UNIVERSIDAD
DON VASCO, A.C.

Escuela de Derecho
UNIVERSIDAD DON VASCO, A. C.

UNIVERSIDAD DON VASCO, A.C.

INCORPORACIÓN No. 8727-09 A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA DE DERECHO

"EL DERECHO INFORMÁTICO COMO INSTRUMENTO JURÍDICO PARA ADICIONAR UNA FRACCIÓN AL ARTÍCULO 387 DEL CÓDIGO PENAL FEDERAL REFERENTE AL FRAUDE INFORMÁTICO"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

PRESENTA:

FRANCISCO JAVIER SÁNCHEZ TORRES.

URUAPAN, MICHOACÁN, MARZO DE 2005.

SUBDIRECCIÓN DE CERTIFICACIÓN

ANEXO 45
FORMA PT01-A

UNIVERSIDAD
DON VASCO, A.C.

IMPRESIÓN DE TESIS INDIVIDUAL

C. DIRECTORA GENERAL DE INCORPORACIÓN
Y REVALIDACIÓN DE ESTUDIOS, U.N.A.M.
P R E S E N T E :

SÁNCHEZ	**TORRES**	**FRANCISCO JAVIER**
APELLIDO PATERNO	APELLIDO MATERNO	NOMBRE(S)

NÚMERO DE EXPEDIENTE: 946602205-8

ALUMNO DE LA CARRERA DE: LICENCIADO EN DERECHO

CUMPLE CON LA REVISIÓN DE LA TESIS TITULADA:

"EL DERECHO INFORMÁTICO COMO INSTRUMENTO JURÍDICO PARA ADICIONAR UNA FRACCIÓN AL ARTÍCULO 387 DEL CÓDIGO PENAL FEDERAL REFERENTE AL FRAUDE INFORMÁTICO"

POR LO QUE SE AUTORIZA LA IMPRESIÓN DE LA MISMA.

URUAPAN, MICHOACÁN, MARZO 18 DE 2005.

FRANCISCO JAVIER SÁNCHEZ TORRES

V° B°

LIC. ANGEL HORACIO BÁEZ MENDOZA
ASESOR DE LA TESIS

LIC. FEDERICO JIMÉNEZ TEJERO
DIRECTOR TÉCNICO

AGRADECIMIENTOS

Agradezco A Dios que siempre me escucha y me ayuda en cada día de mi vida, especialmente en los momentos de angustia y desesperación.

A mi madre, por darme todo el amor, confianza y apoyo a lo largo de mi vida, ya que sin su trabajo arduo y cansado, el logro de esta meta hubiera sido difícil para mí.

A él Licenciado Horacio, mi asesor y amigo, por la ayuda incondicional que me ha brindado a lo largo de la realización de la presente tesis, así como cuando este fue mi profesor de clase y que debido a su profesionalismo he logrado una buena formación universitaria.

A mis hermanos Jessica, Miguel e Israel que de manera especial confiaron en mí.

A Lilia, mi esposa, porque ha estado conmigo en los momentos buenos y malos de mi vida, así como por su apoyo incondicional.

A mi hijo por ser la motivación mas grande que he obtenido en esta vida, y que gracias a el mis deseos de superarme son cada día mas grande.

INDICE

INTRODUCCIÓN.

Hoy en día es bien sabido por todo el mundo que la informática esta abarcando gran parte de nuestra vida cotidiana, además de facilitar el acceso a la información a todo el mundo, nos permite realizar una gran cantidad de actividades de una manera mas sencilla, ya que algo que antes era mas complicado realizar ahora basta con buscar en la INTERNET, para encontrar lo que se necesita ya sea desde una simple información hasta la posibilidad de realizar compras, ventas, transacciones, etcétera. Por otra parte la informática no solo es instrumento de los programadores o ingenieros informáticos, lo es del mismo abogado, solo que aun no es utilizado por la mayoría de los licenciados en Derecho, mas sin embargo la informática hoy en día es contemplada por el derecho, luego entonces el derecho informático nos permite entender conductas afines a la materia abarcando desde un contrato informático, así como los riesgos del mismo y la posibilidad de poder llegar a cometerse conductas ilícitas por alguna de las partes.

Por otra parte como lo define el Dr. Julio Téllez Valdez el Derecho Informático es "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".

Es entonces con esta definición cuando se comprende qué tanto es lo que abarca tal materia de referencia. Es necesario hacerse una pregunta ¿Realmente el Licenciado en Derecho esta conciente de que tiene acceso a tal cantidad de información hoy en día y que esta sucediendo un fenómeno del cual deberá legislarse al respecto? Existe gran falta de doctrina al respecto así como

legislación en la materia, ya que como es algo nuevo y que realmente esto se origina a raíz de los avances tecnológicos y al ser un país tercermundista debemos entender que la tecnología nos tarda en llegar a la gran mayoría de los ciudadanos mexicanos, luego entonces, es una razón de nuestro atraso tecnológico. Países como Argentina, Perú, España, Estados Unidos y otros más ya tomaron cartas en el asunto debido al gran movimiento que se esta dando en tal área. Entonces el licenciado en Derecho debe de preocuparse por tener más conocimiento y si no dominar tal rama por lo menos tener conciencia de que tal instrumento esta a nuestro alcance y nos puede facilitar gran cantidad de trabajos, tales como consultas al diario oficial de la federación, leyes federales, estatales, códigos, tratados internacionales y muchas cosas más. Por tal motivo es prudente y necesario que el Licenciado en Derecho se preocupe por conocer de tal rama que esta comenzando a dominar gran cantidad de actividades de la vida cotidiana del ciudadano ordinario, en consecuencia se debe tener conciencia de que tal acoplamiento de la tecnología de punta y la informática traerá como consecuencia cambios en nuestras legislaciones, debido a que como se ha hecho hincapié anteriormente esto es una actividad cotidiana de las personas, sin tener un limite de edad para hacer uso de esta, ya que desde menores de edad tanto como adultos hacen uso de esta tecnología.

Hoy en día difícilmente algún individuo no ha escuchado hablar de un tipo de Software, de la INTERNET, de las computadoras de escritorio, de las computadoras personales, las PALM e incluso los correo electrónicos, ya que por medio de estos logramos tener acceso a un sin numero de información. Ahora

bien, sí es un problema que el Licenciado en Derecho, no conozca el Derecho Informático, será aun mas problemático el hecho de que no sepa como se podrían cometer conductas ilícitas por medios informáticos, como lo es el Fraude Informático, es pues, de suma importancia que nos preocupemos por conocer de tal polémica ya que siempre se tendrá el concepto de que el Licenciado en Derecho es una persona basta en conocimientos y por supuesto conocedor de su campo de acción.

El desarrollo de toda esta infraestructura en las comunicaciones, informaciones y negocios, que cada día más vemos identificada en las actividades políticas, culturales y comerciales de México, han mostrado un amplio crecimiento y desarrollo de todas las áreas del quehacer nacional, fenómeno mundial que ha ocasionando que el área dedicada a la informática y la computación ganan cada día más un espacio. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para cometer y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para 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 hace enfrentar situaciones que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para sí y en perjuicio de otros, nuevas técnicas de criminalidad para el cometido de sus acciones perturbadoras. Estas acciones perturbadoras de la convivencia social han nacido

al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito mundial, se ha generado una percepción de la seguridad informática, percepción que se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados delitos informáticos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos de control social formal de países que se han preocupado por legislar al respecto, no siendo así la situación de México; es por ello que las experiencias desarrolladas por 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 plantear que el problema de los delitos informáticos y sus consecuencias en la seguridad de las personas y en sus respectivas economías es un hecho grave y que requiere de urgentes medidas de todo tipo, tanto en el ámbito legislativo, de tecnologías y de socialización.

PLANTEAMIENTO DEL PROBLEMA

Nuestra era, se caracteriza por un creciente acceso a la tecnología y a una globalización social de la información y de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas, como Internet, en los próximos años, proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos. La infraestructura de la información se ha convertido en una parte vital del eje de nuestras economías. Los usuarios deberían poder confiar en la disponibilidad de los servicios informativos y tener la seguridad de que sus comunicaciones y sus

datos están protegidos frente al acceso o la modificación no autorizados. El desarrollo del comercio electrónico y la realización completa de la sociedad de la información dependen de ello.

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generalizado. Estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. A medida que las sociedades dependen cada vez más de estas tecnologías, será necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.

El enfoque clásico de la seguridad exige una compartimentación organizativa, geográfica y estructural estricta de la información, según su sensibilidad y su categoría. Esto no es ya prácticamente posible en la práctica en el mundo digital, puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la inter - operabilidad de los sistemas es una condición básica. Los enfoques tradicionales de la seguridad son sustituidos por soluciones innovadoras basadas en las nuevas tecnologías. Estas soluciones

implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo. Garantizar infraestructuras de informaciones seguras y fiables no sólo exige la aplicación de diversas tecnologías, sino también su correcto despliegue y su uso efectivo. Algunas de estas tecnologías existen ya, pero a menudo los usuarios no son conscientes de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias, esta última circunstancia esta muy fuertemente arraigada en la cultura nacional, de no enfrentar esta situación con la debida anticipación, negándonos la oportunidad de tener una clara percepción sobre esta grave problemática.

El hecho de que la informática abarca muchas actividades donde se ve involucrado el Derecho y que estas no se encuentren reguladas por la ley, en consecuencia es viable cuestionarse cuantas personas pueden ser victimas de la carencia que tienen nuestras legislaciones federales y locales, ya que no contemplan las conductas ilícitas denominadas delitos informáticos.

Entonces esto seguirá siendo algo permitido, siendo que no debe de ser así, además debe considerarse que nuestro sistema jurídico se vería beneficiado en gran medida si estipulara y regulara al respecto, ya que tales conductas dejarían de ser atípicas, para pasar a ser algo típico y en consecuencia la sociedad nuevamente tendría la seguridad de que esta puede confiar en que si en un momento dado se ve en la hipótesis de ser victima de un delito informático tendrá la seguridad jurídica de que esta conducta será sancionada por nuestro sistema jurídico. Cabe mencionar que como estudiosos del derecho debemos

tomar cartas en el asunto y no esperar a que estas conductas delictivas se manifiesten de manera muy cotidiana o frecuente, para que se legisle, es pues necesario anteponerse a los hechos ya que el fenómeno informático esta globalizándose y tarde o temprano nuestro país estará haciendo frente a estos problemas. En consecuencia esto será motivo de cambios en las legislaciones vigentes, porque se tendrá que analizar nuevos elementos dentro de los delitos para su adecuada clasificación y tipificación de los mismos, siendo el caso que acontece el presente trabajo, ya que con el mismo se pretende manifestar la necesidad de tomar nuevos elementos para considerar un nuevo Fraude especifico, siendo este el llamado Fraude Informático.

