00721
392

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

"LA NECESIDAD DE LA REGULACIÓN DEL FRAUDE INFORMÁTICO EN NUESTRA LEGISLACIÓN PENAL LOCAL."

T E S I S

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO

P R E S E N T A:
GLORIA CARMEN HEREDIA GARCÍA

ASESOR:
DOCTORA ANA ELOISA HEREDIA GARCÍA

MÉXICO, D.F . 2003

a

A DIOS:

Le Agradezco Por Haber Iluminado Mi Camino Hasta La Terminación De Mi Carrera, La Cual No Hubiese Logrado Sin Su Ayuda.

A MIS PADRES:

LIC. MARIO JOSE HEREDIA BOFILL
Y
GLORIA GARCIA DE HEREDIA

Les Agradezco, Su Amor, Comprensión, Ayuda, Apoyo Y Confianza Que Me Han Demostrado En Todo Momento, Siendo Mi Orgullo Y Un Ejemplo A Seguir, Gracias Por Su Enorme Dedicación Que Al Lado De Sus Sabios Consejos Han Sido Esenciales Para La Culminación De Mi Carrera.

A MIS HERMANOS.

JORGE CARLOS HEREDIA GARCIA
ANA ELOISA HEREDIA GARCIA
MARIO JOSÉ HEREDIA GARCIA

Gracias A Su Lealtad Y Amistad Que Me Han Ayudado A Seguir Adelante En Mis Convicciones Y Porque Aunado A Todo Ello Siempre Mantengamos La Unión, Cariño Y Ayuda Que Hasta El Momento Ha Existido.

A MI PETIT

MIGUEL ANGEL ALVARADO ROSAS.

Gracias, Por Tu Confianza, Apoyo Y Amor, Que Haz Demostrado En Todo Momento Hacia Mi, Y Por El Gran Estimulo Que Me Haz Dado Para Alcanzar Cada Una De Mis Metas & Ilusiones.

e

A MIS SERES QUERIDOS QUE HAN DEJADO ESTA VIDA.

JOSÉ MARIO HEREDIA GARCIA
ANA MARIA CÓRDOBA CURTIS
JERÓNIMO HEREDIA TRUEBA

A LA DOCTORA
ANA ELOISA HEREDIA GARCIA

Le Agradezco El Apoyo Y Consejos Que Me Han Brindado Para La Elaboración De La Presente Investigación, Así Como Por Su Valiosa Amistad.

A MIS
MAESTROS
Con Todo Respeto.

A MIS AMIGOS:
Por Sus Estímulos.

A La Universidad
Nacional Autónoma
de México y a La
Facultad De
Derecho.

"La información significa poder, poder que puede ser objeto de dominio y de control sobre quien no lo detenta"

(Claudio Paul Magliona Markovicth)

"La criminalidad informática es una forma nueva de criminalidad denominada de cuello blanco o de calzones cortos. Esta modalidad ha sido calificada como una subespecie de la llamada criminalidad económica"

(María Fernanda Guerrero M.)

ÍNDICE

INTRODUCCIÓN.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y. condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente, el progreso cada día es más impresionante ya que nos permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza al alcance concreto de millones de interesados y de usuarios, este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas, por ello la informática es hoy una forma de poder social.

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el fraude informático y la forma en que esta siendo regulada, esta problemática en México además del evidente incremento de esta situación es necesario a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países, por ello propongo regular penalmente las conductas ilícitas derivadas del uso de la computadora, como en la presente investigación expondré.

En primer término la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general contribuirá notoriamente al

nivel de concientización sobre el problema que nos ocupa, en esta investigación el siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar este tipo de conductas ilícitas.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente 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. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente 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.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación

en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"

Esta marcha de las aplicaciones 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 espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje

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

La delincuencia informática, y en especial el fraude informático, es una realidad y el desconocer este fenómeno solo hará más fácil la labor de los delincuentes, la defensa contra este tipo de delincuencia puede provenir de dos ámbitos, el legislativo y el técnico, la defensa legislativa debe desplegar toda su capacidad para abarcar las nuevas figuras, a fin de reprimirlas, con pleno respeto al principio de legalidad, por su parte la defensa técnica consiste en medios de prevención, descubrimiento y prueba del ilícito informático, tomando siempre como base en la presente investigación que el bien jurídico tutelado en el fraude informático es primordialmente el patrimonio y la información, por lo que se propone que en él titulo vigésimo segundo que se refiere a "LOS DELITOS EN CONTRA DEL PATRIMONIO" del Código Penal del Distrito Federal y el titulo décimo quinto referente a "DELITOS CONTRA EL PATRIMONIO" del Nuevo Código Penal para el Distrito Federal, se añada un artículo que haga referencia al fraude informático, ya que debido a la ausencia de esta figura en concreto da lugar a que los autores de esos hechos queden impunes ante la comisión de ese acto delictivo, y que en caso de la inexistencia que hay sobre el tema obligue a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos

En el cuerpo de la presente investigación se darán las bases históricas en las que fundo y motivo la causa por las que pretendo que el fraude informático se tipifique en nuestro Código Penal del Distrito Federal, así como proporcionar el

marco teórico de dicha fundamentación, se tratara de delimitar el llamado fenómeno de la delincuencia informática, a través del análisis de los conceptos existentes sobre éste, el estudio incluirá además diversas clasificaciones doctrinarias que se hacen respecto de las conductas que lo componen, como así mismo el de las características de estos hechos delictivos, de los sujetos que intervienen (el delincuente informático y el sujeto pasivo) y en especial del bien jurídico protegido. Así mismo analizare como la legislación de diversos Estados y países, han emitido sobre el tema y sobre todo marcando legalmente, y analizare con un fundamento constitucional en que bases me baso para fundamentar dicha pretensión, de igual manera describo la problemática que se suscita en la actualidad tanto a nivel mundial, como en los estados de la república y en especial en el Distrito Federal a causa del fraude informático, y por último hago un análisis propositivo de las razones por como pretendo se regule en el Código Penal del Distrito Federal al fraude informático, y de que manera debería insertarse en el mismo dicho precepto legal.

CAPITULO I

MARCO HISTÓRICO DE LOS DELITOS INFORMÁTICOS

1.1. - ANTECEDENTES DE LA INTERNET

1.1.1. - LA INFORMÁTICA.

La naturaleza ha dotado al ser humano de diversas habilidades entre las que merecen destacarse la capacidad de abstracción y la posibilidad de realizar cálculos matemáticos complejos; estas habilidades no hubieran podido progresar, en la medida en que lo han hecho, si el hombre se hubiera visto obligado a realizar todos esos laboriosos cálculos mentalmente o con la única ayuda de sus diez dedos.

Debido a ello, la humanidad se vio empujada, desde la antigüedad, a tener que ayudarse en sus cálculos de diversas maneras, las tablas de arcilla que se borraban frotando sobre ellas y las cuentas o conchas de diversos pueblos que a lo largo de todo el planeta, facilitaron el comercio y los intercambios.

1.1.1.1.- EL ÁBACO

En la historia de la humanidad el ábaco fue la primera herramienta de cálculo diseñada y construida por el hombre para ese propósito especifico que le ayudo. De forma significativa, en la tarea de realización de operaciones matemáticas.

"Quizás fue el primer dispositivo mecánico de contabilidad que existió. Se ha calculado que tuvo su origen hace al menos 5000 años y su efectividad ha soportado la prueba del tiempo."[1]

[1] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, http://www.Fisc.utp.ac.pa/museo/historia.htm. fecha de consulta 28/VII/2002,

1.1.1.2.- EL ARITMÓMETRO.

Blaise Pascal inventó una máquina calculadora llamada, aritmómetro en el año 1642, cuando solo tenia dieciocho años de edad, esta calculadora únicamente podía sumar y restar.

"La máquina de pascal se componía de una serie de ruedas dentadas que giraban unidas entre sí, cada una de estas ruedas formaban las unidades, decenas, centenas, etc., cuando al girar la rueda se completaban las diez unidades, en que se dividía cada una de las ruedas hacían girar, por medio de sus dientes, la rueda que formaba la unidad inmediatamente superior, y así sucesivamente hasta que se completaba la operación, el resultado se leía mediante el número que se formaba con cada uno de los dígitos de las diferentes ruedas."[2]

1.1.1.3.- LAS TARJETAS PERFORADAS.

A principios del siglo XIX, la primera revolución industrial estaba en su apogeo, uno de los mayores negocios en los países industrializados eran los tejidos que se realizaban en los telares mecánicos accionados por máquinas de vapor. Los telares mecánicos eran, evidentemente, de mucho más fácil manejo que los manuales, ya que el operario sólo tenia que controlar el hilado del tejido, el problema que tenían los industriales era que este control era una operación muy repetitiva que daba lugar a que los operarios tuvieran frecuentes errores en el control de la producción del tejido retrasando y deteriorando su fabricación en una gran cantidad de piezas.

"En 1805 Joseph Jacquard inventó un telar automático controlado por tarjetas perforadas para agilizar y mejorar la producción de los telares ingleses, las tarjetas de jacquard permitieron realizar las operaciones de hilado de tejido sin errores y por

---

[2] Enciclopedia de Informática y Computación, Tomo ***HARDWARE***, Madrid, España, 1997, Pág. 1

consiguiente se agilizó la producción y se controlaron y disminuyeron los problemas existentes hasta esos días "[3],

1.1.1.4.- LA MAQUINA ANALÍTICA.

"En 1835 Babbage propuso una versión mejorada de su máquina diferencial a la que denominó máquina analítica y que utilizaba como entrada de datos y órdenes del sistema las tarjetas perforadas que se diseñaron para manejar los telares ingleses"[4]

El problema al que tuvo que enfrentarse el constructor en este caso fue que en cierta medida se había adelantado a su tiempo y no conseguía resolver problemas para los que la tecnología existente en ese momento no tenia soluciones. la máquina analítica se componía de:

"Un subsistema de entrada/salida de la información a procesar en la máquina, un mecanismo de cálculo que servia para realizar las operaciones solicitadas, una memoria que permitía almacenar números para su posterior manipulación, el mecanismo que utilizaba era totalmente mecánico y este era controlado por las órdenes que suministraban las tarjetas perforadas."[5]

"Charles Babbage (1793-1871), visionario inglés y catedrático de Cambridge, hubiera podido acelerar el desarrollo de las computadoras si él y su mente inventiva hubieran nacido 100 años después. El adelantó la situación del hardware computacional al inventar la "máquina de diferencias", capaz de calcular tablas matemáticas. En 1834, cuando trabajaba en los avances de la máquina de diferencias Babbage concibió la idea de una "máquina analítica". En esencia, ésta era una computadora de propósitos generales. Conforme con su diseño, la máquina

---

[3] Op, cit, Enciclopedia de Informática y Computación, Tomo ***HARDWARE***. Pág. 7.
[4] Enciclopedia Encarta, Microsoft, 1999, "***INFORMÁTICA***".
[5] Op, cit, Enciclopedia de Informática y Computación, Tomo ***HARDWARE***, España, 1997.Pág. 9

analítica de Babbage podía sumar, substraer, multiplicar y dividir en secuencia automática a una velocidad de 60 sumas por minuto. El diseño requería miles de engranes y mecanismos que cubrirían el área de un campo de fútbol y necesitaría accionarse por una locomotora. Los escépticos le pusieron el sobrenombre de "la locura de Babbage". Charles Babbage trabajó en su máquina analítica hasta su muerte. Los trazos detallados de Babbage describían las características incorporadas ahora en la moderna computadora electrónica. Si Babbage hubiera vivido en la era de la tecnología electrónica y las partes de precisión, hubiera adelantado el nacimiento de la computadora electrónica por varías décadas. Irónicamente, su obra se olvidó a tal grado, que algunos pioneros en el desarrollo de la computadora electrónica ignoraron por completo sus conceptos sobre memoria, impresoras, tarjetas perforadas y control de programa de secuencia." [6]

1.1.1.5.- COMPUTADORAS MECÁNICAS.

Hasta finales del siglo XIX no se realizaron nuevos avances en calculadores mecánicos, fue entonces cuando en 1887 León Bolleè invento una máquina de multiplicar diseñada para realizar la operación de la multiplicación directamente, sin recurrir a la repetición de sumas.

Pero el gran avance de lo que ahora se llama informática se produjo cuando, a finales de la década de los ochenta del siglo XIX, el gobierno de los Estados Unidos convocó un concurso para la compra de una maquinaria que permitiera tabular el censo que se realizaba cada diez años a lo largo de todo el país. En aquel momento los estadounidenses tenían un grave problema, ya que con los medios convencionales de que disponían todavía no habían conseguido realizar la tabulación completa del censo realizado sino hasta "el año 1880, el concurso lo ganó la

---

[6] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, http://www.Fisc.utp.ac.pa/museo/historia.htm. fecha de consulta 28/VII/2002

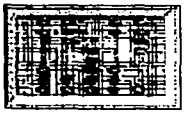
máquina tabuladora de Hermann Hollerith, quien realizó la tabulación del censo de 1890 y consiguió completarlo en tres años"[7].

1.1.1.6.- PRIMEROS ORDENADORES

Los ordenadores analógicos comenzaron a construirse a principios del siglo XX, los primeros modelos realizaban los cálculos mediante ejes y engranajes giratorios, con este tipo de máquinas se evaluaban las aproximaciones numéricas de ecuaciones demasiado difíciles como para poder ser resueltas mediante otros métodos, durante las dos guerras mundiales se utilizaron sistemas informáticos analógicos, primero mecánicos y más tarde eléctricos, para predecir la trayectoria de los torpedos en los submarinos y para el manejo a distancia de las bombas en la aviación. Lo que dio paso a los primeros ordenadores electrónicos, se creo un prototipo del calculador e integrador numérico electrónico (en inglés ENIAC *Electronic Numerical Integrator and Computer.*

" En 1945, el ENIAC, que según se demostró se basaba en gran medida en el ordenador Atanasoff-Berry (en inglés ABC, *Atanasoff-Berry Computer*), obtuvo una patente que caduco en 1973."[8]

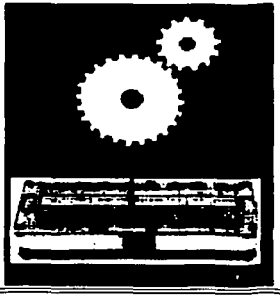
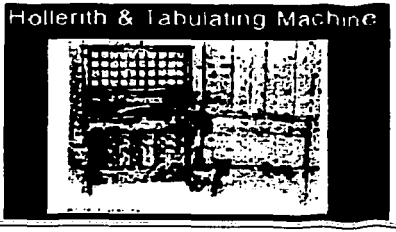
"Evolución de las Máquinas [9]

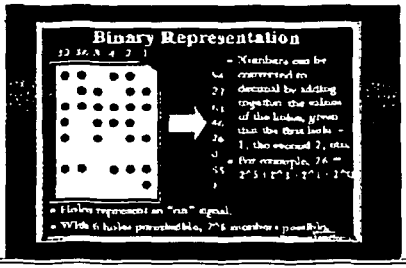
NOMBRE	AÑO	AUTOR	CARACTERÍSTICA
ÁBACO 	5000 años atrás		Se utiliza en la educación, principios de conteo aritmético.

7 Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, http://www.Fisc.utp.ac.pa/museo/historia.htm. fecha de consulta 28/VII/2002.

