. Gracias a la forma de operar de estas personas los expertos criminólogos, como el norteamericano Edwin Sutherland[38] introductor del término *White collar crime* (crímenes de cuello blanco), han identificado que este tipo de delitos son los que más daños económicos ocasionan. Existen diversos tipos de delincuentes informáticos entre los cuales destacan: *Hackers, Crackers, Phreakers*, entre otros sin embargo yo me daré a la tarea solamente de describir aquellos que se dedican solo al crimen a través de medios informáticos, mismos que a continuación describiré.

---

[38] **Bierce William;** *Op. Cit.* página 20

5.1 Hackers como sujetos activos de los delitos informáticos

El término *Hacker,* puede ser entendido hoy en día como sinónimo de delincuente informático para algunos, y genios de las Tecnologías Informáticas para otros, retrocediendo un poco en el tiempo, se les llamaba así a los "técnicos de telefonía por la forma en que solían reparar los teléfonos, con un golpe seco ponían de nuevo en marcha el teléfono y de pronto este modo de operar ostentó el título de *hack*"[39], que traducido literalmente del inglés al español, significa hachazo, y que a su vez resumía el arreglo del aparato tras un golpe certero. Así a los técnicos que empleaban esta técnica se les comenzó a llamar *Hackers.*

Hacker, es un concepto muy utilizado en el ciberespacio, ya que se trata de personas que por simple curiosidad, se introduce por a cualquier sistema informático que sea de su interés, hasta llegar a comprender el funcionamiento de cualquiera de estos sistema mejor que quienes lo inventaron. Toma su actividad como un reto intelectual, no pretende producir daños. *Hacker* es una persona que tiene la inteligencia y la capacidad para entrar a cualquier sistema computacional sin estar autorizado. Existen opiniones encontradas respecto a que si un *Hacker* es un delincuente informático o no lo es, ahora bien de la definición que acabo de proporcionar se desprende que un *Hacker* tiene como único objetivo el aprendizaje, entonces, ¿estaremos ante la presencia de un delincuente informático o no?.

---

[39] **http://inicia.es/de/pazenred/ciber.htm;** Responsable de la página Paz M. de la Cuesta Aguado; Fecha de consulta 13 de abril del 2002

Si partimos del punto en que, la intromisión no autorizada a un sistema (aunque sólo sea eso) ya es delito, entonces se deduce que un *hacker* si es un delincuente informático ya que, aunque su intención sea únicamente curiosear, las consecuencias de los métodos que utilicen, por ejemplo el empleo de troyanos[40], hacen que deriven importantes consecuencias económicas, ya que el administrador del sistema que descubra este tipo de actividades, desconoce las intenciones reales del intruso, y suelen ser importantes los perjuicios ocasionados en tiempo y recursos empleados para limpiar el sistema.

Sin embargo, los mismos *Hackers*, defienden la actividad que ellos desarrollan, justificándose en que, éste no puede ser considerado antiético, ya que ellos buscan la verdad y no el conformismo como el resto de las personas. El *hacker* lucha por una red libre, que no tenga dueños, que todos tengan acceso a la información, pero que la información clasificada esté bien protegida. En este sentido el *hacker*, le hace un favor a la sociedad violando sistemas informáticos porque si lo hiciese un espía o enemigo podría causar graves perjuicios.

Por lo anterior, yo considero que los *Hackers* representan una amenaza para el mundo de la tecnología de la información, por que su actividad los pone en el punto divisorio del bien o el mal, por un lado sus conocimientos aportan muchos beneficios para la sociedad entera, incluso, con los conocimientos que tienen podrían colaborar con las autoridades en la persecución de los delitos informáticos, detectando a

---

[40] **Troyano**, proviene de caballo de Troya, es un programa, cuya función es la de un vigilante, dentro de los sistemas de cómputo, su peligrosidad es debido a que no se sabe con que intención se introducen a dicho sistema.

quienes sí abusan de sus conocimientos para cometer delitos, pero desde otro punto de vista, su facilidad para introducirse en cualquier sistema de alta seguridad, así coma la facilidad de descifrar códigos etc. también los pone ante la inminente tentación de perpetrar ellos mismo dichos delitos.