JUSTIFICACIÓN DEL ESTUDIO.

Actualmente la tecnología permite un sin fin de facilidades para elaborar actividades dentro de todos los campos de acción de la vida humana, así mismo como estos facilitan el modo de vida, esta tecnología del mismo modo permite a los delincuentes realizar conductas ilícitas de una manera mas sencilla por medio de sistemas informáticos, así pues los delitos informáticos hoy en día están tomando auge dentro de nuestra sociedad, así mismo uno de los delitos informáticos que atañe a la presente tesis es el delito de Fraude Informático, delito que no se encuentra contemplado dentro de nuestra legislación penal federal.

Es así pues donde se hace uso del Derecho Informático, una rama jurídica de reciente creación, y que con ayuda de la misma permitirá al Licenciado en Derecho en su momento a comprender estas nuevas formas de delinquir, así

como entender los nuevos elementos que contienen estas nuevas formas de cometer ilícitos a través de medios informáticos, en el transcurso del presente trabajo se hace alusión a los distintos delitos informáticos que existen así como los elementos de los mismos.

Como se puede observar este tema es nuevo y resulta bastante apasionante la manera en que estos delitos deben ser estudiados para su comprobación, ya que si bien es cierto, que la tecnología informática hoy en día está al alcance de todos, una gran mayoría no tiene idea que puede ser victima de un delito informático.

Profesionalmente me es necesario hacer ver a la comunidad jurídica que estamos frente a un fenómeno que debe ser considerado para que este tipo de conductas antijurídicas no se encuentren atípicas. Por otra parte es justo y necesario mencionar que el Licenciado en Derecho debe de ser una persona basta en conocimientos para poder atender los fenómenos sociales que surjan con el paso del tiempo, es pues una tarea del estudioso del derecho comprender los delitos informáticos así como su modo de cometerse.

OBJETIVOS.

General: Analizar como el Derecho Informático es una herramienta jurídica, para tipificar los delitos Informáticos en México.

Específicos:

1.- Describir la necesidad del derecho Informático en el sistema jurídico mexicano.

2.- Identificar el delito Fraude Informático en México.

3.- Determinar como el derecho informático permite estructurar una tipificación del delito de Fraude Informático.

HIPOTESIS.

Si por una parte el Fraude Informático es atípico luego entonces el Derecho Informático es una herramienta jurídica para la tipificación de este.

METODOLOGIA.

Para el desarrollo del presente trabajo de tesis, se opto por la investigación bibliográfica, ya que como menciona Rafael Bisquerra "la revisión de la doctrina puede constituir un fin en sí mismo. La búsqueda, recopilación, organización, valoración, critica e información bibliográfica sobre temas específicos, tiene un valor intrínseco en sí mismo debido, principalmente a que: a) es un medio de evitar que la abundancia y dispersión de publicaciones impida una actualización a otros investigadores, b) permite la difusión de una visión panorámica del problema a todos los interesados del tema..." (Bisquerra, Rafael, 1989: 67).

En consecuencia tenemos que gracias a la información bibliográfica se desarrolla la generalidad de los delitos informáticos para tener una panorámica de este fenómeno que se esta presentando en la actualidad.

Con los datos obtenidos, se realizó una selección de material escrito, emanado de diversas fuentes externas a nuestro país, provenientes de países con mayor desarrollo y experiencias en esta área de los delitos informáticos.

Una vez obtenido el panorama de los delitos informáticos el trabajo de tesis se centra en especifico al delito informático de Fraude Informático, para poder darle ilación a la hipótesis planteada y comprobar como gracias al derecho informático se podrá expresar los elementos que definirán el nuevo fraude especifico dentro de nuestro código penal.

LIMITACIONES DE ESTUDIO.

La poca bibliografía existente en la ciudad de Uruapan se convierte en el obstáculo principal de la investigación. Para enfrentar esta situación se hace uso de bibliotecas que se encuentran fuera de la ciudad y del estado. Por otra parte no existe suficiente doctrina mexicana por ser una materia nueva, motivo por el cual se hace uso de doctrinarios extranjeros sin dejar de considerar a los pocos doctrinarios mexicanos que si han escrito al respecto.

CAPITULO 1. EL DERECHO INFORMATICO.

Debido al avance tan desmedido que se ha venido dando dentro del campo de la informática, se ha tenido la necesidad de preocuparse por regular jurídicamente el aspecto informático, ya que es algo de reciente aparición dentro de la sociedad, pero aun y cuando es novedoso, esta ha evolucionado a pasos agigantados, debido a que es una revolución tecnológica que esta abarcando todos los espacios y actividades cotidianas de la sociedad en general, porque la informática, junto con sus micros, minis y macrocomputadoras, los bancos de datos, la telemática, etcétera, están transformando de manera indudable el mundo.

1.1 Concepto de Informática.

En primer lugar debemos de conocer que es la informática, para poder posteriormente saber en que consistirá el derecho informático.

Por tal motivo se definirá a la informática en su acepción general.

La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962 ya que este fue quien creo la palabra informática.

Dícese de la disciplina que se centra en el tratamiento automático de la información.

Entonces de manera general la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para facilitar la toma de decisiones.

Mora y Molino la definen como el estudio que delimita las relaciones entre los medios (equipo), los datos y la información necesaria en la forma de decisiones desde el punto de vista de un sistema integrado.

Mario G. Losano caracteriza a la informática, como producto de la cibernética, en tanto que es un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario.

La Informática es la ciencia del tratamiento automático de la información por medio de computadoras. Este concepto es el más adecuado porque es sencillo de entender que es la informática y que esta se encuentra orientada al manejo de la información a través de las computadoras.

Ya que se ha determinado que es la informática, es necesario conocer la historia de la misma, para que se entienda de donde surgió y como ha evolucionado dicha ciencia con el paso de los años, además, como ha cambiado la forma de vivir de las personas.

1.2 Historia de la informática.

Para poder conocer la informática es necesario remontarse a épocas remotas donde precisamente se dan los orígenes de la informática. El dispositivo más antiguo de calculo es el "ábaco", el nombre viene del griego abakos, que significa superficie plana; se sabe que los griegos empleaban tablas para contar en el siglo V antes de cristo aproximadamente, hoy en día como se le conoce a

este dispositivo de cálculo esta constituido por una serie de hilos con cuentas ensartadas en ellos. En México, este instrumento de cálculo es bastante común en los juguetes de aprendizaje para menores de edad, así como en las salas de billar.

Después del ábaco de los griegos es necesario remontarse al siglo XVI, para conocer a John Napier (1550 – 1617) fue un matemático escocés, famoso por su invención de los logaritmos, funciones matemáticas que permiten convertir las multiplicaciones en sumas y las divisiones en restas. Napier inventó un dispositivo consistente en unos palillos con números impresos que gracias a un ingenioso y complicado mecanismo le permitía realizar operaciones de multiplicación y división.

El primer calculador mecánico, apareció en 1642 tan sólo 25 años después de que Napier publicase una memoria describiendo su máquina. El inventor de esta máquina fue el filósofo francés Blaise Pascal (1623 – 1662), en cuyo honor se llama Pascal uno de los lenguajes de programación que más impacto causó en los últimos años. A los 18 años Pascal deseaba dar con una forma de reducir el trabajo de cálculo de su padre que era un funcionario de impuestos, motivado por esto Pascal inventó una calculadora que tenía el tamaño de un cartón de tabaco y su principio de funcionamiento era el mismo que rige los cuentakilómetros de los coches actuales; este mecanismo estaba compuesto por unas ruedas, y cada una de estas hacia a su vez avanzar un paso a la siguiente rueda, al completar una vuelta. Las ruedas estaban marcadas con números del 0 al 9 y había dos para los decimales y 6 para los enteros con lo que podía manejar números entre 000,000.00 y 999,999.00. Las ruedas giraban mediante una manivela por medio

de la cual se podía sumar y restar, y girando la correcta manivela los números giraban en un sentido o en otro adecuadamente.

Un contemporáneo de Pascal fue Leibnitz (1646 – 1716) uno de los genios de su época; a los 26 años aprendió matemáticas de modo autodidacta y procedió a inventar el cálculo. Inventó una máquina de calcular por la simple razón de que nadie le enseñó las tablas de multiplicar. La máquina de Leibnitz apareció en 1672; se diferenciaba de la de Pascal en varios aspectos, el más importante consistía en que esta maquina podía multiplicar, dividir y obtener raíces cuadradas. Leibnitz propuso la idea de una máquina de cálculo en sistema binario, base de numeración empleada por los modernos ordenadores actuales. Tanto la máquina de Pascal como la de Leibnitz se encontraron con un grave freno para su difusión: la Revolución Industrial aún no había tenido lugar y sus máquinas eran demasiado complejas para ser realizadas a mano. La civilización que habría podido producirlas en serie estaba todavía a más de 200 años de distancia.

Entre 1673 y 1801 se realizaron algunos avances significativos, el más relevante de estos fue el de Joseph Jacquard (1752 – 1834) quien utilizó un mecanismo de tarjetas perforadas para controlar el dibujo formado por los hilos de las telas confeccionadas por una máquina de tejer. Hacia 1725 los artesanos textiles franceses utilizaban un mecanismo de tiras de papel perforado para seleccionar unas fichas perforadas, las que a su vez controlaban la máquina de tejer. Jacquard fue el primero en emplear tarjetas perforadas para almacenar la información sobre el dibujo del tejido y además controlar la máquina. La máquina

de tejer de Jacquard presentada en 1801, supuso gran éxito comercial y un gran avance en la industria textil.

Como se puede observar estos inventores tenían como objetivo el facilitar sus actividades mediante la automatización y almacenamiento de información que pudiera facilitarles, ya fuera el calculo de información o la simplificación mediante la producción en serie por medio de almacenamiento de información en tarjetas que realizaban lo que en estas se perforaba.

La antesala de la informática, es apreciable desde los logros que obtuvieron distintas personalidades mediante los inventos que estos realizaron. Aunque hubo muchos precursores de los actuales sistemas informáticos para muchos especialistas la historia empieza con Charles Babbage matemático e inventor inglés que al principio del siglo XIX predijo muchas de las teorías en que se basan los actuales ordenadores. Desgraciadamente al igual que sus predecesores vivieron en una época en que ni la tecnología ni las necesidades estaban al nivel de permitir la materialización de sus ideas.

En 1822 diseño su máquina diferencial para el cálculo de tablas de navegación y artillería, lo que permitió a Babbage conseguir una versión de la máquina. Durante 10 años Babbage trabajó sin éxito en una segunda máquina sin lograr completarla y en 1833 tuvo una idea mejor.