8 Enciclopedia Lafer, Editorial Reymo, España, 1988 Págs. 34-35.

9 Última actualización 27/08/98 Por Eduardo Salcedo, Referencia: Long Larry; **"Introducción a las Computadoras y al Procesamiento de la Información"**; Cuarta Edición; Prentice Hall; México 1995, pp. 295-310.Joyanes A. Luis; **Metodología de la Programación"**; McGrawHill; México; 1988;pp 55-56. http://w3.mor.itesm.mx/~issalced/histo1.html fecha de consulta 28/VII/2002

PASCALINE 	1642	Blas Pascal	Solo sumar y restar, ocupa una caja de zapatos. Su diseño se utilizó en las calculadoras mecánicas de los años 60's y se volvieron obsoletas al seguir las calculadoras electrónicas. (Leonardo de Vince tuvo una visión 150 años antes.
M. DIFERENCIAL 	1822	Charles Babbage	Calcula tablas matemáticas impulsada con vapor, no fue terminada y se corto el presupuesto en 1842; tenía 2 m de alto, 3 m de longitud y 4000 partes, pesando 3 ton.
M. ANALÍTICA	1833	Charles Babbage	Incluía una unidad de almacenamiento 60op/min. Era impulsada por una locomotora y ocupaba un campo de Fútbol.
	1835-50	Lady Ada Augusta Lavolace	Ayuda a Babbage, es hija de Lord Byron y fue considerada la primer mujer programadora en Tarjetas perforadas.
M. TABULADORA	1887-90		Máquina tabuladora con tarjetas perforadas, acumulaba y clasificaba la información. Se utilizó para el censo de 1890 y le redituó 40,000 dólares y el Gobierno de los Estados Unidos se ahorro 5 millones de dólares.

		Hernan Hollerith	En 1896 Hernan fundó la Tabulating Machine Company que se fusionó en 1911 con otras para crear Computing-Tabulating-Recording Company. En 1924 el director general Thomas J. Watson, cambió su nombre a *International Busines Machines Corporation IBM.*
ERA DE EAM 	20's a 50's	------	Tecnología a base de tarjetas perforadas, *Electromechanical Accounting Machine* (Máquina de Contabilidad Electromecánica. Llegaron a utilizar carretillas para transportar las tarjetas.
Z3	1941	Konrad Zuse	Construyo la primera computadora programable y resolvía ecuaciones complejas de ingeniería, fue controlada por tarjetas perforadas, y fue la primera que operó con el sistema binario, comparado con otras decimales.
MARK I 	1944	Howard Aiken	1a computadora electromecánica, 17 m largo y 2.5 m de alto. Un adelanto significativo, pero IBM no creía que sustituiría a la de tarjetas perforadas.

ENAC 	1946	J. Presper Eckert John W. Mauchly	Electronic Numerical Integrator and Computer (Integrador Numérico Electrónico y Computadora). Se utilizó en la 2a Guerra Mundial en cálculos balísticos. Su tamaño fue de 1400 m2, 30 ton y de 1800 tubos al vació; cuando funcionaba dejaba sin electricidad a Filadelfia.
EDVAC 	1945	John von Newman	Trabajo con Eckert y Mauchly para su construcción. Él estableció la base del programa almacenado, donde es fundamental para el futuro de las computadoras. El avance primario fue el proveer a la máquina de transferencia de control condicional y por almacenar todas las instrucciones del programa junta con los datos en la misma unidad de memoria. Este grupo incluyo en sus equipos memoria *RAM*.
UNIVAC	1951	J.Presper Eckert John W. Mauchly	*Universal Automatic Computer* (Computadora Automática Universal) Se diseño para la oficina de censos. Utilizó bulbos. Pronóstico la victoria de Dwight Eisenhower sobre Adlai Stevenson con solo un 5% de votos contados

1.1.1.7. GENERACIONES DE COMPUTADORAS.

1941-1948, PRIMERA GENERACIÓN DE COMPUTADORAS (LAS VÁLVULAS)

Las computadoras construidas con válvulas de vació son la primera generación de lo que en la actualidad se conoce como computadoras, las primeras computadoras de válvulas de vació se distinguían por dos aspectos fundamentales: su gran tamaño, el gran consumo de energía que disipaba un fuerte calor.

El tamaño de la máquina era una exigencia de la tecnología de construcción ya que las válvulas generaban mucho calor y debían separarse lo más posible para poder disipar convenientemente el calor.

1948-1962; LA SEGUNDA GENERACIÓN DE COMPUTADORAS. (LOS TRANSISTORES)

"Las computadoras de la segunda generación vieron como algo cambiaba en su interior, en efecto, a finales de la década de los años cuarenta, Schockley, Brattain y Barden inventaron, en los laboratorios *Bell*, el transistor cuyo nombre procede de la contracción "*Transference resistor*", es decir, resistencia de transferencia, rápidamente se vieron las grandes posibilidades que el nuevo descubrimiento tenía como sustituto óptimo de las válvulas".[10]

En esta etapa se consigue simultanear el proceso del programa con las operaciones de entrada y salida, pero solamente dentro del mismo programa al no poderse realizar más que una ejecución de un programa, al mismo tiempo, esto detenía el proceso de otros programas, todo ello originaba un ambiente obsoleto de los elementos más rápidos y, por tanto, más caros, de la máquina y una considerable pérdida de tiempo y dinero.

---

[10] Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, http://www.Fisc.utp.ac.pa/museo/historia.htm. fecha de consulta 28/VII/2002

1962-1971; TERCERA GENERACIÓN DE COMPUTADORAS. (LOS CIRCUITOS INTEGRADOS)

El paso de la segunda a la tercera generación de computadoras se produjo a principios de la década de los sesenta y se debió a la aparición de los circuitos integrados.

"Los circuitos integrados tienen un tamaño similar al de un transistor, pero el grado de miniaturización de sus componentes es muchísimo mayor, pudiéndose incluir la ponencia de varios transistores en un solo circuito de menor tamaño que el de un transistor."[11]

En esta tercera generación de computadoras se introdujo el concepto de multitarea, la cual consiste en una optimización de la utilización de los componentes del sistema Informático, la tendencia actual de los fabricantes es seguir aumentando la escala de integración de los circuitos para conseguir mejorar los rendimientos de los sistemas informáticos (en la actualidad se están consiguiendo tiempos de conmutación del orden de un nonasegundo).

LA CUARTA GENERACIÓN 1971 A 1988.

Dos mejoras en la tecnología de las computadoras marcan el inicio de la cuarta generación, el reemplazo de las memorias con núcleos magnéticos, por las de clips de silicio y la colocación de los circuitos electrónicos, el tamaño reducido del microprocesador de chips hizo posible la creación de las computadoras personales (*PC*)

El término *PC* se deriva de que para el año de 1981, IBM, saco a la venta su modelo *IBM PC*, la cual se convirtió en un tipo de computadora ideal para uso personal, de ahí que el término "*PC*" se estandarizó y los clones que sacaron posteriormente otras empresas fueron llamados *PC y compatibles*, usando

[11] Generaciones de Computadoras WWW. geocities.com, Informática, fecha de consulta 20/06/2002.

procesadores del mismo tipo que las *IBM*, pero a un costo menor y pudiendo ejecutar el mismo tipo de programas, Existen otros tipos de microcomputadoras, como *la Macintosh*, que son compatibles con *IBM*, pero que en muchos de los casos se les llaman también *(lipc, S119)* por ser de uso personal.

MICROPROCESADOR.

El primer microprocesador fue el *intel 4004*, producido en 1971, se desarrollo originalmente para una calculadora, y resultaba revolucionario para su época.

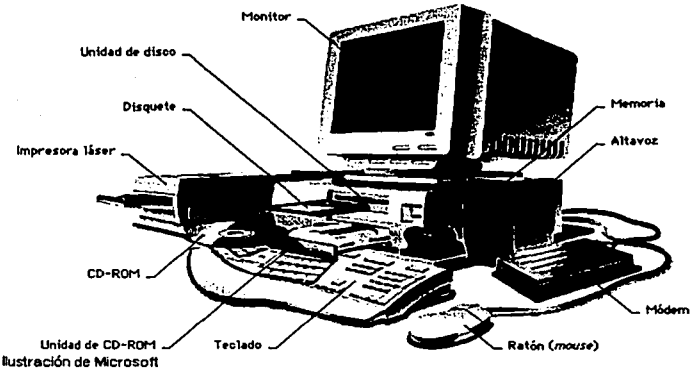


Ilustración de Microsoft

QUINTA GENERACIÓN (1983- ALA ACTUALIDAD) LA INTELIGENCIA ARTIFICIAL.

La inteligencia artificial es el campo de estudio que trata de aplicar los procesos del pensamiento humano usados en la solución de problemas en la computación.

"La Robótica es el arte y ciencia de la creación y empleo de robots"[12], un robot es un sistema de computación híbrido independiente que realiza actividades físicas y de cálculo, están siendo mejorados con inteligencia artificial, para que puedan responder de manera más efectiva a situaciones no estructuradas.

Evolución de las Generaciones de Computadoras [13]

Gen	Año	Característica	Descripción
1a	1951	Bulbos	Sin soporte de programación, memoria de tambor magnético y tubos al vacío se considera a la *UNIVAC* I (Universal *Automatic Computer*) como la primera y se utilizó en el censo de EUA en 1951, Otros modelos son IBM-650, IBM-701.
2a	1959-64	Transistor	Más potentes y confiables, menos costosas con soporte de programación, memoria de núcleos magnéticos. Comienzan las familias de computadoras IBM 1401, 1410 y 1440. *Burroughs, UNIVAC, NCR, CDC y Honeywell (BUNCH group).*
3a	1964-70	Circuitos integrados	Con soporte de programación, forma modular IBM-360, *Spectra*-70.
4a	1971	Microcircuitos Chip de memoria	Mejoras en equipo y programas. Tamaño de escritorio, mayor velocidad y memoria. HP 300, IBM 4341, Cray, IBM 9000.
5a	1983	Microprocesador Chip de memoria Microminiaturización	Diseño de nuevas arquitecturas con procesamiento en paralelo y circuitos de gran velocidad.

[12] Generaciones De Computadoras. WWW. geocities.com, Informática, fecha de consulta 20/06/2002.

[13] Introducción a las Computadoras y al Procesamiento de la Información http://w3.mor.itesm.mx/~lssalced/histo3.html, fecha de consulta 28 /VII/2002,

1.1.2. - INTERNET.

La primera de las preguntas que toda persona se hace cuando no se encuentra familiarizada con la Internet, o que maneje el mismo en forma relativamente especifica o de manera efímera seria la de ¿QUE ES LA *INTERNET*?:

Internet es una gran cantidad de pequeñas redes de computadoras y otras no tan pequeñas que se localizan de una manera interconectadas entre sí, y estas redes se encuentran distribuidas por todo el mundo, en la que se puede encontrar información y servicios de todo tipo, para acceder a todo tipo de información, las cuales requieren herramientas para su acceso que permiten una manera rápida a través de las computadoras.

En los últimos años se ha hecho un enorme esfuerzo para hacer de alguna manera más sencilla la búsqueda de información, en las cuales se han realizado interfaces gráficas con las que se pueden realizar cualquier tipo de tarea de una manera fácil, rápida y practica.

La historia de la Internet y de la web es historia reciente, los albores del Internet están en los años 60 y de la *Web*, su componente más exitoso tiene menos de diez años, Internet y *WWW* han significado el traslado de la importancia de la computadora como una herramienta aritmética hacia la computadora (herramienta de comunicación) esto fue evidente desde sus mismos comienzos.

La motivación inicial de una red de aparatos de comunicación interconectados fue militar, las comunicaciones pasan por nodos de interconexión los cuales, si fallan (son blanco de un ataque) hacen colapsar la integridad de la comunicación, el objetivo era establecer una red que permitiera desviar los mensajes de modo que no tuviesen que pasar por el nodo inservible, la evolución de una red telefónica (lo único usado en el teatro de operaciones militares hasta entonces) así el Internet fue posible gracias al uso de las computadoras.

El hecho de que las computadoras personales se han vuelto casi tan ubicuas como los televisores, jugó un papel preponderante en la casi universal accesibilidad de este nuevo medio, no solo como espectador sino como protagonista, este hecho es sin duda lo que ha convertido la Internet en un fenómeno social.

Los orígenes de la Internet se hallan en la creación hacia el final de la década de los cincuenta de la "Agencia de Proyectos de Investigación Avanzada (*DARPANET* en inglés *Defense Advanced Research Project Network*) del Departamento de Defensa de los EE.UU. en 1960 *DARPANET* fundó la oficina de técnicas de procedimiento de la información (*IPTO*), su misión era desarrollar un sistema militar de comunicación capaz de funcionar después de una devastación nuclear, la filosofía de su director, el psicólogo Carl Licklider, iba más allá; era lograr la interacción del hombre- Ordenador ."[14]

DARPANET tenia el propósito principal que era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes de transmisión de paquetes de diferentes tipos capaces de resistir las condiciones de operación más difícil y continuar funcionando aún con la pérdida de una parte de la red (por ejemplo en caso de guerra).

Estas investigaciones dieron como resultado el protocolo *TCP/IP* (*Transmisión Control Protocol/Internet protocol*) un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet. Durante el desarrollo de este protocolo se incremento notablemente el número de redes locales de agencias gubernamentales y de universidades que participan en el proyecto, dando origen así a la red de redes más grande de el mundo, las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo requiriera sin importar de que país provenía, la solicitud siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión), los usuarios pronto encontraron que la

[14] Generaciones De Computadoras.WWW. geocities.com, Informática, fecha de consulta 20/06/2002.

información que había en la red era por demás útil y si cada quien aportaba algo se enriquecería aún más el acervo de información existente.

Por extraño que parezca no existe una autoridad central que controle el funcionamiento de la red, aunque existen grupos y organizaciones, que se dedican a organizar de alguna forma él trafico en ella, después de que las funciones militares se separaron de la red en una subred de Internet, la tarea de coordinar la red recayó en varios grupos, uno de ellos fue la *National Science Foundation*, fue que promovió bastante el uso de la red ya que se encargo de conectar cinco centros de súper computo que podían ser accesados desde cualquier nodo de la red, eso funcionó bien al principio, pero pronto fueron superadas las cargas de tráfico previstas, fue entonces que se dio la concesión a *Merit Network Inc.* Para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando servicio mucho más rápido, pero este proceso evidentemente nunca termina debido a la creciente demanda de los servicios que se encuentran en la red.

El grupo de mayor autoridad sobre el desarrollo de la red es la *Internet Society* creado en 1990 y formado por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global a través de la tecnología de Internet, puede decirse que esta sociedad es como un consejo de ancianos que tiene la responsabilidad de la administración técnica y dirección de Internet, pero no es el único grupo que puede tomar decisiones importantes, existen otros tres grupos que tienen un rol significativo la Internet *Architecture Board* (IAB), toma las decisiones acerca de los estándares de comunicaciones entre las diferentes plataformas para que puedan interactuar máquinas de diferentes fabricantes sin problema, este grupo es responsable de como se deben asignar las direcciones y otros recursos en la red, aunque no son ellos quienes se encargan estas asignaciones, para eso existe otra organización llamada *NIC* (*Network Information Center*) administrado por el Departamento de Defensa de los Estados Unidos.

Engineering Task Force (IETF) en el cual los usuarios de Internet expresan sus opiniones sobre como se deben de implementar soluciones para problemas operacionales y como deben de cooperar las redes para lograrlo, la dirección de Internet es en cierta manera una autocracia que funciona.