5.2 Crackers como sujetos activos de los delitos informáticos

Realmente es a esta clase de personaje al que si nos podemos referir como delincuente informático. Presenta principalmente dos vertientes:

- El que se cuela en un sistema informático y roba información o produce destrozos en el mismo.
- El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware, para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anti-copia.

Esto quiere decir que los crackers son plenamente unos delincuentes activos, contra los cuales va encaminado este trabajo de investigación, ya que si no fuera por personas como estas, no existiría la necesidad de legislar en materia de *delitos informáticos*.

Los *Crackers*, son *hackers* pero con intenciones que van más allá de experimentar con la intromisión en un sistema informático, ellos se dedican única y exclusivamente a ingresar a un sistema e intentar destruirlo, para luego mostrar al mundo como lo

hicieron, publicando usualmente la metodología que emplearon, y poniendo esa información en servidores públicos.

Son más peligrosos que los *Hackers*, puesto que estos últimos, son idealistas cuyo único objetivo es entrar a un sistema sin autorización, en cambio el *Cracker* destruye, e inutiliza un sistema, con las desastrosas consecuencias que ello apareja.

5.3 Conductas antisociales informáticas cometidas en Internet

Para el análisis de este capitulo es necesario que nos remitamos al Capitulo 4 del presente trabajo de investigación, en el cual, analizamos la definición de Delitos Informáticos, de lo cual retomo que se trata de *toda acción u omisión, realizada en el entorno informático, que cause un perjuicio a otro, existiendo o no ánimo de lucro, o bien, que por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique a la víctima, tipificado por La Ley, y sancionado con una pena.* Ahora bien con este concepto, nos avocaremos al análisis de las conductas informáticas, que pueden ser consideradas como *delitos informáticos.*

5.4 Clasificación de los delitos informáticos

Desde siempre los delitos han sido clasificados dependiendo de su gravedad y las condiciones en que se cometen, por esta razón los delitos derivados del uso de la tecnología también se ven sujetos a una clasificación, con la finalidad de que puedan ser evaluados y sancionados adecuadamente.

Como les mostraré a continuación, los delitos informáticos han sido objeto de variadísimas clasificaciones, sin embargo, en su mayoría, los conceptos fundamentales que han servido de base para llevara acabo dichas clasificaciones son las siguientes:

- El perjuicio causado
- El papel que el computador desempeñe en la realización del mismo
- El modo de actuar
- El tipo penal en que se encuadren
- Clase de actividad que implique según los datos involucrados.

Para el Maestro Diego Castro Fernández clasifica a los delitos informáticos en 2 de acuerdo a los elementos que se utilizan para llevara a cabo este tipo de delitos:

1. La Acción, tanto la que afecta a los componentes de la computadora (hardware y software), como medio o instrumento para perpetrar el delito, y

2. La consumación de un acto ilícito, autónomo como es el uso indebido y sin autorización de una computadora.

El Lic. Julio Téllez clasifica a los delitos informáticos basándose en dos criterios:

1. Como instrumento o Medio. Donde se tienen a las conductas a criminales que se valen de las computadoras como método, medio o símbolo en la realización del ilícito.

2. Como fin y objetivo, en el cual las conductas criminales van en contra de la computadora, accesorios o programas como entidades físicas.

La Lic. María de la Luz Lima, hace alusión a los delitos electrónicos, así denomina ella a los delitos informáticos, y los divide en las siguientes categorías:

1. Delitos que usan a la tecnología electrónica como método, las conductas criminales utilizan medios electrónicos para llegar a un resultado ilícito.
2. Delitos electrónicos que usan la tecnología electrónica como medio, las conductas criminales utilizan la computadora como medio o símbolo para cometer el delito.
3. Delitos que usan la tecnología electrónica como un fin, las conductas criminales emprenden acciones en contra de la entidad física del objeto, maquina electrónica o su material con objeto de dañarla.

5.5 Delitos Informáticos reconocidos internacionalmente.

Estos son algunos de los delitos informáticos, que la ONU, ha reconocido, como tales, y que han sido adoptados por la legislación penal de diversos países de Europa y Sudamérica

5.5.1 Hacking

La actividad de *hachear* un sistema, puede tener diferentes finalidades y alcances. Así en la mayoría de los casos el romper el sistema o eliminar los pasos de seguridad de un sistema tiene por objeto ver, fisgonear el contenido y la información

protegida, otras veces extraer copias de la información y muy raramente destruir o cambiar los contenidos de la información.