Mientras que la máquina diferencial era un aparato de proceso único, Babbage decidió construir una máquina de propósito general que pudiese resolver casi cualquier problema matemático. Todas estas máquinas eran por supuesto movidas por vapor. De todas formas la velocidad de cálculo de las máquinas no

era tal como para cambiar la naturaleza del cálculo además la ingeniería entonces no estaba lo suficientemente desarrollada como para permitir la fabricación de los delicados y complejos mecanismos requeridos por el ingenio de Babbage.

La sofisticada organización de esta segunda máquina llamada máquina diferencial, nombrada así por Babbage, es el motivo por el cual se le considera el padre de la informática actual. Como los modernos computadores, la máquina de Babbage tenía un mecanismo de entrada y salida por tarjetas perforadas, una memoria, una unidad de control y una unidad aritmético – lógica. Preveía tarjetas separadas para programas y datos. Una de sus características importantes era que la máquina podía alterar su secuencia de operaciones en base al resultado de cálculos anteriores algo fundamental en los ordenadores modernos. La máquina sin embargo nunca llego a construirse. Babbage no pudo conseguir un contrato de investigación y pasó el resto de su vida inventando piezas y diseñando esquemas para conseguir los fondos para construir la máquina. Murió sin lograr conseguirlo. Aunque otros pocos hombres trataron de construir autómatas o calculadoras siguiendo los esquemas de Babbage su trabajo quedo olvidado hasta que otros inventores modernos que desarrollaban sus propios proyectos de computadores se encontraron de pronto con tan extraordinario precedente.

Otro inventor digno de mención es Herman Hollerith, quien a los 19 años en 1879 fue contratado como asistente en las oficinas del censo norteamericano que por aquel entonces se disponía a realizar el recuento de la población para el censo de 1880. Este tardó 7 años y medio en completarse manualmente. Hollerith fue animado por sus superiores a desarrollar un sistema de cómputo automático para

futuras tareas. El sistema inventado por Hollerith utilizaba tarjetas perforadas en las que mediante agujeros se presentaba el sexo, la edad, la raza, etcétera. En la máquina las tarjetas pasaban por un juego de contactos que cerraban un circuito eléctrico activándose un contador y un mecanismo de selección de tarjetas. Estas se leían a un ritmo de 50 a 80 por minuto. Desde 1880 a 1890 la población subió de 50 a 63 millones de habitantes aun así el censo de 1890 se realizó en dos años y medio gracias a la máquina de Hollerith.

Ante las posibilidades comerciales de su máquina Hollerith dejó las oficinas del censo en 1896 para fundar su propia compañía la Tabulating Machine Company. En 1900 había desarrollado una máquina que podía clasificar 300 tarjetas por minuto, una perforadora de tarjetas y una máquina de cómputo semiautomática. En 1924 Hollerith fusionó su compañía con otras dos para formar la Internacional Business Machines hoy mundialmente conocida como IBM.

Ya que se ha visto este esbozo, es posible mencionar el nacimiento del ordenador actual. Ante la necesidad de agilizar el proceso de datos de las oficinas del censo se contrató a James Powers un estadístico de Nueva Jersey para desarrollar nuevas máquinas para el censo de 1910. Powers diseñó nuevas máquinas para el censo de 1910 y de modo similar a Hollerith decidió formar su propia compañía en 1911; la Powers Accounting Machine Company que fue posteriormente adquirida por Remington Rand la cual a su vez se fusionó con la Sperry Corporation formando la Sperry Rand Corporation.

John Vincent Atanasoff nació en 1903 su padre era un ingeniero eléctrico emigrado de Bulgaria y su madre una maestra de escuela con un gran interés por las matemáticas, mismo que le transmitió a su hijo. Atanasoff se doctoró en física teórica y comenzó a dar clases en Iowa al comienzo de los años 30. Se encontró con lo que en ese entonces eran dificultades habituales para muchos físicos y técnicos; los problemas que tenían que resolver requerían una excesiva cantidad de cálculo para los medios de que disponían. Aficionado a la electrónica y conocedor de la máquina de Pascal y las teorías de Babbage, Atanasoff empezó a considerar la posibilidad de construir un calculador digital. Decidió que la máquina habría de operar en sistema binario, hacer los cálculos de modo totalmente distinto a como los realizaban las calculadoras mecánicas e incluso concibió un dispositivo de memoria, mediante almacenamiento de carga eléctrica. Durante un año maduró el proyecto y finalmente solicitó una ayuda económica al Consejo de Investigación del Estado de Iowa. Con unos 650 dólares contrató la cooperación de Clifford Berry estudiante de ingeniería y los materiales para un modelo experimental. Posteriormente recibieron otras dos donaciones que sumaron 1460 dólares y otros 5000 dólares de una fundación privada. Este primer aparato fue conocido como ABC Atanasoff- Berry-Computer.

En diciembre de 1940 Atanasoff se encontró con John Mauchly en la American Association for the Advancement of Science (Asociación Americana para el Avance de la Ciencia) abreviadamente AAAS. Mauchly, que dirigía el departamento de física del Ursine College cerca de Filadelfia se había encontrado

con los mismos problemas en cuanto a velocidad de cálculo que Atanasoff y estaba convencido de que habría una forma de acelerar el cálculo por medios electrónicos. Al carecer de medios económicos construyó un pequeño calculador digital y se presentó al congreso de la AAAS para presentar un informe sobre el mismo. A raíz de aquello Atanasoff y Mauchly tuvieron un intercambio de ideas, que muchos años después desembocó en una disputa entre ambos sobre la paternidad del computador digital.

En 1941 Mauchly se matriculó en unos cursos sobre ingeniería eléctrica en la escuela Moore de Ingeniería donde conoció a un instructor de laboratorio llamado J. Presper Eckert. Entre ambos surgió una compenetración que les llevaría a cooperar en un interés común: el desarrollo de un calculador electrónico. El entusiasmo que surgió entre ambos llevo a Mauchly a escribir a Atanasoff solicitándole su cooperación para construir un computador como el ABC en la escuela Moore. Atanasoff prefirió guardar la máquina en un cierto secreto hasta poder patentarla; sin embargo nunca llegó a conseguirlo. Mauchly fue más afortunado. La escuela Moore trabajaba entonces en un proyecto conjunto con el ejército para realizar unas tablas de tiro para armas balísticas.

La cantidad de cálculos necesarios era inmensa tardándose treinta días en completar una tabla mediante el empleo de una máquina de cálculo analógica. Aun así esto era unas 50 veces más rápido de lo que tardaba un hombre con una sumadora de sobremesa. En el laboratorio Mauchly trabajó sobre sus ideas y las de Atanasoff publicando una memoria que despertó el interés de Lieutenant

Herman, joven matemático que hacía de intermediario entre la universidad y el ejército y que consiguió interesar al Departamento de Ordenación en la financiación de un computador electrónico digital.

El 9 de abril de 1943 se autorizó a los dos hombres a iniciar el desarrollo del proyecto. Se le llamó ENIAC (Electronic Numerical integrator and Computer). El presupuesto inicial era de 150,000 dólares cuando la máquina estuvo terminada el costo total había sido de 486,804 dólares. El ENIAC tenía unos condensadores, 70,000 resistencias, 7,500 interruptores y 17,000 tubos de vacío de 16 tipos distintos funcionando todo a una frecuencia de reloj de 100,000 Hertz. Pesaba unas 30 toneladas y ocupaba unos 1,600 metros cuadrados. Su consumo medio era de unos 100,000 vatios (lo que un bloque de 50 viviendas) y necesitaba un equipo de aire acondicionado a fin de disipar el gran calor que producía. Tenía 20 acumuladores de 10 dígitos, era capaz de sumar, restar, multiplicar y dividir; además tenía tres tablas de funciones. La entrada y la salida de datos se realizaban mediante tarjetas perforadas. En un cuestionario de prueba en febrero de 1946 el Eniac resolvió en 2 horas un problema de física nuclear que previamente habría requerido 100 años de trabajo de un hombre. Lo que caracterizaba al ENIAC como a los ordenadores modernos no era simplemente su velocidad de cálculo sino el hecho de que combinando operaciones permitía realizar tareas que antes eran imposibles.

Entre 1939 y 1944 Howard Aiken de la universidad de Harvard en colaboración con IBM desarrolló el Mark 1 también conocido como calculador

Automático de Secuencia Controlada. Este fue un computador electromecánico de 16 metros de largo y más de dos de alto. Tenía 700,000 elementos móviles y varios centenares de kilómetros de cables. Podía realizar las cuatro operaciones básicas y trabajar con información almacenada en forma de tablas. Operaba con números de hasta 23 dígitos y podía multiplicar tres números de 8 dígitos en 1 segundo.

El Mark 1 y las versiones que posteriormente se realizaron del mismo, tenían el mérito de asemejarse considerablemente al tipo de máquina ideado por Babbage aunque trabajaban en código decimal y no binario. El avance que estas máquinas electromecánicas supuso fue rápidamente ensombrecido por el Eniac con sus circuitos electrónicos.

En 1946 el matemático húngaro John Von Neumann propuso una versión modificada del Eniac; el Edvac (Electronic Discrete Variable Automatic Computer) que se construyó en 1952. Esta máquina presentaba dos importantes diferencias respecto al Eniac: En primer lugar empleaba aritmética binaria lo que simplificaba enormemente los circuitos electrónicos de cálculo. En segundo lugar permitía trabajar con un programa almacenado. El Eniac se programaba enchufando centenares de clavijas y activando un pequeño número de interruptores. Cuando había que resolver un problema distinto era necesario cambiar todas las conexiones proceso que llevaba muchas horas.

Von Neumann propuso cablear una serie de instrucciones y hacer que éstas se ejecutaran bajo un control central. Además propuso que los códigos de operación que habían de controlar las operaciones se almacenasen de modo similar a los datos en forma binaria. De este modo el Edvac no necesitaba una modificación del cableado para cada nuevo programa pudiendo procesar instrucciones tan deprisa como los datos. Además el programa podía modificarse a sí mismo ya que las instrucciones almacenadas como datos podían ser manipuladas aritméticamente.

Eckert y Mauchly tras abandonar la universidad fundaron su propia compañía la cual tras diversos problemas fue absorbida por Rémington Rand. El 14 de junio de 1951 entregaron su primer ordenador a la Oficina del Censo el Univac - I.

Posteriormente aparecería el Univac-II con memoria de núcleos magnéticos lo que le haría claramente superior a su antecesor pero por diversos problemas esta máquina no vio la luz hasta 1957 fecha en la que había perdido su liderazgo en el mercado frente al 705 de IBM.