El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada país que forma parte de Internet lo que proporciona un servicio prácticamente gratuito, a principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando su origen a una nueva etapa en el desarrollo de la red.

La historia de la Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, *ITESM* hacia la Universidad de Texas en San Antonio *(UTSA)* específicamente a la escuela de Medicina, Una línea privada analógica de 4 hilos a 9600 bits por segundo fue el enlace.

Para que una terminal esté en condiciones de conectarse a una red de comunicaciones debe dotársele del soporte físico y lógico correspondiente. El soporte lógico necesario no es más que un programa de comunicaciones que permite a la terminal u ordenador enviar los datos de forma acorde con el modo de transmisión que se emplea y con el tipo de red de comunicaciones que se utiliza. Sus tareas concretas son enviar y recibir ficheros, permitir las comunicaciones que requieren diálogo entre los extremos y detectar, y en algunos casos corregir, los posibles errores en el envío de datos o ficheros. Además, el programa de comunicaciones se encarga de controlar y supervisar el soporte físico necesario para la comunicación, que recibe el nombre particular de *modem*[15].

[15] La palabra MODEM proviene de la contracción de los términos modulador y demodulador, lo que da idea de las funciones que lleva a cabo el equipo: transforma la serie de unos y ceros, que proporciona el ordenador para transmitir, en señales de tipo analógico, aptas para viajar por los cables o líneas telefónicas, y viceversa. Para que una transmisión de datos sea posible es preciso que exista un módem en cada uno de los extremos de la línea, conectado a los terminales u ordenadores existentes, y que todos los módems sean compatibles es decir, que procedan de la misma forma con los datos.

1.1.3. - PRINCIPALES SERVICIOS DE INTERNET

1.1.3.1. - REDES

La introducción de los ordenadores personales en la oficina a supuesto un nuevo concepto en el manejo de datos. Generalmente en una oficina se trabaja en equipo, los departamentos (Cobros, Contabilidad, Proveedores...) deben estar interconectados, y deben utilizar una serie de recursos comunes: Impresoras, discos duros de gran tamaño, *streamer*, etc. Si nosotros trabajamos con varios ordenadores, pero es imposible recoger la información directamente de uno a otro, es lo que se denomina trabajar en monopuesto, si podemos realizar este proceso hablamos de un sistema multipuesto.

Anteriormente también era necesario para la gran empresa interconectar todos sus equipos, esto era solo posible utilizando superordenadores como ordenador central, que se encargaban de realizar todos los cálculos, lecturas, grabaciones o impresiones, de todas las terminales conectadas. Terminales que solo tenían la función de recoger datos procedentes del teclado o cualquier otro periférico de entrada, el ordenador central los procesaba y este enviaba a esta los resultados. Por lo tanto todo el peso recaía en el ordenador central ya que el resto de ordenadores eran lo que se denominaba terminales tontas. Con el aumento de exigencias en cuanto al nuevo software y el aumento del número de terminales en las empresas, estos sistemas empezaron a ralentizarse (en ocasiones se sustituía el equipo central por un equipo mayor, como la serie *AS-400 de IBM*) por otro lado los llamados microordenadores empezaban a obtener rendimientos sobresalientes, lo que condujo a pensar que era mucho más práctico dejar al ordenador central para determinadas tareas y el resto que fuesen calculadas por los terminales (divide y vencerás). Con lo cual se empezaron ha aumentar los rendimientos, también debido a un menor coste general las redes locales fueron asequibles no solo a la gran empresa sino a la mediana empresa. Las tres características básicas que potencian una red son:

a) Distribución de periféricos. Nos permite utilizar periféricos de altas prestaciones y costos para todas las terminales. Los periféricos pueden estar conectados en dos modos.

- Local: Solo se puede acceder a ellos desde la terminal en la que estén conectados.
- Red: Se puede acceder a ellos desde cualquier puesto. Los sistemas en Red utilizan sistemas especiales para controlar el acceso a estos periféricos, como los sistemas de cola. En estos los trabajos se van añadiendo a la cola según van apareciendo y según el nivel de prioridad del usuario que envía el trabajo. Estos sistemas nos permiten cambiar el orden de impresión de los documentos en casos especiales.

b) Distribución y seguridad de la información. Al igual que los periféricos en una red podemos tener información local a la cual solo se puede acceder desde una terminal que la posea o información en red. Debido a que la información en red tiene la gran ventaja de poder acceder a ella desde cualquier terminal, tiene la gran desventaja de que cualquiera puede acceder a ella y destruirla (y no hay que olvidar que los datos son dinero). Por ello aparecieron en estas los niveles de seguridad, los usuarios que van a utilizar dichas terminales deben estar divididos en grupos, cada grupo tiene unos determinados derechos y restricciones sobre la información en red, así como pueden existir usuarios que dentro de un mismo grupo tenga más o menos derechos sobre la utilización de ficheros que otros compañeros. Un usuario también puede pertenecer a varios grupos. Así por ejemplo en un sistema en red puede existir un grupo denominado CONTABILIDAD del que el resto del grupo no puede leer su información pero puede transferirle información. Debido a estos niveles de seguridad cada usuario debe de poseer lo que se denomina su *password* o clave de entrada, para que ningún otro usuario tenga la posibilidad de entrar como si fuera él.

Los sistemas de redes como Internet permiten intercambiar información entre computadoras, y se han creado numerosos servicios que aprovechan esta función, entre ellos figuran los siguientes; conectarse a un ordenador desde otro lugar (*telnet*), transferir ficheros entre una computadora local y una computadora remota (protocolo de trasferencia de ficheros o *FTP*) y leer e interpretar ficheros de ordenadores remotos (*gopher*), el servicio de Internet más reciente e importante es el protocolo de trasferencia de hipertexto (http), un descendiente del servicio de *gopher*, el http puede leer e interpretar ficheros de una máquina remota; no sólo texto sino imágenes, sonidos o secuencias de video, el http es el protocolo de trasferencia de información que forma la base de la colección de información distribuida denominada *World Wide Web*.

"*La World Wide Web* (también conocida como *Web o WWW*) es una colección de ficheros, denominados lugares de *Web* o páginas de *Web*, que incluyen información en forma de textos, gráficos, sonidos y videos, además de vínculos con otros ficheros, los ficheros son identificados por un localizador universal de recursos (*URL* siglas en inglés) que especifica el protocolo de trasferencia, la dirección de Internet de la máquina y el nombre del fichero, los programas informáticos denominados exploradores, utilizan el protocolo http para recuperar esos ficheros."[16]

Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información, las diferentes computadoras se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores, estos son computadoras como las estaciones de trabajo, pero poseen funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso de las estaciones de trabajo a la red y a los recursos compartidos (como las impresoras), la línea roja representa una conexión principal entre servidores de red,

---

[16] Investigación Informática. http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos_de informática, fecha de consulta 20/02/2002.

la línea azul muestra las conexiones locales, un módem (modulador demolulador) permite a las computadoras transferir información a través de las líneas telefónicas normales, el módem convierte las señales digitales en analógicas y viceversa, y permite la comunicación entre computadoras muy distintas entre si.

Una red tiene tres niveles de componentes: "*Software* de ligaciones, software de red y hardware de red, el primero está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información ese tipo de software se denomina cliente-servidor, las computadoras cliente envían peticiones de información o de uso de recursos a otras computadoras llamadas servidores, que controlan datos y aplicaciones, otro tipo de hardware es el que se conoce de igual a igual (*peer to peer*), en una red de este tipo, los ordenadores se envían entre si mensajes y peticiones directamente sin utilizar un servidor como intermediario."[17]

"El *software* de red consiste en programas informáticos que establecen protocolos o normas, para que las computadoras se comuniquen entre si, estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes, estos protocolos indican como efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente." [18]

"El *hardware* de red está formado por los componentes materiales que unen las computadoras, dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio que conecta a los ordenadores, recibir paquetes desde el software de red y trasmitir instrucciones y peticiones a otras máquinas, la información se transfiere en forma de dígitos binarios, o bits (unos y

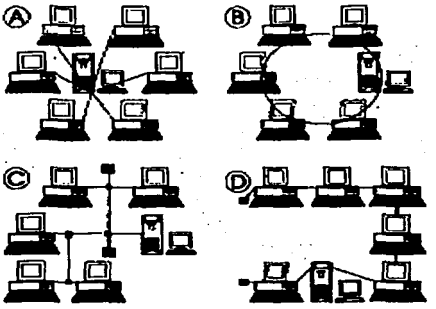
[17] Investigación informática. http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos de informática,. fecha de consulta 20/02/2002

[18] Investigación Informática. http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos de informática., Fecha de consulta 20/02/2002.

ceros) que pueden ser procesados por los circuitos electrónicos de los ordenadores."[19]

TOPOLOGÍA

Las topologías más corrientes para organizar las computadoras de una red son las de punto a punto, de bus, en estrella y en anillo, la topología de punto a punta es la más sencilla, y está formada por dos ordenadores conectados entre sí.



a) ***Estrella***:	En ella todas las terminales están conectadas a un equipo central. Todas las comunicaciones entre ordenadores se hacen a través del ordenador central, por lo tanto si este deja de funcionar deja de funcionar toda la red.
b) ***Anillo***:	Los datos pueden circular en cualquier dirección del anillo.
c) ***Árbol***:	La principal ventaja de este tipo de red es su funcionalidad y su principal inconveniente es que cualquier tipo de fallo en una terminal provoca el no funcionamiento de todos los equipos que estén por debajo de él.
d) ***Bus***:	Como principal característica está su sencillez. Las terminales escuchan todos los mensajes que pasen por el bus, pero solo reconocen y guardan los que van dirigidos a ella.

[19] Investigación Informática http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos de informática, fecha de consulta 20/02/2002.

"La topología de *bus* consta de una única conexión a la que están unidos varios ordenadores, todas las computadoras unidas a esta conexión reciben todas las señales transmitidas por cualquier computadora conectada."[20]

Otra clase de topología es la de *estrella* donde conecta varios ordenadores con un elemento dispositivo central que se denomina *hub*, "el *hub* puede ser pasivo y transmitir cualquier entrada recibida a todos los ordenadores de forma semejante a la topología de bus, o ser activo, en cuyo caso envía selectivamente las entradas a ordenadores de destino determinado".[21]

La topología en *anillo* utiliza conexiones múltiples para formar unos círculos de computadoras, cada conexión transporta información en un único sentido, la información avanza por el anillo de forma secuencial desde su origen hasta su destino.

PROTOCOLOS DE RED.

El ancho de banda, en comunicaciones, es un indicador de la cantidad de datos que pueden transmitirse en determinado periodo de tiempo por un canal de transmisión, por lo general el ancho de banda se expresa en ciclos por segundo (*hercios, Hz* o en bits por segundo).

" Direcciones Ip, *Internet*, dirección de grupo de números que identifica a cada computadora en Internet, consiste en cuatro números separados por puntos, en los que cada número puede variar entre 0 y 255- por ejemplo 123.106.78.90. los

---

[20] Investigación, 'Informática http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos de informática. Fecha de consulta 20/02/2002.

[21] Investigación, Informática http://www.páginas.com%2fdetalle.php3%Fidioma%3DCastellano%26sección%3Dtrab%26categoria%3D41trabajos de informática. , Fecha de consulta 20/02/ 2002.

servidores de nombres de dominio mantienen tablas que permiten traducir la dirección de Internet, también conocida como dirección IP."[22]

Las redes pueden estar conectadas en un entorno cerrado (como puede ser una oficina) lo que se denomina red local o *LAN* [23] (*Local Área Network*).

Las *LANs* hicieron posible que las computadoras compartieran archivos y equipo periférico, tal como impresoras y servidores . Estar conectado a una *LAN* también permite que las computadoras de diferentes distribuidores operen entre si, es decir, que trabajen juntas.

Si el entorno es más abierto, es decir que podemos conectarnos con otras oficinas (ya estén situadas en nuestro país o en cualquier otro) que también posean red local o incluso con sistemas basados en superordenadores es lo que se denomina *WAN* (*Wide Area Network*)[24].

Esta red proporciona proporciones potencialmente globales. Si se emplean facilidades publica, una *Wan* involucra compañías de telecomunicaciones para el intercambio local (*LECs, Local exchange carriers*), compañías de telecomunicaciones para el intercambio a larga distancia (*IXCs, Interexchange Carriers*) y compañías de telecomunicaciones de lugares remotos

---

[22] LAN (siglas en inglés), son redes de área local que conectan ordenadores separados por distancias reducidas, suelen usar topología de bus.

[23] Grupo de computadoras que se encuentran dentro de un área y que por lo general se conectan con menos de 1000 pies (350 metros) de cable. Generalmente , una LAN interconecta cierto número de computadoras e impresoras en un solo piso o un solo edificio. Las LANS pueden conectarse entre si, pero si dos o mas LANS se conectan por medio de modems y líneas telefónicas, la red resultante constituye lo que se llama una Wan. Las LANS se presentan en distintas configuraciones físicas (llamadas topologías), las mas populares de las cuales son de Bus , de anillo y de estrella. También hay diferentes tipos de protocolos y tecnologías disponibles; los que dominan en el mercado son Ethernet, Token Ringy, en menor medida, ARCNET

[24] Una WAN constituye un sistema de comunicación que interconecta sistemas de computadoras geográficamente remotos . Enlaza las computadoras situadas fuera de las propiedades de una organización (edificios o campus) y atraviesa áreas publicas que están reguladas por autoridades locales, nacionales e internacionales. Generalmente, el enlace entre lugares remotos se realiza a través de la red publica de teléfono, pero una organización podría crear sus propios enlaces WAN mediante microondas, satélites u otras tecnologías de la comunicación.

Finalmente la *MAN*[25] consiste en un servicio *INTRA- LATA* limitado a una zona de cableado local, en vez de una zona *INTER -LATA*. Todavía a un mas y los servicios que proporcionan, pueden expandirse a un área de forma que cubran cientos de millas de cuadras.

La *MAN* se construye sobre una arquitectura de *BUS* dual, lo que significa que dos cables de fibra proporcionan transmisiones en direcciones opuestas al mismo tiempo. Un nodo perteneciente al *Bus dual* puede enviar datos en varias direcciones. Se incorpora en una topología de *anillo*.

1.1.3.2. - TELNET.

Es el protocolo de comunicaciones que permite al usuario de una computadora con conexión a Internet establecer una sesión como terminal remoto de otro sistema red, si el usuario no dispone de una cuenta en el ordenador o computadora remoto, puede conectarse como usuario anónimo y acceder a los ficheros de libre distribución, muchas máquinas ofrecen servicios de búsqueda en bases de datos usando este protocolo.

1.1.3.3. - FTP (PROTOCOLO DE TRANSFERENCIA).

Estas siglas significan "un acrónimo de *File Transferi Protocolo*, protocolo de transferencia de archivos que se utiliza en Internet y otras redes para transmitir archivos".[26]

---

[25] Una red de área metropolitana en una red soporte que se expande en un área ciudadana y la regulan las comisiones locales o estatales. La compañía telefónica, los servicios de cables y otros proveedores proporcionan servicios MAN para las compañías que necesiten la construcción de redes que se expanden a través de los derechos de paso de las áreas metropolitanas.

[26] FTP.- se le denomina así a redes de área local que conectan ordenadores separados por distancias reducidas.

El protocolo asegura que el archivo se transmita sin errores, el sistema que almacena archivos que se pueden solicitar por *FTP* se denomina servidor de *FTP*, el *FTP* forma parte del conjunto de protocolos *TCP/IP*, que permite la comunicación en Internet entre distintos tipos de máquinas y redes.