Lo que caracteriza las actuar de estos sujetos es su entrada ilegal al sistema, entendiendo el concepto de entrada ilegal como la entrada de toda aquella persona que no tiene los password o no los ha conseguido por los caminos normales.

5.5.2 Hacking y Cracking desde el punto de vista legal

La detección de un *hacker* es bastante difícil. De hecho a no ser que esa persona quiera ser identificada, es difícil llegar hasta ella. Es por ello, que para las autoridades de los países en los que estas conductas ya son consideradas como delitos informáticos, es casi imposible perseguir estos delitos, requiere de la implementación de alta tecnología y de la capacitación de su personal incluso recurren a los *hackers*, para la investigación de este tipo de delitos. La problemática se extiende o se hace mayor, ya que en cada país la legislación es diferente o incluso inexistente, como el caso de nuestro país. Un ejemplo que podemos tomar en cuenta es el sonado caso de Microsoft, ya que si este problema de hacking se hubiera suscitado en España, éste no se hubiera considerado delito, ya que la ley española exige que se haga con ánimo de lucro, es decir, que reporte beneficio económico, elemento que en caso Microsoft no se dio.

5.5.3 Fraudes cometidos mediante la manipulación de computadoras

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos, o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de acuerdo a la forma de trabajo de un sistema informático.

En un primer término tenemos la figura del *Input, "Input* es la actividad por medio de la cual es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador"[41], esta actividad es una verdadera manipulación de las computadoras.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja la computadora. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema, programas especiales que introduce el autor.

A diferencia de las manipulaciones del *input* que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales, actividad principal de los crackers, el modificar o incluso destruir un sistema.

---

[41] **http://inicia.es/de/pazenred/ciber.htm**; ***Ibidem.***

Por último, es importante señalar que otra forma de llevar a cabo la manipulación de computadoras lo es el *Output "Output* hace posible la falsificación de un resultado que inicialmente es correcto, obtenido por una computadora"[42] Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo lo que en nuestra legislación conocemos como el delitos continuado. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de "manipulación del programa", la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

Me parece oportuno transcribir un ejemplo para que todo lo que acabo de explicar pueda ser comprendido en el ámbito jurídico y porque es necesaria y urgente la legislación al respecto.

El investigador Alemán Urich Sieber cita como ejemplo el siguiente caso, mismo que fue tomado de la jurisprudencia alemana:

"El autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía

---

[42] ***Ibidem.***

a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor"[43].

Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los empleados ficticios y los pagos realizados, no aparecieran en los listados de control.

En este ejemplo podemos ver como afectan las manipulaciones en un programa de computo, en este caso en particular el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal.

5.5.4 Manipulación de programas

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de

[43] **SIEBER, Urich;** *op. cit.;* **página 128.**

computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

5.5.5 Manipulación de datos de entrada

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

5.5.6 Manipulación de datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

5.5.7 Falsificaciones informáticas

Las falsificaciones llevadas a cabo a través de los medios electrónicos los podemos clasificar desde dos puntos de vista:

5.5.7.1 Como objeto

Como Objeto, cuando se alteran datos de los documentos almacenados en forma computarizada. Es decir en este caso, los cyberdelincuentes, se introducen en sistemas informáticos, para alterar información ya existente, generalmente con la finalidad de falsear información confidencial, podría señalar como un simple ejemplo, la introducción de un cracker a un sistema bancario y alterara los estados de cuenta de alguna persona para que ésta pueda obtener algún crédito etc.

5.5.7.1 Como instrumento

Como instrumento, las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

5.5.8 Sabotaje informático. Daños o modificaciones de programas o datos computarizados.

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Encontramos que el sabotaje informático es "el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema"[44]. Es importante señalar que existen dos formas en las que opera el sabotaje informático:

1. Conductas dirigidas a causar daños físicos.-

Este primer grupo, comprende todo tipo de conductas destinadas a la destrucción física del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas

[44] **http://www.informaticamilenium.com.mx;** Responsable de la página Julio García; fecha de consulta 15 de agosto del 2002

conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño, conductas que no son materia del presente trabajo ya que pueden encuadrarse típicamente en los preceptos penales ya existentes.