En 1953 IBM fabricó su primer computador para aplicaciones científicas, el 701. Anteriormente había anunciado una máquina para aplicaciones comerciales, el 702 pero esta máquina fue rápidamente considerada inferior al Univac-I. Para compensar esto IBM lanzó al mercado una máquina que resultó arrolladora, el 705 primer ordenador que empleaba memorias de núcleos de ferrita, IBM superó

rápidamente a Sperry en volumen de ventas gracias a una eficaz política comercial que actualmente la sigue manteniendo a la cabeza de todas las compañías de informática del mundo en cuanto a ventas.

A partir de entonces fueron apareciendo progresivamente más y más maquinas. Veamos las etapas que diferencian unas máquinas de otras según sus características. Cada etapa se conoce con el nombre de generación.

La primera generación, comienza con el Univac 1, que viene a marcar el comienzo de lo que se llama la primera generación. Los ordenadores de esta primera etapa se caracterizan por emplear el tubo de vacío como elemento fundamental de circuito. Son máquinas grandes, pesadas y con unas posibilidades muy limitadas. El tubo de vacío es un elemento que tiene un elevado consumo de corriente genera bastante calor y tiene una vida media breve. Hay que indicar que a pesar de esto no todos los ordenadores de la primera generación fueron como el Eniac las nuevas técnicas de fabricación y el empleo del sistema binario llevaron a máquinas con unos pocos miles de tubos de vacío.

En 1958 comienza la segunda generación cuyas máquinas empleaban circuitos con transistores. El transistor es un elemento electrónico que permite reemplazar al tubo con las siguientes ventajas: su consumo de corriente es mucho menor con lo que también es menor su producción de calor. Su tamaño es también mucho menor. Un transistor puede tener el tamaño de una lenteja mientras que un tubo de vacío tiene un tamaño mayor que el de un cartucho de

escopeta de caza. Esto permite una drástica reducción de tamaño. Mientras que las tensiones de alimentación de los tubos estaban alrededor de los 300 voltios la de los transistores vienen a ser de 10 voltios con lo que los demás elementos de circuito también pueden ser de menor tamaño al tener que disipar y soportar una tensión mucho menor. El transistor es un elemento constituido fundamentalmente por silicio o germanio. Su vida media es prácticamente ilimitada y en cualquier caso muy superior a la del tubo de vacío. Como podemos ver el simple hecho de pasar del tubo de vacío al transistor supone un gran paso en cuanto a reducción de tamaño y consumo y aumento de fiabilidad. Las máquinas de la segunda generación emplean además algunas técnicas avanzadas no sólo en cuanto a electrónica sino en cuanto a informática y proceso de datos como por ejemplo los lenguajes de alto nivel.

En 1964 la aparición del IBM 360 marca el comienzo de la tercera generación. Las placas de circuito impreso con múltiples componentes pasan a ser reemplazadas por los circuitos integrados. Estos elementos son unas plaquitas de silicio llamadas chips sobre cuya superficie se depositan por medios especiales unas impurezas que hacen las funciones de diversos componentes electrónicos. Así pues un puñado de transistores y otros componentes se integran ahora en una plaquita de silicio. Aparentemente esto no tiene nada de especial salvo por un detalle; un circuito integrado con varios centenares de componentes integrados tiene el tamaño de una moneda.

De esta manera se logro otro salto importante en cuanto a la reducción de tamaño. El consumo de un circuito integrado es también menor que el de su equivalente en transistores resistencias y demás componentes. Además su fiabilidad es también mayor.

En la tercera generación aparece la multiprogramación, el teleproceso se empieza a generalizar con el uso de mini computadores en los negocios y se usan cada vez más los lenguajes de alto nivel como Cobol y Fortran.

La aparición de una cuarta generación de ordenadores hacia el comienzo de los años setenta no es reconocida como tal por muchos profesionales del medio para quienes ésta es sólo una variación de la tercera. Máquinas representativas de esta generación son el IBM 370 y el Burroughs. Las máquinas de esta cuarta generación se caracterizan por la utilización de memorias electrónicas en lugar de las de núcleos de ferrita.

Estas representan un gran avance en cuanto a velocidad y en especial en cuanto a reducción de tamaño. En un chip de silicio no mayor que un centímetro cuadrado caben 64.000 bits de información. En núcleos de ferrita esa capacidad de memoria puede requerir cerca de un litro en volumen.

Se empieza a desechar el procesamiento batch o por lotes en favor del tiempo real y el proceso interactivo. Aparecen innumerables lenguajes de programación. Las capacidades de memoria empiezan a ser enormemente grandes. En esta etapa cobran gran auge los mini computadores. Estos son

maquinas con un procesador de 16 bits una memoria de entre 16 32 KB y un precio de unos cientos de miles.

Posteriormente hacia finales de los setenta aparece la que podría ser la quinta generación de ordenadores. Se caracteriza por la aparición de los microcomputadores y los ordenadores de uso personal. Estas máquinas se caracterizan por llevar en su interior un microprocesador, circuito integrado que reúne en un sólo chip de silicio las principales funciones de un ordenador. Los ordenadores personales son equipos a menudo muy pequeños, no permiten multiproceso y suelen estar pensados para uso doméstico o particular. Los microcomputadores si bien empezaron tímidamente como ordenadores muy pequeñitos rápidamente han escalado el camino superando a lo que hace 10 años era un mini computador. Un microcomputador actual puede tener entre 32Mb y 512Mb de memoria, discos con capacidades del orden del Giga bite y pueden permitir la utilización simultánea del equipo por varios usuarios.

Ya que se ha logrado determinar que es la informática y como ha evolucionado esta a través del tiempo es de suma importancia conocer como el derecho se vinculara con la informática.

1.3 Concepto de Derecho.

En razón de que las actividades humanas necesitan de conductas reguladas por una ley, es de ahí la necesidad de que las mismas se encuentren

contempladas dentro de leyes para poder vivir armónicamente en sociedad, en consecuencia tenemos que la creación del derecho es hecha por el ser humano para que él mismo, cree leyes acordes a las necesidades de los humanos, ya que es imperativo saber que el derecho es una rama que evoluciona constantemente y que existirán conductas y actividades que surjan con el transcurso del tiempo que no se encuentren reguladas en su momento, luego entonces el derecho se encargara de su estudio y del mismo modo regulara las actividades que surjan.

Ahora bien debe entenderse que es el derecho para poder relacionar al derecho con la informática y de este modo, comprender como surge el derecho informático y cual será la finalidad de este.

Rafael de Pina Vara, nos define al Derecho de la siguiente manera "... en general se entiende por derecho todo conjunto de normas eficaz para regular la conducta de los hombres...". (Pina Vara, 1998: 228)

La necesidad de una reglamentación coercitiva e imperativa, es una necesidad humana que surgió cuando aparecen los grupos, las familias, los clanes y en si la sociedad moderna, entonces es cierto que el Derecho es producto de la organización social, creado de la mano del hombre, motivo por el cual el ser humano no puede hacerlo a un lado cuando ha alcanzado cierta evolución social.

Atendiendo a la etimología de la palabra, el vocablo Derecho, toma su origen de la voz latina *directus*, que significa recto, directo, participio del verbo *dirigiere*: dirigir. La voz latina *jus*, con la que se designo en Roma al Derecho, no es sino una contracción de *jussum*, participio del verbo *jubere*, que significa

mandar. La palabra derecho ha sido utilizada empleando para ella diversas acepciones, a saber:

a) El conjunto de reglas o preceptos de conducta de observancia obligatoria que el estado impone a sus súbditos.
b) Disciplina científica que tiene por objeto el conocimiento y la aplicación de esas reglas de conducta.
c) Conjunto de facultades que tiene un individuo y que le permiten hacer o dejar de hacer algo frente a los demás y frente al estado mismo.

En base a estos elementos son bastantes los conceptos que se han creado en relación al Derecho como ciencia jurídica, es relevante hacer sobresalir el concepto elaborado por el Maestro Villoro Toranzo, quien expresa del derecho lo siguiente: "... el derecho es el sistema racional de normas sociales de conducta, declarada obligatoria por la autoridad, por considerarlas soluciones justas a los problemas surgidos de la realidad histórica". Entonces el derecho debe estar encaminado también a la búsqueda de la justicia y el bien común. (Pina Vara 1998: 229)

1.4 Concepto de Derecho Informático.

El Derecho Informático es una rama jurídica en constante evolución en razón de que como se ha venido manejando la tecnología informática avanza muy rápido día con día, es en virtud de esta que como consecuencia el derecho informático para no volverse obsoleto tiene que evolucionar con la misma. Se

puede definir de la siguiente manera de acuerdo con el autor Julio Téllez Valdez, "... el Derecho Informático es una rama de ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la información)" (Téllez Valdez, 1999: 65)

Por otra parte Miguel A. Espino González define al derecho informático de la siguiente manera, "... el conjunto de los debates, reflexiones y soluciones generadas en el ámbito jurídico por la irrupción de las computadoras suele denominarse derecho informático".

Tal rama jurídica tiene un contenido muy variado, por otra parte es en distintas ramas jurídicas que la tecnología esta causando un cambio en las mismas, tales contenidos pueden enumerarse de manera sencilla:

a) Contratos Informáticos.

b) Protección del software.

c) Protección de datos personales.

d) Transferencia electrónica de fondos.

e) Documento informático.

f) Delitos Informáticos.

g) Flujo de datos de transfrontera.

h) Política informática.

De esta manera se puede apreciar que el derecho informático estará vinculado a la vez con otras ramas jurídicas para la total comprensión de ciertas conductas que están surgiendo debido al impacto tecnológico que existe actualmente en nuestra sociedad.

CAPITULO 2. LOS DELITOS INFORMATICOS

2.1 Concepto de Delito.

De acuerdo con el autor del Libro de Introducción a la criminalística de Rafael Moreno González nos menciona que "... el delito se transforma al compás de la evolución de la sociedad y va adoptando nuevas modalidades que no constituyen sino eco de las mutaciones, que se operan en aquélla bajo la influencia decisiva de la civilización". (Moreno González, 1997:293)

Partiendo desde aquí se debe entender que el delito evoluciona así como la sociedad misma y esto aunado a la tecnología informática, nos da como resultado nuevos delitos.

Por tal motivo es necesario entender que es un delito, el Diccionario Jurídico Mexicano del Instituto de Investigaciones Jurídicas lo define diciendo que el delito es "... una acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal". (Diccionario Jurídico Mexicano, 2000:868)

Ahora por otra parte el Código Penal Federal en su artículo 7 lo define de la siguiente manera "... delito es la acción u omisión que sancionan las leyes penales". El Código Penal del Estado de Michoacán en su Artículo 7, lo define de la siguiente manera "... delito es el acto u omisión que sancionan las leyes penales.