CAPITULO II

II.- MARCO CONCEPTUAL

2.1. - DELITO.

Guillermo Cabanellas nos define el delito de la manera siguiente: "Etimológicamente, la palabra delito proviene del latín *delictum*, expresión también de un hecho antijurídico y doloso castigado con una pena, en general, culpa crimen, quebrantamiento de una ley imperativa, cumplimiento del supuesto contenido en la ley penal, que el delincuente no viola sino observa."[27]

Como hemos estado mostrando la forma de delinquir es muy diversa en cuestiones de vía Internet, pero en este caso como he estado haciendo referencia al fraude informático podemos decir que antes que nada lo podemos considerar un delito que debe ser tipificado en nuestro Código Penal del Distrito Federal de manera exclusiva, pero antes que nada hay que dar los fundamentos por los que lo consideró como un delito necesario de ser regulado de manera independiente dentro del mencionado código.

De acuerdo a el articulo 15 del Nuevo Código Penal del Distrito Federal.

" TÍTULO SEGUNDO
EL DELITO
CAPÍTULO I

FORMAS DE COMISIÓN

ARTÍCULO 15 (Principio de acto). El delito sólo puede ser realizado por acción o por omisión.
ARTÍCULO 16 (Omisión impropia o comisión por omisión). En los delitos de resultado material será atribuible el resultado típico producido a quien omita impedirlo, si éste tenía el deber jurídico de evitarlo, si:
I . Es garante del bien jurídico;
II . De acuerdo con las circunstancias podía evitarlo; y
III . Su inactividad es, en su eficacia, equivalente a la actividad prohibida en el tipo.
Es garante del bien jurídico el que:
a). Aceptó efectivamente su custodia;
b). Voluntariamente formaba parte de una comunidad que afronta peligros de la naturaleza;
c). Con una actividad precedente, culposa o fortuita, generó el peligro para el bien jurídico; o

[27] Op. Cit, Cabanellas Guillermo, ***TOMO I***, Pág. 603-604.

d). Se halla en una efectiva y concreta posición de custodia de la vida, la salud o integridad corporal de algún miembro de su familia o de su pupilo.
ARTÍCULO 17 (Delito instantáneo, continuo y continuado). El delito, atendiendo a su momento de consumación, puede ser:
I. Instantáneo: cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción legal;
II. Permanente o continuo: cuando se viola el mismo precepto legal, y la consumación se prolonga en el tiempo; y
III. Continuado: cuando con unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo, se concretan los elementos de un mismo tipo penal. "[28]

De acuerdo a lo anterior respecto al fraude informático, no se nos aclara nada en forma substancial de forma directa, pero nos da la base por la que considero que el fraude informático es considerado como delito, ya que por su naturaleza el fraude es un acto el cual se basa en el engaño, en la mentira, en aprovecharse de los individuos, ya sea de su error o ignorancia para obtener de estos un lucro indebido, y si a esto le aunamos que pueden ser los individuos más susceptibles de caer en este tipo de delito si se emplean los medios informáticos como lo es la computadora y la Internet, y para resolver este dilema a continuación se desarrollaran diversos conceptos para aclarar el panorama, para poder llegar al punto medular de nuestra investigación.

Según Carnelutti podemos definir el delito, desde un ámbito sociológico: "Desde este punto de vista un hecho es delito por ser contrario al bien común o, en otras palabras, perjudicial a la sociedad."[29]

Esto lo podemos entender de un modo en el que dicho autor, nos marca que todo hecho que sea contrario a las reglas tanto de trato social, como el bien común, abarcando las normas de conducta, y todo lo que afecte en cierto grado o cause un perjuicio ya sea a un solo individuo, ó a un sector de la sociedad, o a la sociedad en general, provoca en cualquier momento un deterioro, que propicia un perjuicio masivo, a dicha sociedad, y si analizamos que actualmente los medios de

[28] GACETA OFICIAL DEL DISTRITO FEDERAL, 16 de julio del 2002.recinto legislativo a 03 de julio de 2002.
[29] Carnelutti., Francesco, ***TEORÍA GENERAL DEL DELITO.***, Editorial ARGOS, Colombia, 1960. p16.

comunicación como la Internet, es usado por un gran nivel de personas de toda clase social, y si podemos encuadrar al fraude informático, dentro de un ámbito sociológico, como fue analizado anteriormente, podemos confrontarlo simultáneamente en el ámbito jurídico como a continuación expongo.

"Desde el punto de vista jurídico, el mismo hecho es delito por estar castigado como una pena, mediante un proceso."[30]

Como toda definición de delito es siempre o casi siempre el resultado de un silogismo que plantea bien el problema pero que nada nuevo descubre, y añadir que es la negación del derecho, supone hacer un juicio a posteriori, que por eso es exacto pero que nada añade a lo sabido, es una tautología (decir dos veces), hay que aceptar que el delito, desde el plano jurídico, es un acto u omisión antijurídico y culpable.

Carrara opina acerca de la definición de delito como ente jurídico es "la infracción de la ley del estado, promulgada para proteger la seguridad de los ciudadanos resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso".[31]

Dentro de esto se encuentra un pensamiento muy importante el cual dice: "Carrara pensó que su doctrina era inatacable, y de tan perfecta que era, como todo lo perfecto llevaba en si la caducidad, ya no era futuro, sino presente, y por tanto futuro ido, y a pasos agigantados pasado, residuo, una revolución la descoyunto, la enterró, aunque como en los espectros de *Ibsen*, vuelva luego, y a su vuelta da más vigor a lo reencarnado, pero la revolución fue terrible, se llamo el positivismo."[32]

---

[30] Ibidem.
[31] Jiménez De Asúa, Luis, ***LECCIONES DE DERECHO PENAL***, Volumen 7, Editorial Harla, México, 1997.Pág. 130.
[32] Idem.

Por su parte el Profesor Ernesto Beling define al delito y " nos dice que es la acción típica antijurídica, culpable, sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad."[33]

Del concepto mencionado se deduce que para ser delito un acto se necesita reunir dichos requisitos, es decir una acción descrita objetivamente en la ley, ó sea una, tipicidad, contraria al derecho, esto es que exista antijuridicidad; dolosa o culposa, es decir, que medie culpabilidad, sancionada con una pena, ó sea, que tenga fijada penalidad, y que se den las condiciones objetivas de punibilidad.

Por su parte Max Ernesto Mayer define al delito como un "acontecimiento típico, antijurídico e imputable"[34], este autor emplea la palabra imputable en el amplio sentido de culpabilidad y por ello en este punto, no difiere esencialmente su concepto del delito del expuesto anteriormente por Beiling.

Si definimos al delito sistemáticamente podemos decir que es "Un acto típicamente antijurídico y culpable, imputable a un hombre y sometido a una sanción penal, sin embargo, al definir la infracción punible, nos interesa establecer todos sus requisitos, aquellos que son constantes y los que aparecen variables, en este aspecto el delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal, las características del delito serian estas; actividad, adecuación típica; antijuridicidad, imputabilidad, culpabilidad, penalidad y, en ciertos casos, condición objetiva de punibilidad."[35]

El acto, tal y como nosotros lo concebimos, independiente de la tipicidad, es más bien el soporte natural del delito; la imputabilidad es la base psicológica de la culpabilidad y las condiciones objetivas son adventicias e inconstantes, por tanto la esencia técnico-jurídica de la infracción penal radica en tres requisitos: tipicidad,

---

[33] Idem. Pág. 132.
[34] Ibidem
[35] Idem Pág. 133.

antijuridicidad y culpabilidad, constituyendo la penalidad, con el tipo, la nota diferencial del delito. con estos elementos podemos adecuar a nuestro tema por que considero que debe considerarse como delito y debe ser tipificado, con las razones que más adelante se explicarán.

Sabemos que los delitos no pueden ser otra cosa que conductas humanas, pues carecería de sentido hablar de delitos que no fueran conductas humanas.

Zaffaroni nos menciona acerca de esto que "No habrá delito, cuando la conducta, de un hombre no se adecué a alguno de los dispositivos previamente descritos en la ley"[36], y para encuadrar que puede ser considerado como delito el mismo autor nos menciona "afirmando que el delito es la conducta de un hombre, sabemos que entre una infinita cantidad de conductas posibles, solo algunas son delitos, para poder distinguir las conductas que son delito de aquellas que no lo son serian las conductas prohibidas a las que se asocia una pena como consecuencia".[37]

Se pueden señalar tres sistemas en la evolución de la concepción analitica que distingue en el delito los elementos que son acción, tipicidad, antijuridicidad y culpabilidad:

1. El primer sistema llamado del causalismo natural o sistema clásico esta representado por los sistemas de Franz Von Liszt, Ernest Beling y Gustav Radbruch, este sistema como ya hemos analizado en párrafos anteriores impero durante los primeros años del siglo XX y su estilo de pensamiento corresponde al positivismo científico imperante en la segunda mitad del siglo XIX.

2. El segundo sistema corresponde al llamado causalismo valorativo o sistema neo clásico y esta representado fundamentalmente por los sistemas de Mezger, Mayer y Sauer (autores alemanes) en este sistema se configura una concepción

[36] Zaffaroni, Eugenio Raúl, ***MANUAL DE DERECHO PENAL***, Parte general, 2ª edición Editorial Cárdenas , México, 1997, Pág. 339.
[37] Idem.

teleologica del delito en la que todas las características esenciales de la infracción punible aparecen orientadas sobre la idea de valor.

3. El tercer sistema corresponde a la doctrina finalista cuyo fundador y más autorizado representante fue Hanz Welzel, comenzó a elaborarse esta doctrina en la década de los años treintas del siglo pasado en Alemania, modificando el contenido conceptual de los elementos del delito así como su ubicación sistemática dentro de la teoría del delito en comparación con los modelos usados por los sistemas del causalismo natural y del causalismo valorativo.

   Para esta teoría la acción humana es ejercicio de la actividad final, la acción se dirige voluntariamente a un fin, por lo que el dolo y la culpa forman parte de la acción, en tanto que el resultado no es elemento de la acción, permanece fuera de ella.

Según el Ilustre penalista Cuello Calón, los elementos integrantes del delito son:
"a.- El delito es un acto humano, es una acción (acción u omisión)

b.- Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido,

c.- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico,

d.- El acto ha de ser culpable, imputable a dolo (intención o a culpa negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

e.- La ejecución u omisión del acto debe estar sancionada por una pena, por tanto, un delito, es una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena."[38]

La diferencias fundamentales entre las corrientes Causalista y Finalista son:

1.- El contenido de los conceptos,

2.- Su ubicación dentro de la teoría del delito.

A consecuencia del análisis anterior podemos decir, que para poder encuadrar como delito al fraude informático en términos del articulo 230 del Nuevo Código Penal para el Distrito Federal, Comete el delito de fraude "Al que por medio del engaño o aprovechando el error en que este se halle se haga ilícitamente de alguna cosa u obtenga un lucro indebido...", el tipo que se propone como tema de investigación se legisle en el mismo; reúne todos los requisitos necesarios para que sea encuadrado como tal, de la manera que a continuación se indica:

FRAUDE INFORMÁTICO

(Análisis del tipo, como se propone que se regule en la presente investigación):

DELITO.-	Fraude informático
ELEMENTO DE CONDUCTA.-	De Acción.
BIEN JURÍDICO TUTELADO.-	El Patrimonio y la Información
OBJETO MATERIAL DEL DELITO.-	El Patrimonio e información
RESULTADO.-	Formal y Material
DAÑO.-	Detrimento del patrimonio y menoscabo de la información
NÚCLEO ESENCIAL DEL TIPO.-	Usar
DURACIÓN.-	Instantáneo (art17 NCPDF)
FORMA DE PERSECUCIÓN.-	Por querella
ELEMENTO INTERNO.-	Doloso
ELEMENTO OBJETIVO.-	Entrar, usar
ELEMENTO SUBJETIVO.-	Con un fin o Con un Propósito
ELEMENTO NORMATIVO.-	Lucro, bienes
NÚMERO DE SUJETOS.-	Unisubjetivo o plurisubjetivo

[38] El Delito, http://www.monografias.com. Fecha de consulta 18/04/2002

NÚMERO DE ACTOS.-	Unisubsistente
ESTRUCTURA METODOLOGÍCA	Simple
ORDENACIÓN METÓDICA.-	Tipo Básico Fundamental
FORMULACIÓN.-	Casuista Alternativo.

2.2. - DEFINICIÓN DE INFORMÁTICA.

La informática es una ciencia que ha tenido su auge en la tecnología, y que ha tenido sus avances dentro de lo que actualmente conocemos como la cibernética, la robótica, la Internet, etc., debiendo su existencia a la necesidad de la humanidad de valerse de factores que ayuden al progreso del hombre. hasta la actualidad son bastantes y muy fascinantes los logros que ha llegado a tener la informática como consecuencia de la tecnología, pero dentro de este marco cabe señalar que por lo novedoso de esta rama es muy susceptible de tener errores de los cuales es necesario de tipificar para que los individuos no seamos presa fácil de aquellos que valiéndose de esta herramienta como es la Internet, nos perjudiquen de un modo u otro, particularmente el engaño por vía Internet.

Por lo que creo que no se debe permitir que la realidad rebase al derecho, que debido o como consecuencia al desarrollo que ha tenido la informática de como consecuencia la comisión de ilícitos penales para los cuales en la actualidad no se prevé una sanción especifica, dada la carencia que nuestra legislación tiene, correspondiente a dicho tipo penal.

El Doctor Julio Téllez Valdés al respecto de la informática nos comenta: "Es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones, es el estudio que delimita las relaciones entre los medios (equipos), los datos y la información necesaria para la toma de decisiones desde el punto de vista de un sistema integrado."[39]

La Enciclopedia Multimedia de Salvat nos dice que la informática es el "...conjunto de técnicas para el tratamiento automatizado de la información".[40]

---

[39] Téllez Valdez, ***Derecho Informático***, Editorial Mc Graw Hill, México, S. A de C, V. 1996, p 5

[40] Enciclopedia Multimedia, Salvat , Editores , 1999.

El Diccionario Lexis 22 nos dice con respecto a la informática "(del Fr. ***informatique***; compuesto de información + ***automatique)*** f. Ciencia teórica y aplicada que estudia principalmente el tratamiento automático de la información. Para conseguir estos propósitos han sido necesarios una sistematización y ordenación de los procesos, unos estudios matemáticos y lógicos y el desarrollo de mecanismos electrónicos capaces de almacenar, operar y suministrar los datos a los resultados de sus operaciones con gran rapidez y en el momento y forma deseados."[41]

"La Informática, sin embargo, se diferencia de todas ellas en que construye instrumentos que imitan, aumentan, ayudan, facilitan sustituyen tareas psíquicas del ser humano."[42]

De lo anterior podemos deducir que el objetivo que pretende nuestro estudio al dar una concepción del término de Informática no es otro que el de apoyo para adentrarnos a nuestro tema, por lo que se puede decir que la Informática es la creación de instrumentos que sustituyen, o en algún caso, imiten al ser humano en la resolución de casi todo tipo de problemas, ó en si ala construcción de instrumentos que ayuden o faciliten al ser humano la realización de ciertos tipos de tareas, si vemos este punto de vista desde la utilización de estos instrumentos de una forma constructiva y licita, no veríamos ningún problema, la cuestión es que estos instrumentos se han desvirtuado de esta finalidad, ya que interfieren en el desarrollo tanto social como económico y a su vez político de un país, como lo es el tema de esta investigación, para proporcionar una visión acerca del mismo y poder de algún modo regularlo en nuestra legislación penal.