2. Conductas dirigidas a causar daños lógicos

Este segundo grupo, está más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos lógicos, esto quiere decir que, son todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático. Este tipo de daño a un sistema, se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (*crash programs*), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

A este segundo grupo es al que pertenecen todas aquellas técnicas, que permiten cometer sabotajes informáticos las cuales son: Virus, gusanos, Bombas lógicas o también conocidas como Bomba cronológica, reproducción no autorizada de programas informáticos de protección legal etc. Algunos de ellos los explicaré a continuación.

5.5.9 Virus

El virus informático, es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado, así como también en todos los datos y programas contenidos en los distintos discos con los que toma contacto, a través de una conexión. "Los virus son una serie de claves programáticas, que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos"[45]. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada.

De lo anterior puedo explicar en otras palabras qué, se entenderá por virus a aquél programa, que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa, se instala, se reproduce y causa daño. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, como el caso del *ping-pong* (mismo que a continuación conceptualizaré), pero también existen aquellos que pueden llegar a eliminar el contenido de una base de datos.

En estados Unidos, se publicó un artículo, elaborado por el investigador William. Bierce, llamado "El delito de violencia tecnológica en la legislación de nueva York" de la revista Derecho de la Alta Tecnología, nos hace alusión de los virus más conocidos que han aparecido en los últimos tiempos, explica la diversidad de virus y su peligrosidad de la siguiente forma:

---

[45] **http://inicia.es/de/pazenred/ciber.htm**; ***loc. Cit.***

- Virus del ping-pong: consiste en un punto que se mueve por toda la pantalla y parece rebotar en los bordes.
- Datacrime o virus del viernes 13: el virus Jerusalén estaba destinado para destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988.
- Michelangelo: este último de fama más reciente.

Actualmente existe una gran competencia entre aquellos que crean los virus y los que desarrollan los antivirus. Hasta ha llegado a decirse que los virus son desarrollados por los mismos productores de antivirus, ya que hoy en día es fundamental adquirir antivirus y los mismos deben ser renovados constantemente, por supuesto que no existe ninguna prueba concreta, aunque después de estudiar todo lo que hemos estudiado hasta este punto dl trabajo, ésta, no sería una idea descabellada.

5.5.10 Gusanos

Se fabrica de forma análoga al virus, se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se

destruirá, lo que en el derecho penal tradicional conocemos como el delito continuado, este generalmente se utiliza para lleva a cabo los fraudes llevados a cabo mediante la manipulación de computadoras.

5.5.11 Bomba Lógica o Cronológica

En esta modalidad también conocidas como *Time Bombs*, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

Un claro ejemplo lo encontramos en un artículo publicado en Internet, en el cual se dice que la Jurisprudencia Francesa registró un caso muy particular en el que "un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa"[46]

Este tipo de técnicas, requiere conocimientos especializados ya que es necesaria la programación de la destrucción o modificación de datos, en un momento dado del

---

[46] **www.bufetalmeida.com/index.htm;** Responsable de la Página Gustavo A. De Cara Correa; fecha de consulta 20 de agosto del 2002

futuro. Ahora bien, al diferencia de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba, la cual desencadena la comisión de otros delitos, es decir lo que en el capitulo 4, cundo hablamos del Dolo indirecto.

5.5.12 Acceso no autorizado a servicios y sistemas no autorizados

Puede darse por motivos diferentes: desde la simple curiosidad, como en el caso de muchos piratas informáticos es decir los *Hackers*, hasta el sabotaje o espionaje informático es decir la actividad desarrollada por los crackers. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. Podríamos llegar hasta actos de atentados terroristas, por ejemplo en el caso de intervenir sistemas de tráfico aéreo. Es por ellos que países como Estados Unidos se han dado a la tarea de legislar lo más ampliamente posible en materia de este tipo de delitos, tal como lo analizamos en el capitulo Primero de esta investigación.

CAPÍTULO SEXTO

OBSTÁCULOS QUE SE PRESENTAN PARA LA PERSECUCIÓN DE DELITOS INFORMÁTICOS.

Es importante reconocer que, legislar en materia de Delitos informáticos, no es una tarea fácil, ya que los legisladores que han realizado propuestas en esta materia, al llevar a cabo esta tarea se enfrentan con diversas problemáticas, a las cuales aparentemente no encontramos una solución que sea eficaz, sobre todo, cuando el problema de los *delitos informáticos*, se elevan a la escena internacional, por que se magnifican los inconvenientes y las insuficiencias, debido a que los *delitos informáticos* constituyen una nueva forma de crimen transnacional y su combate, requiere de una eficaz cooperación internacional concertada.