Es claro que las definiciones que se han manejado en el fondo tienen los mismos elementos, coincidiendo en que el delito para ser considerado como tal

debe estipularse así dentro de un cuerpo legal, luego entonces este cuerpo señalara que conductas serán las que puedan ser consideradas como delitos.

Cabe mencionar que Carranca y Trujillo consideran al delito como "... el acto típicamente antijurídico culpable, sometido a veces a condiciones de penalidad, imputable a un hombre y sometido a sanción penal. (Carranca y Trujillo, 1991:223)

Una vez que se ha analizado distintos conceptos de delito debe entenderse que el delito es considerado como tal cuando una conducta sea considerada dentro de un cuerpo legal como delictiva.

2.2. Concepto de Delito Informático.

Hoy en día las computadoras no solo son utilizadas como herramientas de trabajo sino también como aquel medio a través del cual se puede obtener y conseguir información, luego entonces, esta tecnología esta creciendo y evolucionando a pasos agigantados. Por tal motivo la informática esta involucrada directamente en casi todos los campos de la vida moderna, ya que de una u otra manera todos los conocimientos y actividades humanas están cambiando su manera de elaborarse en razón de que en el pasado cosas que se realizaban manualmente empleaba bastante tiempo siendo que en el presente hace falta acceder a una computadora para realizarlo y ahorrarse tiempo. Del mismo modo se están viendo afectadas las mas diversas esferas del conocimiento humano, en

lo científico, en lo técnico y en lo profesional están siendo incorporados tales conocimientos a sistemas informáticos que, en la práctica cotidiana, proporciona con facilidad a quien lo desee un conjunto de datos que hasta hace unos años solo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las maquinas existentes tenían rango de equipos auxiliares para imprimir los resultados. En la actualidad, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse mediante documentos electrónicos y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Este es el panorama de este nuevo fenómeno científico- tecnológico en las sociedades modernas. Las facultades que el fenómeno pone a disposición de gobiernos y de particulares, con rapidez y ahorro de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Esta nueva aplicación de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

El siguiente extracto del trabajo elaborado Por el Licenciado Marcelo Manson nos narra que "... el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la ultima década en los Estados Unidos,

Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto". (http://www.ambito-juridico.com.br/aj/dp0019.htm)

Pero para entender tal amenaza, es necesario saber que significa un delito informático, así mismo conocer de qué maneras se le conoce en el mundo a este.

A los Delitos Informáticos se les denomina de distintas maneras: delitos electrónicos, delitos relacionados con la computadora, crímenes por computadora, delincuencia relacionada con el ordenador, entre otras.

Según Helen Peña, Silvia Palazuelos y Rosalía Alarcón, estudiosos de la División de Postgrado de la Facultad de Derecho de la Universidad Nacional Autónoma de México, 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, falsificaciones, perjuicios, estafa, sabotaje, fraudes, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. (http://tiny.uasnet.mx/prof/cln/der/silvia/).

Así mismo existen distintas definiciones de Delito Informático; la Doctora María José Viega Rodríguez en su artículo sobre delitos informáticos hace una recopilación de algunas de estas definiciones, citando la que realiza la Universidad de México, la cual define a los Delitos Informáticos como: "... toda conducta ilícita susceptible de ser sancionada por el Derecho Penal, por hacer uso indebido de

cualquier medio informático". (http://www.cni.org/Hforums/cni-copyright/1998-04/1074.html)

Jijena Leiva lo define como: "... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma". (http://www.juridicas.unam.mx/publica/rev/boletin/cont/79/bib/bib21.htm).

Julio Téllez Valdez, señala que "... no es labor fácil dar un concepto sobre Delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "Delitos Informáticos esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún.

Para Carlos Sarzana, en su obra Criminalidad y tecnología, los crímenes por computadora comprenden "... cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo". (http://www.geocities.com/delincuentes_digitales/).

Nidia Callegari define al Delito Informático como "... aquel que se da con la ayuda de la informática o de técnicas anexas". (http://www.aadat.org/delitos_informaticos20.htm).

Rafael Fernández Calvo define al Delito Informático como "... la realización de una acción que reuniendo las características que delimitan el concepto de

delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos".

Maria de la Luz Lima dice que el "... Delito Electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Julio Téllez Valdez, define al delito informático en forma típica y atípica, entendiendo por la primera a "... las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (y por las segundas), actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". Téllez Valdez 1998: 103).

Atendiendo a esta definición del Doctor Julio Téllez Valdez, de Delito Informático, se puede observar como una gran cantidad de estos delitos, son los mismos que encontramos tipificados en nuestro ordenamiento jurídico, como lo son: robo, fraude, falsificación, etcétera, con la peculiaridad de que muchos de ellos son ejecutados a través de novedosas modalidades.

De acuerdo con la Doctora María José Viega Rodríguez, el Delito Informático trasciende las fronteras de los estados convirtiéndose en un delito internacional, debido a que la información viaja sin importar las fronteras de l os estados.

2.3. El Sujeto Activo y Pasivo del Delito Informático.

Un elemento importante dentro del concepto de Delito Informático es con respecto de la participación de los sujetos en el hecho delictivo, sea que esta participación se dé de forma activa o pasiva.

2.3.1. El Sujeto Activo.

Se trata de un tipo de delincuente especial, por cuanto en la mayoría de los casos son personas con conocimientos avanzados en cómputo y estos tipos de tecnología. Sin embargo, algunos autores no comparten esta forma de pensar toda vez que afirman que el nivel educacional no es indicativo de esta clase de delincuentes.

Según un estudio de trabajo sobre delitos informáticos elaborado por la facultad de Derecho de la Universidad de Costa Rica, se trata de sujetos que ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter confidencial. A pesar de estas características podemos apreciar que puede tratarse de sujetos completamente diferentes. No es lo mismo el joven que ingresa en un sistema de seguridad o base de datos por mera curiosidad, por un reto personal a violar la seguridad, a aquel empleado que realiza actividades irregulares dentro de su propio trabajo con el afán de obtener un beneficio.

2.3.2. El Sujeto Pasivo.

Según la Doctora María José Viega, "... sujeto pasivo es la persona o entidad sobre la cual recae la conducta que realiza el sujeto activo. La mayoría de los delitos informáticos no son descubiertos, pero es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica".

Debido a lo mencionado anteriormente debe hacerse hincapié en lo siguiente, para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las victimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

2.4. Clasificación.

Se debe entender que los delitos informáticos tienen una variada forma de cometerse y por tal distintas modalidades, entonces para clasificar los delitos informáticos, se ha de tomar en cuenta distintos elementos y criterios; de acuerdo con un estudio elaborado por la Facultad de Derecho de la Universidad de Costa Rica, los elementos y criterios a considerar son:

- 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.

Tomando en cuenta lo expuesto en los puntos anteriores, Jorge Pacheco Klein hace la siguiente clasificación:

- Delito informático interno, manejando el ejemplo de sabotaje de programas.
- Delitos a través de telecomunicaciones, como ejemplo tenemos al hacking.
- Manipulación de computadoras, y un caso de este es la apropiación indebida y fraudes informáticos.
- Utilización de computadoras en apoyo a empresas criminales, como lavado de dinero o distribución ilícita de drogas.
- Robos de software, aquí tenemos todo lo relacionado a la piratería de los mismos. (http://www.unifr.ch/derechopenal/articulos/pdf/Montano1.pdf)

Por otra parte el Doctor Julio Téllez Valdez, este tipo de acciones 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) pueden llegar a cometerlas.
- Son acciones ocupacionales, en debido a que muchas veces se realizan cuando el sujeto se halla trabajando.
- 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.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Así mismo él Doctor Julio Téllez Valdez clasifica a estos delitos de acuerdo a dos criterios:

1. Como instrumento o medio. En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planteamiento y simulación de delitos convencionales (robos, homicidio, fraude, etcétera.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo. En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etcétera).

Por otra parte María de la Luz, presenta una clasificación, de lo que ella llama Delitos Electrónicos, manifestando que existen tres categorías a conocer:

1. Los que utilizan la tecnología electrónica como método.
2. Los que utilizan la tecnología electrónica como medio.
3. los que utilizan la tecnología electrónica como fin.

Como método – conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio – conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin – conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Existe otra clasificación la cual fue publicada en la Revista de la Policía Nacional del Perú elaborada por el Coronel Hugo Müller Solón la cual manifiesta que "... la ley que incorpora los Delitos Informáticos al Código Penal Peruano ha considerado únicamente dos tipos genéricos, de los que se desprenden una serie de modalidades. Para ello, el legislador se ha basado en el criterio del uso de la computadora como instrumento o medio y en el de su utilización como fin u objetivo.

El primer tipo genérico lo encontramos en el artículo 207 – A que describe una conducta criminógena que se vale de la computadora para la comisión del ilícito penal. Un ejemplo de ello lo constituyen los fraudes cometidos en perjuicio de las instituciones bancarias o de cualquier empresa por personal del área de sistemas que tiene acceso a los tipos de registros y programas utilizados. También se encuadra el fraude efectuado por manipulación informática, es decir, cuando se accede a los programas establecidos en un sistema de información y se les manipula para obtener una ganancia monetaria. Otras modalidades son la falsificación informática, que consiste en la manipulación de la información arrojada por una operación de consulta en una base de datos: el acceso no autorizado a sistemas o servicios; la reproducción no autorizada de programas informáticos de protección legal, conocida como piratería, entre otras.

El segundo Tipo Genérico lo encontramos en el artículo 207 – B, donde se enmarcan las conductas criminales dirigidas a la utilización, interferencia o ingreso indebido a una base de datos con el fin de alterarla, dañarla o destruirla. (http://www.pnp.gob.pe/culturales/revista_81/pag_36_40.pdf).

2.5. Tipos de Delitos Informáticos conocidos.

Ya que se conoce la clasificación de los delitos informáticos, es necesario conocer que tipos de delitos existen, para tener conocimiento de cómo se les puede identificar, así mismo saber como se les denomina a los mismos para poder ubicarlos dentro de un espacio y no solo sea una mera clasificación teórica.

La Organización de las Naciones Unidas reconoce distintos tipos de delitos:

Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los 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.

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

c) Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían 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.

d) Fraude efectuado por manipulación informática: Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van secando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas.

a) Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

b) Como instrumentos: 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.

Daños o modificaciones de programas o datos computarizados.

a) 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. Las técnicas que permiten cometer sabotajes informáticos son:

- Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- Gusanos: se fabrica de forma analógica al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero de una cuenta ilícita.
- Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, lo contrario 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 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 lógica.

b) Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: Desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

- Piratas informáticos o Hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c) Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a

sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicación moderna.