---

[41] Lexis 22, Diccionario Enciclopédico Vox, Circulo de Lectores, ***HOMS/JOLO, Tomo 11***, Barcelona 1976, Págs. 3019 y 3020.

[42] Enciclopedia De Informática Y Computación, ***INGENIERÍA DEL SOFTWARE E INTELIGENCIA ARTIFICIAL***, Editorial Cultural S, A. España, 1997. Pág. 6.

2.3. - INFORMÁTICA JURÍDICA.

Peña Helen clasifica de la siguiente manera los delitos informáticos en base a dos criterios;

"como instrumento o medio, o como fin u objetivo:

1. COMO INSTRUMENTO O MEDIO:
   - Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

2. COMO FIN U OBJETIVO.
   - En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física."[43]

María de la Luz Lima, nos proporciona otra clasificación, de lo que ella llama *delitos electrónicos*, diciendo "que existen tres categorías, a saber:

1. - Los que utilizan la tecnología electrónica como método,
2. - Los que utilizan la tecnología electrónica como medio y,
3. - Los que utilizan la tecnología electrónica como fin.

Como Método.- conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como Medio.- conductas criminógenas en dónde para realizar un delito utilizan una computadora como medio o símbolo.

Como Fin.- conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla."[44]

---

[43] Peña Helen, Palazuelos Silvia, Alarcón Rosalía, DIVISIÓN DE ESTUDIOS DE POSTGRADO, Facultad De Derecho, UNAM http://www.peña.unam.derecho.mx.

[44] Idem.

A su vez el Dr. Héctor Fix Fierro establece lo siguiente: la informática jurídica debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho, o más precisamente, a los procesos de creación, aplicación y conocimiento del derecho

El Dr. Antonio Pérez Luño, "define al derecho Informático como: la aplicación de los sistemas informáticos a las distintas esferas del derecho, sin embargo debería de añadirse a este concepto el estudio, análisis y aprovechamiento de los recursos que ofrece la informática al que hacer jurídico."[45]

Por su parte Daniel Ricardo Altamark define a esta disciplina indicando que "derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática."[46]

La informática en la actualidad esta inmersa en todas las ramas del Derecho y requiere del establecimiento de nuevas reglas jurídicas como muestra de las diversas soluciones que los estudiosos del derecho Informático tienen que aportar a este ámbito.

Debido a su actual auge es que se encuentran muy pocas y loables iniciativas en toda América Latina relacionadas al estudio y desarrollo del derecho Informático.

2.4. - DELITO INFORMÁTICO.

El primer antecedente al que deberemos de referirnos lo encontramos, en el año 1949, apenas un año después de que en los Estados Unidos, se da a conocer la obra "*cibernética*", de Norbert Wiener, obra la cual motiva a el juez Norteamericano

---

[45] Pérez Luño, Antonio Enrique, ***MANUAL DE INFORMÁTICA Y DERECHO***, Editorial Ariel, S, A, Barcelona, 1996. Pág. 69.

[46] Informática Y Derecho, http://www.Informática y derecho/régimen jurídico de los bancos de daos de buenos aires. Fecha de consulta 30/05/2002. ALTAMARK, D, R, INFORMÁTICA Y DERECHO, aportes de doctrina Internacional , volumen 6, Régimen Jurídico de los Bancos de Datos de Buenos Aires.

Lee Loeverger a escribir un articulo titulado, *El Próximo Paso*, y en el cual por primera vez se utiliza el término *Jurimetria* primer antecedente del derecho informático y con el cual se vislumbraba el surgimiento de una nueva rama del derecho, encargada de las aplicaciones *cibernéticas* a la información jurídica. El juez Loeverger circunscribió la utilidad y fin de la jurimétrica al estudio y la racionalización del derecho a través de la aplicación de la automatización elevando inclusive una propuesta de aplicación limitada únicamente al derecho fiscal.

En 1958, en Francia el jurista, Lucien Mehl, desarrolla el trabajo titulado *Automatización en el mundo legal*, exponiendo puntos de vista relativos a lo que se dio en nombrar las *máquinas Leyes*, calificando las mismas en dos categorías distintas; máquinas documentales y máquinas de consulta.

Para 1963 se publica un articulo, en el que se dan a conocer ideas de gran interés sobre la aplicabilidad de la Cibernética al Derecho, este articulo conocido como el de *Knapp* (nombre de su autor), no tuvo mayor relevancia ya que fue escrito en checoslovaco, sin embargo este inconveniente fue superado posteriormente al publicar el mismo autor un estudio titulado "*Stadd an Reich*" publicado en Alemán.

Estos antecedentes continúan en Italia, donde encontramos el trabajo de dos juristas de nombres Frosini, escritor del libro titulado *Cibernética Diritto e Società* publicado en 1968 y Mario Lozano, quien se encargo de recopilar y publicar todas las notas de la cátedra que impartía denominada *Introducción a la informática jurídica*.

Este proceso continúo en los sesentas hasta establecer que los bancos de datos que se utilizaban en ese entonces se podían utilizar no solo para almacenar y obtener información de una manera sencilla, sino que algunas actividades jurídicas tales como certificaciones, atribuciones de juez competente, elaboración de sentencias, podían ser realizadas fácilmente auxiliándose de la informática, originándose en consecuencia la informática jurídica decisional.

Ya con la aparición de las primeras computadoras se introduce la automatización en los estudios de operadores jurídicos (jueces, abogados, fiscales, asesores jurídicos) y las redes de información penetran tempestuosamente en las administraciones publicas.

Este desarrollo continúa a pasos agigantados hasta que alrededor del año de 1991, cuando nace la *World Wide Web* (*www* por sus siglas, conocida en español como la súper carretera de la información)

Ya el nacimiento del comercio electrónico se sitúa en 1995, precisamente al utilizar la Internet para los negocios y con ello la mayoría de los país del mundo en mayor o menor medidas comienzan a legislar respecto al tema.

En contraparte a los beneficios que el desarrollo de la informática aporta a la humanidad, nos encontramos con la inconveniencia que casi siempre acompaña a la solución, las conductas delictivas y punibles que el gran avance tecnológico ha generado, y que han encontrado un espacio tan prolífico en el campo de la informática.

En los inicios del desarrollo de la informática y al detectarse las primeras violaciones al derecho intrínseco a ella, se pretendió desarrollar sistemas de seguridad que proporcionan la inviolabilidad de los mismos sin embargo el desarrollo de estos sistemas de seguridad únicamente han presentado un reto, para los delincuentes dedicados a la violación de los mismos, por lo que diversos países se dieron a la tarea de desarrollar el derecho Informático, pero en el caso de nuestro país estos esfuerzos han sido limitados ya sea por la creación de leyes demasiado particularizadas hacia un sólo tipo de delito o porque los congresos estatales se han encargado de regular su ámbito de competencia sin que exista la comunión necesaria para que se le de él carácter de federal a las leyes necesarias.

El tema resulta apasionante ya que al pretender tratar de regular los delitos informáticos y en especial el que es derivado del fraude informático, necesariamente

requiere que los encargados de establecer las conductas delictivas y sus correspondientes castigos y medidas de prevención, estén a un paso adelante del posible delincuente, lo cual resulta un tanto difícil ya que se ha abierto la puerta a conductas antisociales y delictivas, que se manifiestan de formas variadas.

Del análisis anterior podemos ver que 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.

Al definir el delito Informático resulta relativamente difícil ya que los conceptos básicos así como las definiciones varían de una manera importante de un país a otro, derivado esto desde el idioma utilizado, las frases o expresiones que cambian y se utilizan inclusive por cada país, esto es notorio al analizar el delito Informático ya que tiene diversas acepciones en cualquier parte del mundo como a continuación se muestran algunas:

1. - Delincuencia informática,
2. - Criminalidad informática,
3. - Delitos informáticos
4. - Delitos relacionados con las computadoras,
5. - *Computer Crimen* (crímenes por computadora),
6. - delincuencia relacionada con el ordenador.
7. - Abuso Informático

El jurista Julio Téllez Valdés nos dice en su obra Derecho Informático: "El concepto típico, los delitos informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin, El concepto atípico, Los delitos informáticos son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin."

Nidia Callegan define al delito Informático como " aquel que se da con la ayuda de la informática o de técnicas anexas".[47]

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 definidos en el titulo 1 de la Constitución Española".[48]

María 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"[49]

El Italiano Carlos Sarzana define el delito Informático como "cualquier comportamiento criminógeno en que la computadora esta involucrada como material, objeto o mero símbolo."[50]

La delincuencia informática es definida por el jurista Gómez Perals como "conjunto de comportamientos dignos de reproche, pena que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos."[51]

---

[47] Callegari, Lidia, ***DELITOS INFORMÁTICOS Y LEGISLACIÓN*** en revista de la facultad de derecho y ciencias políticas de la Universidad Pontificia Boliviana Medellín, Colombia, No 70 Julio-Agosto -Septiembre, 1985. p 115.

[48] Fernández Calvo, Rafael, ***EL TRATAMIENTO DEL LLAMADO DELITO INFORMÁTICO EN EL PROYECTO DE LEY ORGANIZA DEL CÓDIGO PENAL***, reflexiones y propuestas de la LI (Comisión de Libertades e Informática) en Informática y Derecho pp. 1150.

[49] Lima Malvido, María De La Luz, ***DELITOS ELECTRÓNICOS***, en criminalia, México-Academia Mexicana de Ciencias Penales, Editorial Porrúa, número 1-6, Año L, Enero-Junio, 1984, Pág. 100.

[50] Sarzana, Carlos, ***CRIMINALITA E TECNOLOGÍA***, en computers crime, Rassagna Penitenciaria e Criminologia, No 1-2, Año 1 1979, Roma Italia, p 53.

[51] Gómez Perals, Miguel, ***LOS DELITOS INFORMÁTICOS EN EL DERECHO ESPAÑOL***, informática y derecho nº4 UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de informática y Derecho 21-25, septiembre 1992, Mérida, 1994, Editorial Aranzadi, Págs. 489

Baòn Ramírez define la criminalidad informática como "la relación de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento Informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento Informático, ya sea hardware (en esté caso lo Informático es finalidad)."[52]

Romeo Casabona "se refiere a la definición propuesta por el departamento de justicia norteamericana, según la cual delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución."[53]

Davara Rodríguez, al estudiar el tema manifiesta lo siguiente. "No parece adecuado hablar de delito Informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito, ni el Código Penal de 1995 introduce el delito Informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio Informático."[54]

Ruiz Vadillo recoge la " definición que adopta el mercado de la OCDE en la recomendación número R(81)12 del Consejo de Europa indicando que abuso Informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos."[55]

---

[52] Baòn Ramírez, ROGELIO, ***VISIÓN GENERAL DE LA INFORMÁTICA EN EL NUEVO CÓDIGO PENAL***, en ámbito jurídico de las tecnologías de la información, cuadernos de derecho judicial, Escuela Judicial / consejo General del Poder Judicial, Madrid, 1996.Págs.89

[53] Romeo Casabona, Carlos María, ***LOS LLAMADOS DELITOS INFORMÁTICOS***, Revista de informática y derecho, UNED, Centro Regional de Extremadura, Mérida, 1995, Pág. 15.

[54] Davara, Rodríguez, Miguel Ángel, ***MANUAL DE DERECHO INFORMÁTICO***, Ed, Aranzadi, Pamplona, España, 1997. Pág. 39

[55] Ruiz Vadillo, Enrique, ***RESPONSABILIDAD PENAL EN MATERIA DE INFORMÁTICA***, nº 9, 10 y 11, UNED, CENTRO REGIONAL DE EXTREMADURA, Mérida 1996, Págs. 458

Según Barriuso Ruiz los podemos clasificar en:

" 1. - Delitos contra la intimidad

2. - De los robos,

3. - De las estafas,

4. - De las defraudaciones,

5. - De los daños,

6. - Relativo a la protección de la propiedad industrial,

7. - Relativos al mercado y a los consumidores."[56]

De acuerdo con Pérez Luño podemos hacer la siguiente clasificación:

"A) Desde el punto de vista subjetivo,

B) Desde el punto de vista objetivo,

- Los fraudes.- los daños engañosos (*data diddling*), los caballos de Troya (*Troya Horses*), la técnica del salami (*salami technique/rounching down*),
- El sabotaje Informático: bombas lógicas (*logic bombs*), virus informáticos,

- El espionaje Informático y el robo o hurto de software. fuga de datos (*data leakage*)

- El robo de servicios.- hurto del tiempo del ordenador, apropiación de informaciones residuales (*scavenging*), parasitismo Informático (piggybacking), suplantación de personalidad (*impersonation*).

---

[56] Jurídica Y Derecho, http: //www.informática-juridica.com. fecha de consulta 20/04/2002

Técnica del Salami.- aprovecha las repeticiones automáticas de los procesos de computo, es una técnica especializada que se denomina "técnica del salami" en la que las cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfieren a otra, esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar, uno de los casos más ingeniosos e s el usado en el redondeo hacia abajo, que consiste en una instrucción que se le da al sistema informático para que transfiera a una determinada cuenta los centavos que se descuenten por el redondeo.

- El acceso no autorizado a servicios informáticos: las puertas falsas (*trap doors*), la llave maestra (superzapping), pinchado de líneas (*Wiretapping*).

C) Funcionales."[57]

Por otro lado, siguiendo a Uhlrich Correa clasifica los delitos informáticos de la siguiente manera: " A) fraude por manipulaciones de un ordenador contra un sistema de procesamiento de datos, B) espionaje Informático y robo de software. C) sabotaje Informático, D) robo de servicios, E) acceso no autorizado a sistemas de procesamiento de datos, F) ofensas tradicionales en los negocios asistidos por ordenador."[58]

El delito Informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en actitudes típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios estafa, sabotaje, etc., sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. Y el desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo, ya que ha abierto la puerta a conductas antisociales y delictivas que se manifiestan en formas que hasta ahora no era posible imaginar.

Se podría definir el delito Informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique en forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno Informático y esta sancionado con una pena.

---

[57] Jurídica Y Derecho, http://www.informática-jurídica.com. fecha de consulta 20/04/2002
[58] Jurídica Y Derecho, http://www.informática-jurídica.com. fecha de consulta 20/04/2002

2.5. - COMERCIO ELECTRÓNICO.

Para poder comprender un poco más lo que en el punto quiero dar a conocer es conveniente que analicemos que entendemos primero por comercio:

La Enciclopedia Jurídica Omeba señala lo siguiente: "En sentido general, la Academia Española lo define en forma un tanto incompleta y justamente criticada, como de negociación que se hace comprando, vendiendo o permutando unas cosas por otras, en que existen muchas diversas formas de comerciar que nada tienen que ver con las cosas que se compran, se venden o permutan. Desde otros puntos de vista, llámese comercio a la comunicación y trato de unas gentes o pueblos con otros...."[59]

El Diccionario de Derecho Usual por su parte nos dice que el Comercio es: "Negociación o actividad que busca la obtención de ganancia o lucro en la venta, permuta o compra de mercaderías. Fuera del derecho mercantil, comercio significa trato o comunicación personal o social, "[60]

Como podemos ver la concepción de Comercio es un tanto escasa, ya que sino es enfocada a un ámbito mercantil como evidentemente es su finalidad no tiene una valoración jurídica fuera de ella, y lo correcto es suponer que el comercio tiene netamente una connotación ampliamente económica, por lo que podemos llegar a la conclusión de que el comercio es en si toda finalidad de lucro, ya sea por medio de bienes o servicios, pero siempre esperando una ganancia o remuneración ya sea en especie o en dinero.