A continuación realizaré una síntesis de los posibles problemas, con los cuales nos enfrentamos en el área de los *delitos informáticos*:

- Falta de acuerdos globales acerca del tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Destrucción u ocultación de pruebas, en la comisión de delitos informáticos, dada la importancia de este obstáculo, lo explicaré en el apartado siguiente.

- Falta de especialización de los organismos encargados de la persecución de los delitos y así como del órgano judicial en el campo de los *delitos informáticos.*

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

- Existencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados ineficaces, que permitan la actividad de organismos de cooperación internacional.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de sistemas informáticos y la interconexión de la computadora a una red, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, incluso en países como el nuestro en el desarrollo esta muy por debajo de ser comparado con países de primer mundo, nos pone también, ante la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto tanto para los legisladores de nuestro país, como, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

6.1 Problema de la Prueba en materia de los delitos informáticos

Uno de los mayores obstáculos que se encuentran en la persecución de los *delitos informáticos,* es el hecho de que los delincuentes pueden destruir fácilmente las pruebas, ya sea cambiándolas, borrándolas o trasladándolas. Si el órgano en

cargado de la persecución del delito, opera con más lentitud y la capacidad del personal que los integran no es lo suficientemente elevada como la de los delincuentes, se pierde gran parte de las pruebas; o puede ser que los datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

Tal vez la "criptografía"[47], estorbe en las investigaciones penales, pero los derechos humanos podrían ser vulnerados, si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Diversas empresas electrónicas, sostienen que, el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en bases de datos.

6.2 Policía de red en México

En un articulo publicado en el periódico el financiero, se comunica, que la Secretaria de Gobernación, se esta planteando la posibilidad de crear un nuevo tipo de cuerpo policiaco, la función de está nueva policía, será la de detectar a *hackers* que pirateen los sistemas informáticos del gobierno, empresas y particulares.

En la actualidad, podríamos tener la certeza de que algunos sistemas informáticos, bases de datos, han sido vulneradas, así como también, algunas páginas en Internet

---

[47] **Criptología** Se entiende por *criptología*, el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.

de dependencias federales y estatales, han sido *hackeadas* y dañadas, incluso se han encontrado indicios, de que *hackers* o *cackers,* han tratado de penetrar algunos sistemas financieros del país.

"Esta nueva Policía, estará a cargo de la Policía Federal Preventiva (PFP) y su objetivo será detectar delincuentes de Internet en menos de 15 minutos"[48].

Los recursos son escasos, el personal todavía lo están seleccionado y el equipo técnico no ha quedado totalmente instalado", apuntó el diario. Los delitos a combatir son el robo de tarjetas de crédito y de información oficial, los donativos a grupos terroristas la pornografía, la piratería de música y la falsificación de documentos.

6.3 Posibles tipos penales, en materia de delitos informáticos

Antes que proponer específicamente que tipos penales deben incluirse en nuestro Código penal federal, considero de gran importancia, establecer un criterio del cual debemos partir para llevar a cabo esta tipificación de conductas.

Existen diversidad de opiniones respecto a la necesidad o no de legislar en materia de *delitos informáticos*, ya que consideran que éstos, no existen, estas opiniones argumenta en que éstos delitos informáticos, no son más que delitos *tradicionales,* que en lo único que se pueden diferenciar, de otro delito cualquiera, son en las herramientas empleadas o en los objetos sobre los que se producen, y considero que en parte si tienen razón, cuando se habla del empleo de sistemas informáticos para

---

[48] **Ruiz Sánchez** Pablo; "México pone en marcha su policía de la red"; México. D.F; El financiero; sección política; 3 de Agosto del 2002; Año XXII; número 6152; página 27

la comisión de u delito, es decir cuando, la tecnología informática se utiliza solo como un medio o instrumento para perpetrar el delito.

Sin embargo, creo que ésta es una visión demasiado limitada de la realidad ya que existen muchos otros delitos que difícilmente podemos tipificar en nuestra legislación actual, mismas que tendrán que adaptarse rápidamente o bien, redactarse acorde a los nuevos tiempos, que impone el uso de las tecnologías de la información. Partiendo de este punto de vista vemos que en ocasiones habrá necesidad de crear un nuevo tipo penal, y otros casos, solo será necesario aumentar la pena en tratándose de delitos ya tipificados, que se lleven a cabo a través de medios electrónicos o informáticos.