Aparte de los que reconoce la Organización de las Naciones Unidas existen otra técnica conocida para cometer sabotaje informático y esta es conocida con el nombre de "rutinas cáncer" las cuales distorsionan el funcionamiento del programa y se auto reproducen al estilo de las células orgánicas alcanzadas por un tumor maligno, es decir comienza a reproducir archivos hasta que satura la unidad de almacenamiento, conocida como disco duro, dañándolo permanentemente ya que una vez que un disco duro se llena totalmente ya no sirve.

Ya que dentro de los tipos de delitos informáticos que reconoce la Organización de las Naciones Unidas, hace referencia al espionaje sin ahondar dejar claro tal tipo de delito, entonces se deberá entender por "espionaje informático", el acceso telemático no autorizado, así como la fuga de datos a un sistema realizado por los llamados Hackers o piratas informáticos. El acceso se puede dar en forma directa, cuando alguien se introduce a información no autorizada desde adentro de una red interna y lo puede ser también de manera indirecta accediendo a información de sistemas por medio de la red, mas conocida como Internet.

Este acceso no autorizado a sistemas informáticos se puede dar de distintas maneras empleando:

- Puertas Falsas: es la intromisión indebida aprovechando los accesos de entrada.

- Llave Maestra: permite abrir cualquier archivo de una computadora, aunque sea protegido por medidas de seguridad.
- Pinchado de Líneas: es la interferencia de líneas telefónicas en las que se transmiten datos informáticos.

A los individuos capaces de realizar estas conductas se les ha denominado de la siguiente manera:

- Hacker: es la persona que explora detalles de los sistemas programables y aprendiendo a usarlos al máximo.
- Cracker: es el que rompe con la seguridad de un sistema.
- Preacker: es el que rompe la red telefónica para beneficios personales, como para llamadas gratis de larga distancia.

Existe otro tipo reconocido y denominado "violación a la intimidad", que consiste en observar, escuchar, registrar hechos, palabras o imágenes valiéndose de procesos técnicos u otros medios.

Como se ha podida observar existe un gran número de delitos informáticos, razón por la que distintos países han considerado tipificarlos dentro de sus legislaciones penales, no siendo así el caso de México.

CAPITULO 3. ORDENAMIENTO JURIDICO A NIVEL INTERNACIONAL.

El presente capitulo tendrá por finalidad presentar todos aquellos elementos que han sido contemplados por organismos internacionales así como por distintos países dentro de sus cuerpos legales para enfrentar la problemática de los delitos informáticos

3.1 Organismos Internacionales.

Durante los últimos años se ha perfilando en el ámbito internacional un cierto consenso de las valoraciones jurídico políticas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado como consecuencia que se modifiquen las leyes penales de distintos países en el mundo.

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

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración *ius comparativista* de los derechos nacionales

aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

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

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía

conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos

en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran establecer un marco de seguridad para los sistemas informáticos el mismo año.

Es apreciable que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, esto es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la necedad transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal - hasta ese entonces -era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros

automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo lo sucedido, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

Debe mencionarse que la Asociación Internacional de Derecho Penal durante una conferencia celebrada en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones

contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas. Además, las nuevas disposiciones deberán ser precisas, claras.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa" que se elaboro en la OCDE.

Como se ha analizado es importante la participación internacional para que exista una precisa delimitación de los delitos informáticos así como la definición de los mismos.

3.2 Situación jurídica en el Mundo.

No todos los países disponen de una legislación adecuada para enfrentarse con el problema de los Delitos Informáticos, sin embargo con objeto de que se consideren las medidas que han tomado algunos países respecto de tal problema es necesario considerar sus legislaciones para entender la panorámica mundial respecto del fenómeno de los Delitos Informáticos.

3.2.1 Legislación Internacional.

Estados Unidos, adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó al acta de Fraude y Abuso Computacional de 1986. La mencionada acta tiene por finalidad eliminar los razonamientos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, esta acta a su vez prevé la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C. Sec. 1030 (a) (5) (a). Es pues esta acta un adelanto significativo ya que la misma prevé directamente los actos de transmisión de virus así como de aquellos programas o comandos que pueden afectar la funcionalidad de sistemas informáticos, redes, computadoras etcétera.

El acta de 1994 hace una relevante distinción entre dos tipos de individuos que crean virus, para que estos sean tratados de manera distinta:

a. Los individuos que intencionalmente causan daño por la transmisión de un virus, serán castigados hasta con 10 años de prisión federal mas una multa.
b. Aquellos individuos que los transmiten sólo de manera imprudencial la sanción podrá ser administrativa siendo la imposición de una multa o en su defecto un año de prisión.

Esta distinción constituye un acercamiento responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo la conducta que será castigada, esto es relevante toda vez que de

definir a los virus, como se ha venido haciendo mención la tecnología informática cambia constantemente entonces de conceptualizar un virus pronto sería obsoleta tras un corto periodo de tiempo, porque pronto una nueva era de ataques tecnológicos a los sistemas informáticos podrá surgir.

En lo que se refiere a defraudaciones informáticas y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena administrativa y privativa de la libertad, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

El Estado de California adopto en 1992 la Ley de Privacidad la cual contempla los delitos informáticos, teniéndolos con sanciones por menores que los referentes a los delitos contra la intimidad, que son el principal motivo de la mencionada ley. Los legisladores del estado de California consideraron que la proliferación de las computadoras traería consigo la proliferación de delitos informáticos y que la protección legal en todos sus tipos y formas es de vital importancia para la protección de la intimidad de los individuos y el bienestar de las instituciones financieras, negocios, agencias gubernamentales y todas aquellas relacionadas con el estado de California que legalmente utilizan computadoras, sistemas y bases de datos.

Alemania, creó el 15 de mayo de 1986 la Ley Contra la Criminalidad Económica la cual consideró los siguientes delitos:

Espionaje de datos (202 a), estafa informática (263 a), falsificación de datos probatorios (269), el engaño jurídico mediante la elaboración de datos (270),

falsedad ideológica (271) uso de documentos falsos (273), alteración de datos (303 a), sabotaje informático (303 b) y la utilización abusiva de cheques o tarjetas de crédito.

Es relevante notar que no existe un apartado especial para los delitos informáticos sino que estos delitos los contempla dentro de una ley de carácter económico, previendo las hipótesis en las que se pueda cometer delitos de tal carácter económico.

Una ley aprobada en Japón en 1988, impuso multas de hasta 100 mil yenes a quien incumpla las regulaciones para la protección de datos o realice otros actos ilícitos relacionados con el procesamiento de datos.

Luxemburgo desde 1979 tenía contemplada distintas conductas típicas relacionadas con la obtención y procesamiento ilegal de datos, a las cuales les corresponden sanciones administrativas y privativas de la libertad hasta por un año.

La Gran Bretaña, a consecuencia de un caso de hacking ocurrido en el año de 1991, comenzó a regir en este país la Computer Misuse Act. (Ley de Abusos Informáticos). Dentro de esta ley el intento o la alteración de datos informáticos es castigada hasta con 5 años de prisión o multas. Esta ley contiene un apartado donde contempla la modificación de datos sin autorización considerándose dentro de este mismo apartado a los virus informáticos. La liberación de virus en la mencionada ley, tiene una sanción que van desde 1 mes hasta 5 años de prisión dependiendo del daño que este cause.

En Holanda el 1° de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, donde se castigan actos ilícitos como el hacking, preacking y la distribución de virus.

La ley de este país considera dos conductas respecto de la liberación de virus, la primera de estas dos es cuando se libera con toda la intención de causar daño con un virus informático, mismo que es sancionado con una que pueda llegar hasta los cuatro años de prisión de ser comprobada tal conducta, y en el segundo supuesto cuando un virus se escapa por error, mismo que si se comprueba tal conducta la pena no superaría el mes de prisión.

En enero de 1988, Francia dictó la Ley relativa al Fraude Informático, la cual prevé penas que van de los dos meses a los dos años de prisión así como una multa que oscila de 10 mil a 100 mil francos por la intromisión fraudulenta que suprima o modifique datos.

España por su parte creo un nuevo Código Penal de España, en su artículo 264 – 2 manifiesta que se impondrá la pena de 1 a tres años de prisión y multa "... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

Esta misma ley sanciona de forma detallada a quien cometa los delitos de violación de secretos, espionaje y divulgación, aplicándoles pena privativa de la libertad y administrativa, agravándolas cuando existe una intención dolosa, así mismo si estas conductas son cometidas por funcionarios públicos se penaliza con inhabilitación del cargo público.

En Austria dentro de la ley de reforma del Código Penal, sancionada el 22 de diciembre de 1987, en el artículo 148, castiga a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en la elaboración de datos de forma automática a través de la elaboración de un programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además sanciona de distinta forma a quienes cometen este delito utilizando su profesión de especialistas en sistemas.

Como se ha podido analizar, son numerosos los países que han contemplado conductas ilícitas cometidas a través de medios informáticos, y las han introducido dentro de sus cuerpos legales para que estos sean susceptibles de ser sancionados y no dejar a la sociedad en estado de indefensión cuando llegasen a ser victimas de un delito informático.

Es necesario notar que como en el caso de Gran Bretaña, fue necesario que sucediera un delito para que dicho país tomara cartas en el asunto, y no dejar sin castigar tales conductas.

De tal modo que no es necesario esperar a que cada país sea victima de un delito informático para que pueda comenzar a legislar al respecto, debe de considerarse que la consideración de un delito no solo es para la sanción del mismo sino para la prevención de que tales conductas por considerárseles perjudiciales a la sociedad. La preocupación internacional por el creciente problema con la tecnología informática, los ha motivado a que además de que dentro de sus leyes internas analicen dentro de las cumbres, convenciones y tratados internacionales el problema de los delitos informáticos.

3.2.2 Legislación Nacional.

Es necesario presentar la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los Delitos Informáticos. Es necesario recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

El tratado de Libre Comercio con América del Norte (TLCAN), es un instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, en la 6ª parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de

medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

El relevante el contenido del párrafo 1 del artículo 1717 titulado procedimientos y sanciones penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLCAN.

Así mismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Es relevante que en su párrafo 2 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.

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.

Es de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos

comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

De esta forma, cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos de autor había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado *"De los delitos en materia de derechos de autor"*.

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en 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, 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 de autor 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 que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las 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, es importante presentar los artículos 102 y 231. El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

Aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

Esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un Delito Informático debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los Delitos Informáticos el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etcétera.