Con lo anterior damos entrada a el término Comercio Electrónico, si partimos de la base que es la de lucrar u obtener ganancias de cualquier tipo, pero en este

---

[59] Enciclopedia Jurídica Omeba, ***Tomo III, CLAUS-CONS***, Editorial Driskill, S.A, Buenos Aires, 1979, Pág. 305.
[60] Cabanellas, Guillermo, ***DICCIONARIO DE DERECHO USUAL***, Tomo I, 10 edición, Editorial Heliasta, Buenos Aires, 1976. Pág., 423.

sentido seria mediante el medio de comunicación vía electrónica (Internet), por lo que es preciso manifestar que se entiende a continuación por este término.

Podemos decir que, los diversos estudios que se han llevado a cabo en torno al tema que define el comercio electrónico como *cualquier forma de transacción comercial en las que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo,* dicha definición tan solo nos marca una característica de esta modalidad de comercio, en la cual las relaciones entre las partes se desarrollan en vía electrónica.

Sin embargo, los alcances del comercio electrónico no puede quedar restringido a las relaciones de compraventa entre las partes a través de medios electrónicos pues tal figura podría confundirse con la doctrina del derecho Informático, como una simple contratación electrónica, que por lo que abarca el comercio electrónico es un amplio espectro tal y como nos lo indica el jurista Argentino Antonio Millè quien afirma que "bajo la denominación de comercio electrónico se distingue el basto conjunto de actividades con finalidad mercantil que se desarrolla mediante el uso de sistemas de procesamiento de datos y de comunicación sin que exista un contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda, la denominación no cubre solamente actos comerciales directos, como la compraventa o el alquiler, sino también acciones preparatorias o conexas como las de publicidad o mercadeo.

Es decir, el Comercio Electrónico comprende no solo las ventas o adquisiciones que el empresario y el usuario realizaran a través de la Internet, sino que engloba todas las bases del negocio empresarial. por lo que es correcto llegar a pensar que después de cualquier transacción que se realice vía electrónica (Internet) es necesario tener una protección como la que se tendría en dado caso que se adquiriera un bien o servicio de manera personal y directa, ya que el hecho de que se pueda realizar por el medio que se propone en el presente punto no excluye que

tengamos algún respaldo jurídico para exigir de terceros el cumplimiento, y que no se cometan atropellos debido a la vía que se esta manejando.

Podemos decir que el comercio electrónico en la actualidad como hemos tratado en el desarrollo de la presente investigación es una rama del derecho Informático que se encarga de promover y proteger los derechos de los consumidores en las operaciones efectuadas a través de los medios electrónicos ópticos o de cualquier otra tecnología pues prevé las obligaciones de los proveedores en este tipo de transacciones pues con ello se garantiza de manera integral los derechos de los consumidores, evitando en todo caso el manejo fraudulento de la información proporcionada y la correcta utilización de los datos aportados.

2.6. - DEFINICIÓN DE LA INTERNET.

A la Internet se le puede definir de la siguiente manera como: "interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente, este término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales, también existen sistemas de redes más pequeños llamados intranet, generalmente para el uso de una única organización, la Internet también se le conoce como la superautopista de la información, y permite el acceso universal a información de calidad."[61]

Lo anterior se refiere a que varias computadoras individuales conectadas entre sí forman una red de área local (Lan), Internet consiste en una serie de redes (Lan) interconectadas, las computadoras personales y las estaciones de trabajo pueden estar conectadas a una red de área local mediante un módem a través de una conexión.

[61] Conceptos Informáticos, http: //www.com/html/paginas/ficha.php3?zip=coninternet.zipficha y descarga del doc. Fecha de consulta 20/03/2002

" Internet.- Conjunto de millones de ordenadores conectados entre si a nivel mundial, es lo que se conoce como la red".[62]

DISTINCIÓN ENTRE RED DE AREA LOCAL Y UNA RED DE AREA INTERNA	
• Los usuarios de Internet son sus clientes	• Los usuarios de intranet son sus empleados
• Los usuarios externos requieren un tipo de información limitado relacionado con los negocios de la empresa, trabajo, investigaciones etc..	• Los usuarios internos necesitan **información para su desempeño laboral**
• Los diseños de Internet no soportan diseños demasiado elaborados debido a la capacidad de la memoria para guardar la información.	• Los diseños de intranets pueden soportar un entorno mucho más unificado
• El diseño de las páginas en Internet solo cumple estándares básicos, por lo cual no esta al día la información proporcionada.	• El diseño de la intranet no sólo debe cumplir los estándares oficiales del sistema, sino que también estará al día sobre los distintos departamentos

Por otro lado la Enciclopedia de Informática y Computación nos señala con respecto al tema: "En la terminología de las comunicaciones, Internet es una agrupación de redes conectadas entre si, de esta forma se puede decir que una Internet es una red de redes, por otro lado se denomina Internet (con I mayúscula) a la red que engloba a miles de redes de todo el mundo y que se basa en los protocolos de comunicaciones descritos por la arquitectura."[63]

Cabe aclarar que por red de computadoras se entiende " como la conexión de dos o más computadoras entre si para, de esta manera, poder compartir la información que esta distribuida entre todas las máquinas conectadas"[64]

No cabe duda de lo que es la Internet, ya que es todo el conjunto de redes mediante las cuales tenemos contacto con todo el mundo, y de esta manera se puede decir que tenemos acceso a diversos tipos de información, claro siempre y

[62] Artículos de Informática
http://Internet.fiestras.co.../Render&inifile=futurentese.ini&c=Articulo&cid=98356248099, Fecha de consulta 20/03/2002
[63] Enciclopedia De Informática Y Computación, ***TELEINFORMÁTICA***, Editorial Cultural, s. a. España, 1997. Pág. 128.
[64] IDEM, Pág. 114

cuando exista una computadora conectada a esta vía, ya sea con la finalidad de compartir información, vender bienes o servicios, comprar de igual manera bienes o servicios, lo que le da la finalidad licita o ilícita es el animó con que se hace dicha manipulación de información, para los efectos de esta investigación es obtener el benefició económico, mediante el engaño al usuario que requiere un bien o servicio y pretende o adquiere por dicho medio.

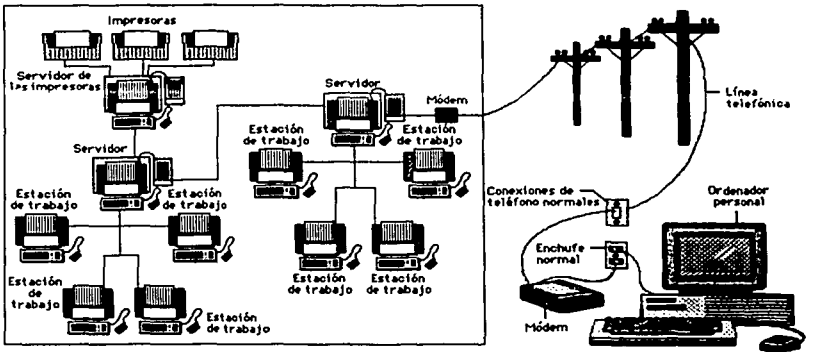


Ilustración de Microsoft

2.7. - FRAUDE.

El Diccionario de Derecho Usual de Guillermo Cabanellas nos dice al respecto "En un sentido general, engaño, abuso de confianza, acto contrario a la verdad o a la rectitud"[65]

La Enciclopedia Jurídica Omeba se refiere al tema señalando que: "Si un hecho reúne en si todos los caracteres de la estafa será siempre punible por este

[65] Op,Cit, Cabanellas, Guillermo, Pág. 222.

solo titulo, cualesquiera que sean las consecuencias, las modalidades y contingencias del hecho mismo."[66]

Francesco Carrara dice: " El legislador de las siete partidas de España señalo sabiamente que este delito no podía ser definido, que se le podía ejemplificar en algunas de sus formas, de las cuales los juzgadores pudiesen deducir un criterio para distinguir los artificios criminosos de los no criminosos en las transacciones humanas, en la infinita variabilidad de las astucias humanas es, en efecto, imposible enumerar taxativamente todos los modos con los cuales se puede cometer este delito, engañando a otro para inducirlo a realizar una convención obligatoria en contra suya o que importe abdicar de su propiedad, por eso todos los legisladores contemporáneos se han encontrado frente a la dificultad que confeso el antiguo legislador de la península ibérica, y han repetido el sistema de ejemplificar algunas formas de este delito, advirtiendo luego a los magistrados que estas indicaciones no eran sino demostrativas." [67]

Por otro lado Demetrio Sodí dice: "Toda ley casuística es defectuosa y más que defectuosa tiene que serlo cuando pretende limitar a determinados casos todos los engaños y todos los fraudes de que es capaz la malicia humana."[68]

Francisco Arroyo dice al respecto: "que siempre podrán inventarse nuevas maniobras o engaños y así va aumentando a medida de que se legisla, el número de disposiciones consideradas como delitos, con el tiempo se pierde la unidad del concepto e invade la esfera de otros delitos."[69]

De las definiciones anteriores, podemos darnos cuenta de que el fraude constituye una gran preocupación tanto para la iniciativa privada como para las entidades gubernamentales, debido al impacto negativo en sus ingresos y en el

---

[66] Enciclopedia Jurídica Omeba, ***Tomo XII, Fama-Gara***, Editorial Driskill, s.a. Buenos Aires, Argentina, 1977, Pág. 696.
[67] Reynoso Dávila, Roberto, ***DELITOS PATRIMONIALES***, Editorial Porrúa, México, 1999, Pág. 211.
[68] Idem.
[69] Ibidem.

bienestar general de la organización, a pesar de los esfuerzos de los auditores, la mayoría de los fraudes pasan desapercibidos por la dificultad de identificarlos y corregirlos, el fraude requiere para ser cometido de personas que tengan amplios conocimientos y para poder identificarlos se requiere de técnicas casi detectivescas y de la implementación de mecanismos para su debida detección.

Gutiérrez Francés, señala que "el vocablo fraude y sus derivados (defraudar, fraudulento, o defraudación), en lenguaje común, con frecuencia suelen identificarse con la idea de engaño, aunque percibe que no es fraude cualquier engaño."[70]

Por otro lado para el tratadista ecuatoriano Jorge Zabala Baquerizo el fraude es "un modo de actuar dentro de la vida, una conducta que se manifiesta, unas veces, mediante el engaño y, en otras mediante el abuso de confianza".[71]

Y haciendo una oportuna mención en lo que corresponde al fraude pero desde el punto de vista de nuestra legislación Penal del Distrito Federal nos dice: "articulo 230.- Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero...."[72]

Por lo tanto de todo lo analizado anteriormente se puede afirmar que cuando se habla de fraude se esta aludiendo al *modus operandi*, a la dinámica intelectiva, ideal, que caracteriza un determinado comportamiento, implica la presencia dominante de un montaje o artimaña ideal que desencadena determinada modalidad de acción.

En consecuencia puedo decir que si bien el fraude encuentra en el engaño su máxima expresión, este no se agota, ya que el fraude no solo supone como medios

---

[70] Delitos Informáticos, http://www.delitosinformaticos.com. Fecha de consulta 24/04/2002

[71] Delitos Informáticos, http://www.delitosinformaticos.com. Fecha de consulta 24/04/2002

[72] Agenda Penal Federal 2002, compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia, Editorial Grupo ISEF.

para su comisión el engaño o el abuso de confianza como señala Zabala Baquerizo, sino que también supone el uso o empleo de otros medios intelectuales para elaborar ciertas maquinaciones, que como señala el tratadista ecuatoriano deben ir encaminadas a perjudicar el patrimonio ajeno, otro elemento para que se configure el fraude, es la existencia de una lesión o la puesta en peligro de un bien jurídico protegido, doctrinalmente el bien jurídico protegido por las defraudaciones es el patrimonio, considerando este como el conjunto de relaciones jurídicas activas o pasivas que pertenecen a una persona y que son estimables económicamente, por lo tanto cuando se utiliza la formula fraude se hace en relación con específicos bienes jurídicos lesionados o puestos en peligro.

En consecuencia diremos con fundamento en la tratadista española Gutiérrez Francés que la defraudación: "es el perjuicio económico ocasionado mediante fraude, el cual comprende no solo el engaño y el abuso de confianza sino también el uso de otros medios fraudulentos, que no solo afectan el patrimonio individual de una persona, sino que también lesionan otros intereses económicos de carácter macrosocial."[73]

"Constituye fraude el omitir hacer saber a la víctima el estado de error en que se encuentra y del cual se aprovecha para obtener la entrega de una cosa o cualquier lucro indebido, por ello implica la afirmación de que el activo tiene un deber jurídico de manifestar la verdad sacando así de su equivocación al potencial defraudado"[74]

El fraude puede ser definido como engaño. o como acción contraria a la verdad o a la rectitud, muchos estudiosos del derecho penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países, esto no ha sido posible dada la intima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta. y más aún porque va

[73] Delitos Informáticos, http://www.delitosinformaticos.com fecha de consulta 24704/2002.
[74] Reynoso Dávila, Roberto, ***DELITOS PATRIMONIALES***, Editorial Porrúa, México, 199, Pág. 204.

evolucionando debido a la tecnología en la que se le puede encuadrar como el Internet, pero si adecuamos este concepto a la finalidad de nuestra investigación que perseguimos más adelante consideraremos las diversas acepciones que se tienen acerca del fraude informático.

2.7.1. – FRAUDE INFORMÁTICO.

Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina, esto supone que ya no existe un contacto directo entre las personas para cometer determinadas actividades. Como consecuencia de ello se han producido un gran cambio tanto en el mundo empresarial y de negocios, y en otras cosas, se han abierto nuevas perspectivas de consumo mediante el uso de Internet, todos los que navegamos por Internet conocemos que se venden cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas, lo cual es muy lógico, pues se ahorran muchos costos y amplían su potencial de mercado, lógicamente todo depende de tipo de empresa de que se trate y del producto o servicio que venda, pero esta reflexión nos sirve para pensar en la importancia de la red para muchas empresas.

"El fraude es una realidad sencilla, su objetivo es lograr un beneficio ilegal reduciendo las propiedades de la víctima, es claro y patente, el sujeto activo introduce deliberadamente un elemento de confusión antes, durante o después de la comisión del acto delictivo, para ocultarlo o ayudar a su realización"[75]

El fraude sigue pautas crecientes, aunque a veces un tanto caprichosas, limitadas tan solo por la codicia de su autor, por las oportunidades surgidas, accidentales o maquinadas y por el éxito logrado en ocultar las perdidas ya ocasionadas, rara vez hay fraudes menores generalmente son grandes fraudes que han tenido tiempo suficiente para poder desarrollarse, así como la codicia propicia la

[75] Artículos Sobre Internet, http:// www.geocities.com/area51/vault/3230/art-seguridad y privacidad.html. Fecha de consulta 20/03/2002.

explotación delictiva de las oportunidades, la autoprotección es un factor crucial en la cuestión de la ocultación.

Por otro lado nos podemos encontrar con que la supuesta empresa nos manda productos que no son, no podemos reclamar directamente porque no sabemos dónde se ubica la empresa, o simplemente hemos hecho un pago con la tarjeta de crédito y no nos han dado el servicio o producto, todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio de una estafa, pensando en dar número de tarjetas de crédito falsas pero que el robot acepta como válidas, conocido en el mundo Internet como "*Carding*", etc., con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos, por supuesto estos solo son unos ejemplos relativos a la red, pero evidentemente se pueden dar otros casos.