A continuación, procederé a describir diversas conductas antisociales informáticas, a manera de tipo penal, como desde mi punto de vista deberían considerarse en nuestro Código penal Federal.

6.3.1 Acceso indebido a programas o sistemas de cómputo.

Comete este delito, el que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información.

6.3.2 Sabotaje o daño a sistemas.

Comete este delito, el que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

Considero que la pena debe ser mayor cuando los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

6.3.3 Acceso indebido o sabotaje a sistemas protegidos.

En relación con este delito considero pertinente que la pena se aumente cuando los efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas, instituciones financieras o que contenga información personal o patrimonial de personas ya sean físicas o morales.

6.3.4 Posesión de equipos o prestación de servicios de sabotaje.

Comete este delito, el que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe,

fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines.

6.3.5 Espionaje informático.

Comete este delito, el que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes.

Considerando en este caso también, que la pena se aumente, cuando este delito se cometa con el fin de obtener algún tipo de beneficio para sí o para otro, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones objeto del espionaje, o bien que resultare algún daño para las personas físicas o morales, como consecuencia de la revelación de las informaciones de carácter reservado.

6.3.6 Violación de la privacidad de la data o información de carácter personal.

Comete este delito, el que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información.

6.3.7 Violación de la privacidad de las comunicaciones.

Comete este delito, el que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena.

6.3.8 Revelación indebida de data o información de carácter personal.

Comete este delito, el que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos.

Considerando la posibilidad de que la pena se aumente siempre y cuando la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro.

6.3.9 Difusión o exhibición de material pornográfico.

Comete este delito, el que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas,

6.3.10 Exhibición pornográfica de niños o adolescentes.

Comete este delito, el que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos.

6.3.11 Apropiación de propiedad intelectual.

Comete este delito, el que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.

CONCLUSIONES.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legal, es difícil la clasificación de éstos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática, la tecnología es tan cambiante que el derecho debe actuar al mismo paso en que va avanzando la tecnología informática.

La falta de cultura informática es un factor crítico en el impacto de los *delitos informáticos* en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual debe ser aplicar.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

La inexistencia de grupos especializados para la persecución de delitos *informáticos* impide la solución al impacto de los delitos es por ellos que la creación de este tipo de órganos de control informático, resultaría benéfico para la eficacia de una legislación informática, de tal forma que estos órganos se encarguen de la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones y a los particulares en general, a minimizar las amenazas que presentan los delitos informáticos.

Para concluir con esta investigación, de un tema tan novedoso, actual y de gran interés para el mundo jurídico, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, mismos que garanticen la eficacia de su aplicación, de igual manera, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Desde hace algunos años los las conductas antisociales informáticas, han comenzado a ser una verdadera amenaza para los sistemas informáticos, y para la sociedad entera, causando perdidas millonarias en las empresas todos los años, es

por eso, se hace necesaria una respuesta jurídica determinante ante tal severa amenaza.

Como he comentado, es necesario armonizar las legislaciones de los distintos países, ya que los efectos transfonterizos de los virus, hace que en ocasiones los culpables queden impunes ante las débiles legislaciones que los cobijan.

Por todo lo anterior y después de haber realizado un análisis comparativo entre diversos países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, considero necesario, a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en otros países, que México logre una legislación basta y eficaz regule penalmente las conductas ilícitas derivadas del uso de la computadora.

En primer término, considero que la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización, sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, consideramos que es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia

de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que en nuestro país, el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, considero necesario que con la finalidad de no provocar un conflicto de competencia entre los congresos locales y el de la Unión, el Congreso de la Unión, fundamentándose en las facultades que nuestra carta magna le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

En este mismo sentido, y aunque nuestra investigación es única y exclusivamente desde el punto de vista legal, considero importante que tratando se de la ciencia del derecho, no nos podemos deshumanizar ante la presencia de este tipo de actividades delictivas, ya que pienso, que esta problemática tal vez no sea únicamente y exclusivamente un problema legal, sino también un problema social, moral y tecnológico. La ley sola no nos podrá salvar del futuro virus, pero si actúa a la vez con una norma social ampliamente aceptada y escudo tecnológicos. El camino

es difícil, más sin embargo no imposible, los tiempos cambian y las leyes deben cambiar también, es labor de nuestros legisladores mantenerlas a la vanguardia.