Por otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

La redacción de estas fracciones prevén evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título

Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos de autor y de propiedad industrial, principalmente.

México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Como ejemplo tenemos el artículo publicado por la prensa en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Muchas personas sentirán que el país está ajeno a estas pérdidas por cuanto estas compañías no son mexicanas, sin embargo, si analizamos los sujetos que cometen estos delitos, según la nota de prensa, podríamos sorprendernos al saber que empresas mexicanas como TAESA y Muebles Dico enfrentan juicios administrativos por el uso de programas piratas.

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico.

En consecuencia por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

El Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información. Así, el acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

Asimismo, la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

Esta Ley, además establece en el Título X, en su capítulo único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultado para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

De esta forma, las modificaciones a la ley de derechos de autor permitieron incluir en su enunciado la expresión "fonogramas, videogramas o libros", además del verbo "reproducir", quedando el artículo 231 fracción III "...III Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".

Con las reformas al Código Penal en su artículo 424 Fracción III se especifica que "...A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, videogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos ".

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, es pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

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

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

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

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

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.

Debe de considerarse que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se quebrantan 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.

CAPITULO 4. EL FRAUDE INFORMÁTICO.

Una vez que se obtuvo una visión en general de los delitos informáticos es necesario centrarse al tema especifico del delito de Fraude Informático, por lo cual es necesario primeramente conocer el concepto de fraude así mismo tener una visión de los elementos del fraude genérico así como conocer algunos específicos para poder analizar los elementos que integran estas dos acepciones del Fraude en México, para poder tomar los elementos que constituyen este nuevo fraude especifico motivo de la presente tesis.

4.1 Concepto y Naturaleza Jurídica del Fraude.

El fraude a lo largo del tiempo ha tenido diferentes modos de cometerse en la actualidad la doctrina lo define tomando los elementos que de este surgen para comerte del mismo modo se obtiene que la legislación contempla elementos del mismo para que este pueda encuadrar en un código y así este sea típico, partiendo de esto entonces es necesario que analizar el concepto que la doctrina da del delito de fraude así como el que le da la código penal federal. Por otra parte se analizara la naturaleza jurídica del mismo.

4.1.1 Concepto de Fraude.

Para poder llegar al concepto jurídico y doctrinario del Fraude es necesario saber que este proviene del latín *fraus,* que significa engañar, usurpar, despojar, burlar con fraude; *fraudulentas,* equivalente a fraudulento, engañoso, fingido, falaz,

malicioso. Gramaticalmente es engaño o acción contraria a la verdad o rectitud. (Instituto de Investigaciones Jurídicas, 2000: 1469).

Es de suma importancia definir claramente el fraude genérico para determinar los elementos del mismo, partiendo de este principio es necesario retomar como se define jurídicamente dentro del Código Penal Federal vigente dentro de su Artículo 386 "...Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido".

Por otra parte el Código Penal del Estado de Michoacán dentro de su artículo lo define diciendo que "... Comete el delito de Fraude, quien engañando a alguien o aprovechándose del error en que éste se halla, se haga ilícitamente de alguna cosa o alcance un lucro indebido para sí o para otro.

La Suprema Corte de Justicia de la Nación ha resuelto lo siguiente "... el delito de Fraude porque fue sancionado el reo, se realizó mediante la concurrencia de los elementos que lo constituyen: a) un engaño o el aprovechamiento de un error; b) que el delincuente se haga ilícitamente de una cosa o alcance un lucro indebido; y c) relación de causalidad entre la actividad engañosa y la finalidad de obtener un lucro..." (6ª Época, t. XL, p. 40).

De Acuerdo a la noción doctrinaria penal, "...el fraude es un delito patrimonial que consiste, en términos generales, en obtener mediante falacias o engaños, o por medio de maquinaciones o falsos artificios de cosas o derechos ajenos". (González de la Vega, 1999: 244).

Se puede observar que tanto doctrinalmente como jurídicamente se observan dos puntos importantes: que se cometa por medio de engaños o artificios y la segunda que se obtenga un lucro indebido.

En conclusión de los conceptos antes manejados se obtiene que la esencia del delito de fraude, es el engaño de que se vale el agente, para hacerse en perjuicio de otro de un objeto de ajena procedencia.

4.1.2. Naturaleza Jurídica del Fraude.

Ya que se ha obtenido los elementos del concepto es necesario analizar la naturaleza jurídica del delito de Fraude, en razón tenemos que el delito de Fraude se encuentra regulado en nuestro Código Penal Federal, en el Capítulo III, Titulo Vigésimo segundo "Delitos en contra de las personas en su patrimonio", en el libro segundo.

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

Según el maestro Jiménez Huerta, los elementos son: a) Una conducta falaz; b) un acto de disposición; y c) un daño y un lucro patrimonial. (Jiménez Huerta, 1983: 159).

De lo anterior tenemos que el legislador considero que el delito de fraude se distinguía de los demás delitos patrimoniales por tener elementos particulares que lo hacen distinto de los demás de los cuales se distinguen la conducta engañosa y la disposición de algo que no le pertenece así como un lucro indebido.

4.2 Breve reseña histórica del delito de Fraude.

Cabe mencionar que desde tiempos remotos se ha hecho la distinción del delito de fraude ya que este se caracteriza por la astucia que presenta el sujeto activo al realizar su apoderamiento o obtención de un lucro indebido, sin tener que cometer un acto violento para la obtención de estos. En consecuencia resulta necesario conocer como se ha presentado el fraude a lo largo de la historia del ser humano.

Tenemos que las primeras manifestaciones del fraude surgen cuando es indispensable la tutela de la honestidad en las relaciones comerciales, tratando de evitarlas alteraciones de calidades, pesas y medidas.

El Código de Manú castigaba al que vendía grano malo por bueno, cosa vil por fragante, hierro por plata, etcétera; el Código de Hammurabi sancionó la falsificación de las pesas y medidas; las leyes Hebraicas castigaron a los que abusaban de los compradores necesitados; el Corán por su parte condenó a los que se aprovechaban de las condiciones o necesidades del comprador, sobre todo cuando esto era a precio mayor del adecuado

Por otra parte el Derecho Romano contemplo diversos crímenes como el *furtum*, el *falsum* y el *stellionatus*. El *furtum* se presentaba cuando alguien obtenía un dinero haciéndose pasar por acreedor, simulando la cualidad de heredero, asumiendo el nombre del procurador verdadero o fingiendo serlo, quien pedía dinero haciéndose pasar por pobre o quien en daño del vendedor entregaba al comprador un peso mayor del justo. El *falsum* fue aplicable a quien usaba el

nombre ajeno, simulando determinada caridad personal para alcanzar provecho y a quien vendía con diversos contratos a dos personas la misma cosa. El *stellion* que era un animal dotado de colores imprecisos y favorables a los rayos del sol, se aplicaba a todos aquellos delitos cometidos en perjuicio de la propiedad ajena, que fluctuaban entre la falsedad y el hurto.

El fraude alcanzó su desarrollo en el siglo XIX con la frecuencia e intensidad del tráfico mercantil, aun cuando se le da el nombre de estafa en otros códigos penales como el francés, alemán y español.

El Código Toscano determinó que incurre en ese delito el que sorprendiendo la buena fe ajena, con artificios, maniobras o ardides diversos de los específicamente mencionados, obtiene una ganancia injusta en provecho de otro.

Como es apreciable a lo largo de la historia universal el fraude se ha hecho presente, manifestándose en sujetos que utilizan la inteligencia para engañar a las personas y obtener de estos un beneficio ya sea desde la posesión de un objeto hasta un lucro indebido. Es apreciable y relevante hacer notar que las artimañas para cometer el delito de fraude según la época han ido cambiando, por tal motivo cada vez es más difícil su comprobación más no imposible. Por otra parte los medios para cometerlos hacen que aparezcan fraudes específicos, toda vez que de tenerse solo el supuesto del fraude genérico, innumerables conductas estarían siendo atípicas toda vez que la conducta no encuadraría dentro del fraude genérico, de ahí la necesidad de que se haya ido adecuando el código penal

federal agregándole fraudes específicos para que estos sean típicos y susceptibles de ser sancionados.

4.3 Sujetos del Delito de Fraude.

Dentro del delito de fraude encontramos dos tipos de sujetos que participan dentro de la conducta delictiva, el sujeto activo, quien comete la conducta antijurídica en perjuicio de otro, llamado sujeto pasivo. En esta razón describiremos cada uno de estos sujetos del delito de fraude.

4.3.1 Sujeto activo.

El sujeto activo en el delito de fraude genérico contemplado dentro del artículo 386, así como en los de fraude específico estipulado en el artículo 387 fracciones: I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XIV, XVIII, XIX; 388, 388 bis y 389 bis, será cualquier persona que engañe o se aproveche del error en que se encuentra otro, para hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido.

De acuerdo con el maestro Pavón Vasconcelos señala que sujeto activo es aquel que "... engaña o se aprovecha del error para hacerse ilícitamente de una cosa o bien, alcanza un lucro indebido". (Pavón Vasconcelos, 1986: 163).

En los casos de los Artículos 387 fracción XII, XIII y 389, serán respectivamente el fabricante, empresario, contratista o constructor de una obra cualquiera; el vendedor de materiales de construcción o de cualquier especie; los constructores o vendedores de edificios en condominio; quién tenga un cargo en el

gobierno en una empresa descentralizada o de participación estatal o de cualquier agrupación de carácter sindical, o que tenga relaciones con los funcionarios o dirigentes de dichos organismos.

4.3.2 Sujeto Pasivo.

En el delito de fraude genérico y en los específicos, con excepción del artículo 387, fracciones VII y XIX tercer párrafo, el sujeto pasivo puede ser cualquier persona, física o moral, quién sufre el daño patrimonial.

En cuanto al artículo 387 fracciones VII y XIX, párrafo tercero, los sujetos pasivos serán respectivamente: el primero o segundo comprador; las personas morales.

4.4. El Fraude Informático.

"Con el avance de las nuevas tecnologías, la informática se ha convertido en un instrumento que nos proporciona infinitas posibilidades de desarrollo y progreso. Sin embargo, se ha dado lugar a una nueva forma de delincuencia, la delincuencia informática, ya que esta tecnología pone a disposición del delincuente un abanico de nuevas técnicas y métodos para alcanzar sus propósitos criminales". Es así como comienza la exposición sobre el fraude informático de los autores chilenos Magliona y López, ellos mencionan que el fraude informático es uno de los fenómenos más importante dentro de la delincuencia informática, dado al creciente aumento de las manipulaciones

fraudulentas, y es por tanto la zona más inexplorada y la que mayores problemas enfrente en cuanto a su prevención, detección y represión.