La diferencia que después del análisis de este tema encuentro entre el fraude cometido dentro del sistema conocido como fraude informático y del cometido fuera del mismo, las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño o error sobre un ser humano, y los fraudes cometidos fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo estás las causantes del engaño que determina la disposición patrimonial.

Una característica general de este tipo de fraudes, que resulta interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo, lo que sucede es que una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera la comisión del hecho.

Respecto a los objetos sobre los que recae la acción del fraude informático estos son, generalmente los datos informáticos relativos a activos o valores, en la mayoría de los casos estos datos representan valores intangibles, como depósitos

monetarios, créditos, etc. en otros casos, los datos que son objeto del fraude, representan objetos corporales como mercaderías, dinero en efectivo, etc., que obtiene el autor mediante la manipulación del sistema, estas son en las manipulaciones referidas a datos que representan objetos corporales, las perdidas para la víctima son generalmente menores ya que están limitadas por la cantidad de objetos disponibles, en cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser creado por el autor.

Con todo lo anterior podemos definir a el fraude informático, como la manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de este, realizada con animo de lucro y causando un perjuicio económico a un tercero.

2.7.2. - CONCEPTOS FUNDAMENTALES RELACIONADOS CON LAS FORMAS EN LA COMISIÓN DEL FRAUDE INFORMÁTICO.

2.7.2.1. - HACKER, CRACKER Y PHREAKER.

La red ha dado muchos titulares a los periódicos sobre vulneraciones de sistemas obtención de datos secretos, etc., y como había que llamarlos de alguna forma se les denomina, *Hackers*, dicho nombre se les atribuye a causa de los medios de comunicación, por no informarse sobre un tema antes de escribir o hablar sobre él, y todo esto ha creado en la sociedad una confusión sobre la denominación a estas personas, y se utiliza esta palabra para comportamientos diferentes, que no tienen ni punto de comparación con lo que ese término significa.

Un *Hacker* es una persona muy interesada en el funcionamiento de sistemas operativos; "suele tener mucho conocimiento en lenguajes de programación, además conoce la mayoría de los agujeros de un sistema operativo o de los protocolos de Internet".[76]

[76]INFORMÁTICA DE SISTEMAS, Derechos Y Delitos Informáticos, www.informaticadesistemas.com, fecha de consulta 18703/2002.

Es una "Persona muy hábil con los ordenadores, penetra en sistemas informáticos ajenos sin su consentimiento, tanto virtualmente como físicamente."[77]

Un *Hacker* conoce muy bien el funcionamiento operativo de la Internet, el busca dichos protocolos y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor, se puede decir que los *Hackers* se mueven por fines de autorrealización y conocimiento, nunca provocan daños intencionados en las máquinas, y comparten su información de forma gratuita y desinteresada.

Obviamente la difunden también para que se le reconozcan los méritos de su trabajo, pero eso sucede en todas las actividades humanas, no estoy justificando con esto las actividades que realizan los *Hackers*, pues su actividad por muy pedagógica y desinteresada que pueda parecer vulnera el derecho a la intimidad, un derecho fundamental que todo individuo posee.

El *Cracker* Es una "Persona que elimina las protecciones lógicas y a veces físicas del *software*, que emplea la fuerza bruta, o métodos que dañan el sistema que intenta *hackear*."[78]

Por otro lado tenemos que "Los *Crackers* son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas."[79]

Un aspecto para diferenciar a un *Hacker* de un *Cracker* puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación, y además en varios lenguajes de programación, mientras que el segundo se basa en programas ya creados que pueden adquirir, normalmente, vía

---

[77] Términos Informáticos, http: //angelfire.com/ga/metalsystem/terminologia_T`tecnica_del _*Hacker*.html, fecha de consulta 20/03/2002.

[78] Términos Informáticos, http://www.angelfire.com/ga/metalsystem/terminologia_T`tecnica_del _*Hacker*.html fecha de consulta 20/03/2002.

[79] INFORMÁTICA DE SISTEMAS, Derechos Y Delitos Informáticos, www.infòrmaticadesistemás.com, fecha de consulta 18703/2002.

Internet, otro aspecto diferenciador es que el interés de un *cracker* es destrozar la máquina que hay al otro lado, no es constructivo como un *Hacker*, que trata de mejorar la red dando a conocer sus incursiones y los fallos que ha encontrado.

Entonces podría surgir la pregunta porque existen los *crackers*, y es muy simple porque al igual que en la vida real nos podemos encontrar personas constructivas y otras destructivas, en la red sucede de igual forma, los cracker los podemos comparar como mercenarios, es decir, que obtiene información restringida de los sistemas a los que entran y luego la venden a el mejor postor, o puede ser incluso que haya sido contratado para que busque algo en concreto que interesa a alguien (normalmente empresas que quieren conocer secretos de otras).

Los *Hackers* utilizan métodos o herramientas que más suelen utilizar para sus ataques, los cuales están limitados desde el mismo momento en que se decide a crearlos, porque la mayoría de los *Hackers* saben programación y se hacen sus propios programas para entrar a los sistemas.

Los *Phreaker* "en castellano se denominan piratas, que manipulan los sistemas informáticos de las compañías de teléfonos, ahorrándose una considerable cantidad de dinero, puesto que activa teléfonos convencionales piratas y además teléfonos celulares, constituyendo un grado de peligro para las empresas que manejan esta línea comercial".[80]

2.7.2.2. - CAZADORES DE CONTRASEÑAS.

Un cazador de contraseñas es "un programa que desencripta las contraseñas o elimina su protección".[81]

---

[80] Soto Gálvez, Gerardo, ***LA NECESIDAD DE REFORMA DE LA LEY FEDERAL ANTE LA IMPUNIDAD DE LOS DELITOS INFORMÁTICOS***, Tesis de licenciatura de Atemajac, Guadalajara Jalisco, 1997, según cita de lic. Alberto Rafael Horacio Buendía Madrigal " El Derecho Penal y los Delitos informáticos", Pág. 209.

[81] Informática de Sistemas, Derechos y Delitos Informáticos, www.informaticadesistemas.com, fecha de consulta 18703/2002.

Aunque estos programas no han de desencriptar nada, y además con determinados sistemas de encriptación es imposible invertir el proceso, si no es en forma autorizada, el funcionamiento es el siguiente:

"Tomamos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización."[82]

Los cazadores de contraseñas que podemos encontrar son: *Crack, CrackerJack, PaceCrak95, Qcrack, Perack, Hades, Star Cracker,* etc., hay cazadores de contraseñas para todos los sistemas operativos.

2.7.2.3. - CABALLOS DE TROYA

"Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actué de una forma diferente a como estaba previsto."[83] por ejemplo formatear el disco duro, codificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc.

Los Caballos de Troya son creados por los programadores, ya sea creando ellos un programa original, introduciendo el código maligno, o tomando el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

---

[82] Idem
[83] Idem

2.7.2.4. - HERRAMIENTAS DE DESTRUCCIÓN.

Este suele ser el procedimiento de sabotaje más utilizado por empleados descontentos, "consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocara el cuelgue del sistema"[84]

Podemos distinguir cuatro métodos de destrucción: *mailbombing, flash bombs*, aplicaciones especiales de negación de servicio, y virus.

Mailbombing:" este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario."[85]

Las herramientas que existen para estos ataques son: "*Up yours, KaBoom, Avalanch, Unabomber, eXtreme mail, Homicide, Bombtrack*, etc.,"[86] la mayoría de estas aplicaciones suelen ser gratuitas, y se encuentran por todas las plataformas.

Flash Bombs: " Son herramientas que se utilizan en el *IRC*[87], cuando nos conectamos a un *IRC*, hay varios canales o *chats*, y cada *chat* tiene su operador que es la autoridad en ese *chat*, y decide la persona que ha de marcharse del *chat*."[88] Las personas expulsadas del *chat* toman represalias, y es como aparece el *Flash Bombs*, sus aplicaciones atacan el *IRC* de una forma diferente, pero básicamente lo que pueden hacer es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura *(flooding)* un canal.

---

[84] Idem

[85] Idem

[86] Idem

[87] IRC (Internet Relay Chat). *(Internet)* Es un programa que permite conversaciones simultáneas (a través de su teclado) es decir realizar un chat. Es como estar en varias conversaciones a un mismo tiempo Escrito por Jarkko Oikarinen (jto@tolsum.oulu.fi) en 1.988. Desde su comienzo en Finlandia, ha sido usado en más de 50 paises alrededor del mundo. fue diseñado para reemplazar al programa 'talk', pero ha llegado a ser mucho más que esto. IRC es un sistema de conversación multiusuario, donde la gente se reúne en canales (lugar virtual, normalmente con un tema de conversación) para hablar en grupo o en privado. IRC consigue fama internacional durante la guerra del Golfo Pérsico, cuando las noticias llegaban a través de telegramas a todo el mundo, la gente que estaba en irc, recogía estas noticias en un simple canal de irc.

[88] INFORMÁTICA DE SISTEMAS, Derechos Y Delitos Informáticos, www.informaticadesistemas.com, fecha de consulta 18/03/2002.

Aplicaciones de negación de servicio: este tipo de ataques tratan de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligara a reiniciar la máquina.

Los virus tenemos que por otro lado constituyen un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección.

"Un virus Informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de si mismo en un fichero, los virus se adhieren a cierta clase de archivos, normalmente *EXE y COM*, cuando estos ficheros infectados se transmiten a otro sistema este sistema queda también infectado, y así sucesivamente, los virus entran en acción cuando se realiza una determinada actividad, como puede ser que se ejecute un determinado fichero."[89]

Los virus son programas, y para crearlos los programadores de virus utilizan kits de desarrollo de virus que se distribuyen por Internet, entre los que se pueden destacar los siguientes: "*Virus Creation laboratories, Virus Factory, Virus Creation 2000, Virus Cdestruction Est, o The Windows virus Entine.*"[90]

Por ello cualquiera que se haga de alguno de estos kits y sepa programación pueda crear sus propios virus.

2.7.2.5. - INGENIERÍA SOCIAL.

Básicamente consiste en convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el *password* con alguna excusa convincente.

---

[89] Idem
[90] Idem

2.7.2.6. - SIMULACIÓN DE IDENTIDAD.

Básicamente es usar una terminal de un sistema en nombre de otro usuario, ya sea porque se conoce su clave, o bien porque este se retire de la terminal, pero no se ha desconectado y nos introducimos y ocupamos su lugar, el término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

2.7.2.7. - SNIFFER

Un *sniffer* es "un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su trafico, este trafico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el *sniffer* esta diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad."[91]

Un ataque mediante un sniffer se considera un riesgo muy alto, ya que se pueden utilizar los *sniffers* para algo más que para capturar contraseñas, como obtener números de tarjetas de crédito, información confidencial y privada, etc., actualmente existen *sniffers* para todas las plataformas, ya que los *sniffers* se dedican a capturar datos en computadoras, y por ello es igual la plataforma que se utilice, algunos *sniffers* son los siguientes: "*Gobbler, ETHLOAD, Netman, Esniff.c(se distribuye en código fuente), Sunsniff, Linux_sniffer.c, etc*".[92]

Algo que hace especialmente peligroso a los *sniffers* es que no se pueden detectar, ya que son aplicaciones pasivas y no generan nada, con lo que no dejan ningún tipo de huella, y son especialmente indetectables en *DOS y Windows 95* básicamente y trabajo en grupo, aunque en *UNIX y Windows NT* y posteriores a *Windows 96* dónde hay más posibilidades de detectarlo.

---

[91] Idem

[92] INFORMÁTICA DE SISTEMAS, Derechos Y Delitos Informáticos, www.informaticadesistemas.com, fecha de consulta 18/03/2002.

2.7.2.8. - CARDING.

Es el que se dedica al uso ilegitimo de las tarjetas de crédito, o sus números pertenecientes a otras personas, se relaciona de gran manera con el *hacking*, porque para conseguir números de tarjetas de créditos, se requiere de gran habilidad para poder inducir a las personas por un lado a proporcionar dicho número, que de una u otra manera seria el camino largo, o pueden optar por el camino corto el cual es entrar al sistema de contraseñas y claves de dichos números de tarjetas y obtener la información necesaria para utilizar dichos números y trasladar el dinero a otra cuenta.

2.7.3- MEDIOS ALTERNOS EN LOS CUALES SE HACE USO DE LA INTERNET PARA COMETER FRAUDES INFORMÁTICOS.

2.7.3.1. - ESCÁNERES.

Los escáneres han sido las herramientas más efectivas dentro del *hacking*, se dice que un escáner que vigile a un único puerto tiene más eficacia que miles de *passwords*.

Un *escáner* es "un sistema que encuentra automáticamente los fallos de seguridad de un sistema remoto."[93]

Es decir, una persona desde su habitación puede conocer los agujeros de seguridad de un sistema en otro país, los escáneres son programas que tocan puertos, como pueden ser el *telnet*, almacenando la respuesta que se obtiene, y así una persona puede obtener todo tipo de información de otro sistema, como por ejemplo, que sea posible que un usuario anónimo se registre.

Existen escáneres para todas las plataformas, tanto *UNIX, Windows, Macintosh*, etc. al construirse una persona su propio escáner no es difícil, pero no

[93] INFORMÁTICA DE SISTEMAS, Derechos Y Delitos Informáticos, www.informaticadesistemás.com, fecha de consulta 18/03/2002.

sería muy lógico teniendo en cuenta que hay programas muy buenos, gratuitos y comerciales por ejemplo, *NSS, Strobe, Satan, Jakal, IdentTCPScan, Connect, FSPScan*, etc.

2.7.3.2. - SÚPER ZAPPING.

Se denomina *superzapping* " al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador".[94]

El nombre proviene de una utilidad llamada *SUPERZAP* diseñada para *mainframes* y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un *PC* serían las protocolos o el *Norton Disk Editor*.

2.7.3.3. - PUERTAS FALSAS.

Es una practica acostumbrada en el desarrollo de aplicaciones complejas, consistente en que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc., con objeto de producir un atajo para ir corrigiendo los posibles errores.

Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al *Hacker* de accesos o facilidades en su labor si sabe descubrirlas.

2.7.3.4. - ATAQUES ASINCRÓNICOS.

Este es quizá el procedimiento más complicado y del que menos casos se ha tenido conocimiento, se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica si

[94] Idem

alguien consiguiera hacer caer el sistema y codificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema este continuara con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

2.7.3.5. - RECOGIDA DE BASURA.

Este procedimiento consiste en aprovechar la información abandonada en forma de residuo, existen dos tipos:

" El físico y el electrónico, el físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, el electrónico, se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada. Como ficheros *swapping*, ficheros borrados recuperables (*Undelete)*, ficheros de *spooling* de impresora, etc."[95]

2.7.3.6. - *SPOOFING*

Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña, esto ocurre utilizando la dirección *IP* de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado, en maquinas *UNIX* se suelen utilizar para estos ataques los servicios *"r"* es decir, el *rlogin y rsh*; el primero facilita el procedimiento de registro en un ordenador remoto, y el segundo permite iniciar un *shell* en el ordenador remoto.