Los delitos que se pueden cometer en la actualidad mediante el uso de la tecnología son múltiples y de tipos muy variados, nadie puede estar seguro de que uno no va a ser víctima de alguno de ellos y por lo anterior considero que tanto nosotros las personas que estamos sumergidos en los medios informáticos junto con los legisladores, ocuparnos de la creación de un instrumento confiable que nos permita identificar y sancionar de una manera correcta los delitos que con el uso de la tecnología se puedan presentar. Pese a la desregulación de que adolece la red, muchas de las eventuales conductas lesivas pueden considerarse tipificadas en delitos tradicionales, no obstante, es precisa una intervención de las autoridades para que se proporcione una pena a los cyberdelincuentes e impidan que se sigan causando este tipo de abusos.

Es una obligación del estado, adaptar su derecho penal, es decir leyes, penas y procedimientos a la nueva realidad tecnológica.

BIBLIOGRAFÍA

LIBROS

1. **AMUCHATEGUI REQUENA Irma;** "Derecho Penal"; México D.F; Harla; 1993

2. **BIERCE, William**; "El delito de violencia tecnológica en la legislación de nueva York"; Derecho de la Alta Tecnología; Febrero 1994; Revista bimestral; No. 66; Estados Unidos

3. **CALVO Nicolau Enrique y Montes Suárez Eliseo;** "Tratados Internacionales en materia Tributaria"; México D.F; Themis; segunda Edición; 1998

4. **CASTELLANOS Fernando;** "Lineamientos elementales de Derecho Penal"; trigésima sexta edición; México D.F; Porrúa; 1996

5. **GRIMES Brad;** "Nuevos equipos para la seguridad pública";_ PC Computing 1998; Revista mensua; Editorial Palsa; número 43; México

6. **JIMÉNEZ DE ASÚA** Luis; "La ley y el Delito"; principios del derecho penal; 10° edición; Buenos Aires Argentina; 1980

7. **MOLINA García** Pablo; "Informática y Derecho Penal, en Implicaciones socio-jurídicas de las tecnologías de la información"; Madrid España; Editorial Citema; 1984

8. **SIEBER, Urich;** "Criminología Cibernética"; Manchen Deutschland; Mc. Graw Hill; México;1995

9. TELLEZ Valdez Julio; "Derecho Informático"; México; Mc Graw Hill; 2a. edición; 1996

10. ZAMORA SÁNCHEZ Pedro; *"Marco Jurídico del Lavado de Dinero";* México; Oxford University prees México; 1999

LEYES

11. Código Penal para el Estado de Sinaloa; México D.F; Editorial Delma 2001

12. Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de fuero Federal; México D.F; Editorial Delma; página 143; 2000

13. Constitución Política de los Estados Unidos Mexicanos; Editorial Alco; año 2000

14. Ley Federal de Derechos de Autor; Editorial Delma; sexta edición 2002

PÁGINAS DE INTERNET

15. http://www.buesa.net/enlaces/hacking.html; Responsable de la Página Carlos Busón Buesa; fecha de consulta 21 de Septiembre de 2002.

16. http://info4.juridicas.unam.mx/ijure/fed/8/; Responsable de la Página UNAM, fecha de consulta 18 de mayo 2002.

17. http://www.informaticamilenium.com.mx; Responsable de la página Jorge Marcelo Torres Lipe; fecha de consulta 13 de Abril del 2002.

18. http://inicia.es/de/pazenred/ciber.htm; Responsable de la página Paz M. de la Cuesta Aguado; Fecha de consulta 13 de abril del 2002

19. http://www.informaticamilenium.com.mx; Responsable de la página Julio García; fecha de consulta 15 de agosto del 2002

20. www.bufetalmeida.com/index.htm; Responsable de la Página Gustavo A. De Cara Correa; fecha de consulta 20 de agosto del 2002

PERIÓDICOS

21. **Ruiz Sánchez** Pablo; "México pone en marcha su policía de la red";El financiero; sección política; 3 de Agosto del 2002; Año XXII; número 6152; México. D.F