Ya que se ha logrado estudiar el fraude en su acepción general desde el punto de vista jurídico y doctrinario es necesario centrarse en el tema especifico del presente trabajo el cual es el Fraude Informático, por tal motivo se analizara el concepto del presente delito, los elementos del mismo y los sujetos que participan dentro del delito de Fraude Informático.

4.4.1 Concepto de Fraude Informático.

Para el tratadista Romeo Casabona el fraude informático, es "...la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero".

Como es notorio lo sobresaliente de tal concepto elaborado por el tratadista español consiste en que la acción del sujeto activo vaya encaminada a la modificación del resultado de un procesamiento automatizado de datos, para así lograr un enriquecimiento injusto en detrimento del patrimonio de un tercero, hay una apropiación ilícita de dinero, bienes o servicios ajenos.

Por lo tanto el concepto de Fraude Informático será "El conjunto de conductas dolosas, que valiéndose de cualquier manipulación fraudulenta, modifiquen o interfieran el funcionamiento de un programa informático, sistema

informático, sistema telemático o alguna de sus partes o componentes, para producir un perjuicio económico del cualquier índole".

Por último cabe mencionar que en el fraude informático, existe la utilización de un medio fraudulento para la comisión de la infracción que es, a saber, la manipulación informática fraudulenta y que la intención del agente va dirigida en primer lugar a causar un perjuicio económico a la víctima y en segundo lugar está el ánimo de lucro con el cual este actúa.

4.4.2 El carácter "informático" del Fraude.

Una vez que se tiene la noción del concepto de Fraude Informático es de suma importancia el desglosar, por qué Fraude informático, por tal motivo es menester decir en cuanto al carácter "informático" del Fraude.

Al respecto el Doctor Santiago Acurio del Pino nos refiere que "...lo informático del Fraude está en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera, subrepticia... con animus decipiendi". Por lo tanto el carácter informático del fraude alude al instrumento informático con cuyo auxilio se efectúa la defraudación. Es decir, el fraude informático adquiere esta separación de las demás formas de defraudación por la manera de lograr la defraudación a través o por medio de medios informáticos, entendiéndose por estos como los sistemas informáticos conocidos como computadoras personales, caseras, redes internas y externas como la Internet, la comunicación satelital, etcétera.

En tal virtud para que se hable de defraudación informática esta debe tener las notas características y configuradoras de una defraudación, es decir que debe existir la causación de un perjuicio económico, irrogado mediante un comportamiento engañoso, astuto, artero, o sea un, medio fraudulento que en este caso sería la propia manipulación informática.

Para los autores Magliona y López esto es muy importante ya que ayuda a distinguir el fraude informático de otros hechos delictivos, que no obstante ser realizados por medios informáticos, no constituyen defraudaciones, por ejemplo, atentados contra la intimidad cometidos por medio de manipulaciones informáticas. A este respecto Marcelo Huerta y Claudio Líbano señalan que la finalidad perseguida por el sujeto activo, es la que condiciona el tipo de delito que se produce, ya que para ellos las manipulaciones informáticas se aplican a todos los delitos informáticos.

Al respecto cabe mencionar que si bien la finalidad del sujeto activo ayuda a saber que tipo de delito se comete, así como el aprovechamiento de las características y peculiaridades de los sistemas de procesamiento automatizado de datos es una característica común en todos los delitos informáticos, dichos supuestos no pueden cambiar la naturaleza del hecho delictivo en tal razón y siguiendo a la tratadista española Gutiérrez Frances que al respecto dice "...nada será defraudación informática sin ser antes defraudación".

CONCLUSIONES.

La inquietud que motivo a la realización del presente estudió estriba en que actualmente en nuestro país no existe un apartado en nuestro código penal Federal donde se clasifiquen los Delitos Informáticos, ni mucho menos pensar que existe una clasificación para el Fraude Informático, por lo tanto, al encontrarse esta conducta actualmente atípica nos encontramos en una situación donde se deja desprotegido al gobernado por no encontrarse reguladas tales conductas antijurídicas. Partiendo de ese principio se elaboro un objetivo general que dice a la letra: "Analizar como el Derecho Informático es una herramienta jurídica, para tipificar los delitos informáticos en México".

De acuerdo con esto , el presente trabajo de investigación partió de la necesidad de saber que es el derecho informático del cual se obtuvo que esta permite dar un conocimiento al licenciado en derecho sobre del tema informática ya que como se preciso a lo largo del presente trabajo esta rama jurídica trata directamente al derecho y a la informática cosa que pareciera desde un punto de vista imposible de relacionar; pero esto no es así toda vez que esta rama jurídica nos permite visualizar el campo de la informática y como la podemos relacionar con la vida cotidiana de los seres humanos en sociedad ya que como se ha manejado hoy en día la mayoría de las actividades humanas se encuentran vinculadas directamente con la informática.

Por lo tanto tenemos que esta rama jurídica permitirá al licenciado en derecho no solo la posibilidad de interrelacionar al derecho con la informática sino, crear normas afines a las necesidades de la sociedad por la evolución que esta va

adquiriendo con el paso de los años, y que estas normas no solo sean creadas por crearse sino que realmente tengan una aplicación real en la vida humana ya que la finalidad de vivir bajo un sistema de normas, es buscar que estas reglas permitan vivir armónicamente al hombre en sociedad.

Ya que el Derecho Informático permitió tener una visión de cómo esta afectando los avances tecnológicos a la vida ordinaria del ciudadano, se debe hacer notar que así como existen cambios en el actuar del hombre también existen nuevas formas de cometer delitos, gracias a la ayuda que le proporciona los mismos avances tecnológicos, donde el sujeto activo busca cada vez mas la manera de que este no pueda ser detectado en la comisión de un delito, es de ahí que hoy en día los delincuentes hacen uso de la informática para poder cometer sus delitos, pero es necesario adecuar nuestra legislación penal para no quedar desprotegidos de tales conductas delictivas.

De ahí surge la necesidad de identificar que tipos de delitos informáticos han sido detectados y que clasificación se les ha logrado dar jurídicamente en otros países. Así como otros países se encuentran adelantados tecnológicamente, lo mismo se encuentran en la rama jurídica, razón por la cual podemos aprender de estas sus aciertos tanto como sus errores para poder crear normas afines a las necesidades que presenta el país actualmente.

A mi criterio, el tipo penal que mas esta propenso a ser cometido hoy en día es el Fraude Informático , ya que existen personas que su capacidad intelectual la destinan a buscar nuevas maneras de hacerse de dinero sin que estos trabajen por hacerse merecedores a este dinero. Los fraudes informáticos son fáciles de

cometer para aquellos con los suficientes conocimientos informáticos para cometer tal delito, ya que estos pueden ser realizados desde el interior de una red informática, como desde el exterior solo teniendo acceso a la información de la base datos los cuales puedes ser susceptibles de ser modificados, pudiendo engañar al dueño de tal información para desposeerlo de sus bienes económicos.

PROPUESTA.

La propuesta que se brinda está planteada en virtud de la necesidad de actualizar nuestra legislación añadiendo una fracción más al Artículo 387 Capitulo III del Titulo Vigésimo Segundo; el cual a la letra diría:

ARTICULO 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

XXII.- Al que por cualquier medio informático con ánimo de lucro, valiéndose de engaños o artimañas perjudique en el patrimonio de otra persona, modificando o introduciendo datos falsos en un sistema informático para su beneficio.

Es necesario mencionar que para considerarse un tipo de fraude se deberá considerar los siguientes elementos:

- Exista un ánimo de lucro.
- Que por medio de engaños o artimañas se perjudique patrimonialmente a un individuo.
- Y el que lo hace peculiar es que se realice por medio de un sistema informático.

BIBLIOGRAFIA.

Bisquerra, Rafael (1989)
Métodos de Investigación Educativa
Editorial CEAC

CARRANCA y Trujillo, Raúl, CARRANCA y Rivas, Raúl (1991)
Derecho Penal Mexicano
Editorial Porrúa.

CORREA, Carlos, PAGANO, Rodolfo, LOSANO, Mario, BERGEL, Salvador. (1988)
*Informática y Derecho. Aportes de Doctrina Internacional. Volumen 2
Ed. Depalma, Buenos Aires.

DEPALMA, Alfredo y Ricardo (1998)
*Informática Jurídica.
Ed. Astrea.

DUFFY, Tim (1993)
Introducción a la Informática.
Grupo editorial Ibero América.

FERNANDEZ PEÑA, Juan (1998)
Informática I
Ed. Nueva Imagen S.A. de C. V.

GAROFALO, R. (1999)
Criminología: Estudio sobre el Delito y la teoría de la represión.
Ángel Editor.

GONZALEZ, Moreno Rafael (1999)
Introducción a la Criminalística
Editorial Porrúa.

HUERTA MIRANDA, Marcelo (1989)
Los Delitos Informáticos.
Editorial Jurídica Cono del Sur.

Instituto de Investigaciones Jurídicas UNAM. (2000)
Diccionario Jurídico Mexicano
Editorial Porrúa.

LOPEZ BETANCOURT, Eduardo (1998)
*Delitos en Particular.
Ed. Porrúa.

MAGLIONA MARKOVICTH, Claudio LOPEZ MEDEL, Macarena (1999)
Delincuencia y Fraude Informático.
Editorial Jurídica de Chile.

PARKER, C. S (1986)
Introducción a la Informática
McGraw – Hill

PAVON, Vasconcelos Francisco (1999)
Diccionario de Derecho Penal.
Editorial Porrúa.

PINA Vara, Rafael. (1998)
Diccionario de Derecho
Editorial Porrúa.

ROMEO CASABONA, Carlos Maria (1987)
Poder Informático y Seguridad Jurídica
Editorial Fundesco, Madrid, España.

TELLEZ VALDEZ, Julio (1996)
Derecho Informático.
Ed. McGraw – Hill.

TELLEZ VALDEZ, Julio (1988)
Contratos, riesgos y seguros informáticos.
Instituto de Investigaciones Jurídicas Serie G
Estudio Doctrinales, Núm. 117.

Direcciones Internet
http://www.ambito-juridico.com.br/aj/dp0019.htm

http://www.cni.org/Hforums/cni-copyright/1998-04/1074.html

http://tiny.uasnet.mx/prof/cln/der/silvia/

http://www.juridicas.unam.mx/publica/rev/boletin/cont/79/bib/bib21.htm

http://www.geocities.com/delincuentes_digitales/crimenes.htm

http://www.aadat.org/delitos_informaticos20.htm

http://www.unifr.ch/derechopenal/articulos/pdf/Montano1.pdf

http://www.pnp.gob.pe/culturales/revista_81/pag_36_40.pdf