---

[95] Idem
IP (Internet Protocol). *(Internet* Es el estándar utilizado por las computadoras para transmitir información a través de Internet. Se suele hacer referencia a un "número IP". IP es una serie de números específicos (cuatro grupos de valores entre 0 y 255, llamados octetos) que se asignan a cada máquina que está conectada a la Red. Un DNS convierte los números IP a nombres comunes
SHELL.- *(Internet)* Frente a los productos comerciales, muchos autores de software han optado por poner a disposición de usuarios potenciales sus programas. Se paga un importe al autor si el programa cuadra con las necesidades del usuario. Suele, pues, existir un periodo de prueba, normalmente unos 30 días, para que la persona compruebe si el programa es el adecuado para atender sus necesidades. Los importes que se abonan suelen ser bastante menores que los de los productos comerciales.

2.7.3.7. - PIRATA INFORMÁTICO.

"Persona dedicada a la copia y distribución de *software* ilegal tanto *software* comercial *crakeado*, como *software* registrado, etc. persona que elimina las protecciones *software*, más conocido como *craker,* delincuente Informático."[96]

2.7.3.8. - BOMBAS LÓGICAS.

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos, el cual consiste en introducir un programa o rutina que en una fecha determinada destruye o modificara la información, o provoca la caída del sistema, ósea produce errores y por consiguiente tendrá que reiniciarse, el programa de nuevo teniendo como consecuencia la perdida de la información hasta ese momento.

2.7.3.9. - ADMINISTRADOR, SYSOP, Ó ROOT.

Es la persona que se encarga del mantenimiento de un sistema Informático, generalmente tienen control total sobre el sistema, ya que tiene acceso a todo tipo de información que este dentro de sus dominios con esto me refiero a la compañía donde este ubicado el servidor, ellos son los que se encargan de depurar la información que se encuentra en las bandejas de entrada del correo electrónico, y por consecuencia tienen acceso a cualquier cuenta, debido que ellos controlan todas las contraseñas de los usuarios.

2.7.3.10.- CORTAFUEGO, FIRE WALL, Ó BASTION.

"Es un sistema avanzado de seguridad que impide a personas no acreditadas el acceso al sistema"[97]

96: Términos Informáticos, http://wwwangelfire.com/ga/metalsystem/terminologia_ T`tecnica_ del _*Hacker*.html , fecha de consulta 20/03/2002

97 Términos Informáticos, http:: //www.angelfire.com/ga/metalsystem/terminologia_T`tecnica_ del _*Hacker*.html , fecha de consulta 20/03/2002

Este sistema novedoso, como se conoce, hace bastante referencia a que impide el acceso a toda persona no autorizada como yo o cualquier persona, pero entonces cualquier persona si autorizada o autorizada puede tener acceso además del usuario, esto es algo ilógico por lo que podemos creer que cualquier persona ajena al sistema de cualquier tipo dentro de Internet, que se apodere de las claves o contraseñas puede tener acceso.

2.7.3.11. - ANARQUIA O ANARKIA.

" Además de los significados oscuros, como son caos o lió, la anarkia es una rama del pensamiento *cyberpunk o craker*, consiste en la lucha contra la sociedad, generalmente es el texto sobre la *anarkia*, son sobre explosivos, armas, técnicas de lucha, etc. Pensamiento ideológico y político, resumiendo se podría decir que se basa en la búsqueda de la libertad y en la eliminación de cualquier poder central o estatal, aunque muchos de los que dicen ser *anarkistas* son en una demagogia barata, el movimiento *anarkista* tiene una gran profundidad de pensamiento..., la ideología *anarkista*, esta muy relacionada con el mundo *cracker*, ya que algunos de sus pilares son los mismos que los de la cultura *Hacker*, y muchos de los mejores *Hackers* son y fueron *anarkistas*."[98]

Si entendemos esta ideología desde un punto de vista en donde el *Hacker* es un sujeto que tiene elevados conocimientos de computación, y los ejerce de forma en que proporciona a todos los demás usuarios de la red los elementos para allegarnos de información que tal vez por la situación económica en que vivimos y sabiendo que no somos una primera potencia mundial, considero a mi punto de vista que es bueno el que nos proporcione las diversas herramientas para que de alguna forma nos abramos más al espacio de conocimiento que tenemos muy atrasado, en lo que no estoy de acuerdo es que dichos conocimientos en informática sean empleados para conducir al error a los usuarios y se afecte el patrimonio de las personas, pero si

98; Términos Informáticos, http://www.angelfire.com/ga/metalsystem/terminologia_ T'tecnica_ del _*Hacker*.html, fecha de consulta 20/03/2002

vemos que todo *Hacker* es una persona con los conocimientos de informática y sistemas, El problema surge en la degeneración del individuo a la inutilización de sus conocimientos para su beneficio propio, mediante usos ilícitos de la Internet.

2.7.3.12. - *CYBERPUNK*

Es al igual que la anarkia un tipo de ideología o de sub-cultura, que se basa en el culto a la tecnología, a la ciencia pero lo que hace la diferencia de la anarkia es el odio o cualquier forma de poder organizado, produciendo una mala imagen de este grupo.

El pensamiento *cyberpunk* al igual que la anarquía son susceptibles de ser interpretados por sujetos con criterios equivocados, que desvirtúan tanto a uno como a otro en su estructura y forma funcional.

CAPITULO III

III.-MARCO LEGAL SOBRE EL FRAUDE EN LOS DELITOS INFORMÁTICOS.

3.1. - CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

Históricamente se conocen algunos antecedentes de declaraciones sobre las libertades del hombre, antecedentes que influyen sin duda alguna en los inicios de la regulación informática, en el siglo XVIII, las filosofías políticas convergen en dos documentos primordiales para las definiciones de derechos fundamentales del hombre y su garantía frente al estado, el primero es la declaración de los derechos del hombre y del ciudadano producto de la revolución Francesa, la cual se mantiene viva y vigente como texto legal por la remisión que hace el preámbulo de la Constitución de Francia, el segundo de los documentos mencionados, será el de la Constitución de los Estados Unidos de América.

La declaración de los derechos del hombre y del ciudadano: "En 1789 la declaración de los derechos del hombre y del ciudadano, presenta una profunda unidad en su inspiración, una destacable coherencia, hasta tal punto que con razón se puede ver en ella un resumen convincente de la filosofía de las luces, en sus artículos X y XI de dicha declaración de los derechos del hombre y del ciudadano, establece, ningún hombre debe ser molestado en sus opiniones es uno de los derechos más preciosos del hombre todo ciudadano puede, pues, escribir e imprimir libremente, salvo la responsabilidad por el abuso de esta libertad en los casos determinados por la ley."[99]

De la Constitución de los Estados Unidos de Norteamérica, cabe mencionar que la primera y la cuarta enmienda de 1791 establecen la libertad de expresión y la libertad de prensa, sí como la protección a las personas, cosas, papeles y posesiones con molestias sin debido orden.

Siempre ha parecido una parte dogmática, durante la historia Constitucional mexicana, que ha contenido tanto la libertad de expresión como la libertad de

[99] C. MEJAN, Luis Manuel, ***El Derecho a la Intimidad y la Informática***, Editorial Porrúa, México, 1994, Pág. 13-14.

imprenta, como la garantía de legalidad en las molestias a las propiedades o posesiones.

Aunque cabe aclarar que la importancia de la información es tal que se ha reformado nuestra Constitución y se reconoce el derecho a la información, contenida en los artículos 6°, para establecer este concepto o garantía individual, política y social.

"Articulo 6° de la Constitución Política de los Estados Unidos Mexicanos.-La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público, el derecho a la información será garantizado por el estado"[100]

Este precepto nos da pauta para poder establecer el fundamento constitucional en el que versa nuestra investigación sobre el fraude informático que debería ser tipificado en nuestra legislación penal, ya que en el precepto "... los derechos de terceros, provoquen algún delito... " nos deja muy amplio el campo en el que se podría tipificar dicho tema de investigación como un delito, con un apartado exclusivo en nuestro Código Penal para el Distrito Federal y ahora en el Nuevo Código Penal para el Distrito Federal, ya que el engaño al que se lleva al usuario de Internet en cuestiones de compraventas afecta sus derechos, y provoca un delito que es el de fraude pero en una modalidad novedosa debido al medio físico-material, ya que es un engaño mediante un medio de comunicación donde se utiliza la Internet. Y sobre todo su característica especial que se trata de explicar en la presente investigación radica en que no existe un ente material o tangible que pueda responder de las defraudaciones, que se cometen en contra de los usuarios.

Por lo tanto el derecho informático tiene la función de proporcionar seguridad, al usuario, al creador de programas, al inversionista, la seguridad de que cualquier

---

[100] ***Constitución Política de los Estados Unidos Mexicanos***, Editorial Porrúa, 138ª edición, México, 2002.

conducta que pudiera afectar sus intereses será prevista y en su caso castigada, que las controversias que pudiesen surgir por el uso de la informática, serán aquellas resueltas por tribunales que se especialicen en la materia o que por lo menos tengan conocimiento de la misma, y en general de proporcionar a la comunidad participante y usuaria de esta tecnología, la certeza de estar en un ambiente regulado alejado de la anarquía reinante en un sistema sin normalidad. Pero para ello, los fundamentos deben estar contenidos antes que nada en nuestra Constitución ya que no se pretende que todos los negocios vía Internet nos vayan a defraudar, sino que se tomen las medidas necesarias para que se pueda proteger al usuario de Internet de uno de tantos delitos a los que es susceptible, en este caso el del fraude informático, y nos basamos en ello debido a que en el mismo artículo 6 de nuestra Constitución Política en donde establece "...el derecho a la información será garantizado por el Estado", esto implica que el estado es el guardián que debe cuidar nuestros derechos en todo ámbito, tanto el de ser usuarios de Internet, tanto como el de ser comprador o vendedor por el mismo medio o el de proteger información de todo tipo, para tener seguridad de que no estemos desprotegidos en las diversas transacciones que realicemos, y no solo limitándose a defendernos cuando exista un ente físico al que podamos "reclamar" sino que debe tomar las medidas, para que de acuerdo a las mismas nos protejamos del sujeto que comete el delito.

A su vez el artículo 16 de nuestra Carta Magna nos indica "(REFORMADO PRIMER PÁRRAFO, D.O.F. 3 DE SEPTIEMBRE DE 1993) Art. 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento..."[101]

De esta manera podemos observar que en el referido artículo se encuentra regulada la garantía de seguridad jurídica, esto es sin duda un ordenamiento amplio y suficiente que garantiza el derecho a la privacidad, a la intimidad de los individuos, pues regula con precisión los requisitos que debe reunir el mandamiento legal

[101] *Compila VI*, Poder Judicial de la Federación, Suprema Corte de Justicia de la Nación Legislación Federal y del Distrito Federal, 2002.

transcrito, mediante el cual pueda afectarse o molestarse a la persona con la utilización de algún medio electrónico, vía Internet.

3.2.- ORGANIZACIÓN DE NACIONES UNIDAS (ONU).

El ámbito internacional de comisión de estos delitos informáticos tiene como características, la falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos, ya que dada las diferentes legislaciones de una nación a otra existen conductas tipificadas como delito en algunos países mientras que en otras no es así, por lo tanto existe una ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

"La ONU, en el marco del octavo congreso sobre prevención del delito y justicia penal, celebrado en 1990 en la Habana, Cuba, estableció 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."[102]

Actualmente, la comunidad internacional no ha conciliado conceptos o parámetros fijos para determinar a los delitos informáticos en el derecho penal, tales como; 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.

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando

---

[102] Universidad Autónoma De Sinaloa. http://uny.uasnet.mx/prof/cln/der/silvia/lexis.htm. Fecha de consulta 20 de marzo del 2002.

una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de un modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que es tema principal de esta investigación, sino la utilización real por el hombre de los sistemas de información con fines delictivos.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de los individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y del detrimento tanto humano como patrimonial del ser humano, asimismo, la amenaza constante es en un futuro directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso desde el

derecho administrativo, estas distintas medidas de protección no tienen porque ser de ningún modo excluyentes unas de otras, sino que, por el contrario, estas deben estar estrechamente vinculadas, por eso dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Por su parte el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos "señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada así mismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- " Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos

- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

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

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permiten la puesta en vigor de la cooperación internacional."[103]

En síntesis es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio, las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente en estos delitos, por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura critica de un país, como para los legisladores, las autoridades policíacas encargadas de las investigaciones y los funcionarios judiciales.

3.2.1.- TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS.

El progreso cada día es más importante y debido a que los sistemas computacionales permiten hoy procesar y mantener a disposición de la sociedad, una cantidad creciente de información de toda naturaleza al alcance concreto de millones de interesados y de usuarios, sobre las más diversas esferas del conocimiento humano, en lo científico, en lo técnico en lo profesional y en lo personal, lo cual esta siendo incorporado a sistemas informáticos que, en la practica cotidiana, es puesta a disposición a quien lo desee, lo cual hasta hace unos años este acceso solo podía ser ofrecido a grandes costos y tras horas de largas búsquedas, en la actualidad ese enorme caudal de conocimientos puede obtenerse, en segundos o minutos, transfiriéndolo incluso documentalmente, y llegar a un receptor mediante sistemas sencillos de manejo, que sea capaz de responder casi a toda la gama de interrogantes que se planten a los archivos informáticos, Pero esto a la vez es un arma de doble filo puesto que si el mayor tesoro que podemos tener es

[103] Organización De Naciones Unidas. http://www.monografías.com. Fecha de consulta 26 de julio del 2002. y comentarios de Helen Peña, Silvia Palazuelos, Rosalía Alarcón, División de Estudios de Postgrado, Facultad de Derecho, UNAM, 21 mayo 1997. (comentarios realizados por las profesionistas sobre el tema) fecha de consulta 25 de agosto del 2002. sgpalazu@themis.derecho.unam.mx.

el conocimiento, muchas de las variantes que se utilizan son perjudiciales para el mismo humano, y con este tipo de tecnología es aun más propicia la comisión de actividades ilícitas, y de una manera alarmante, es por ello que a continuación haremos referencia a lo que las Naciones Unidas han determinado respecto al tema, haciendo una clasificación de los delitos que esta institución considera como métodos informáticos delictivos.

Los tipos de delitos informáticos reconocidos por las Naciones Unidas son:[105]

FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS.	
DELITO	**CARACTERÍSTICAS**
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
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 pueda realizar una función no autorizada al mismo tiempo que se realiza una función normal.
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 utilizan ampliamente en equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnética de las tarjetas bancarias y de las tarjetas de crédito.
FRAUDE EFECTUADO POR	Aprovecha las repeticiones automáticas de los procesos de cómputo,

[105] Naciones Unidas, ***Revista Internacional de Política Criminal Manual de las Naciones Unidas sobre Prevención del delito y control de delitos informáticos***, Oficina de las naciones Unidas en Viena, Centro de Desarrollo Social y Asuntos Humanitarios Naciones Unidas, Nueva York, números 43 y 44. se refiere: 1. - Fraudes cometidos mediante manipulación de computadoras, 2. - Falsificaciones informáticas, 3. - Daños o modificaciones de programas o datos computarizados. 4. - Acceso no autorizado a servicios y sistemas informáticos, 5. - Piratas informáticos o *Hackers*, 6. - Reproducción no autorizada de programas informáticos de protección legal.

MANIPULACIÓN INFORMÁTICA	es una técnica especializada que se denominan técnica del salchichón en la que rodajas muy finas apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
	FALSIFICACIONES INFORMÁTICAS
COMO OBJETO	Cuando se alteran datos de los documentos almacenados en forma capturizada.
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 alteraciones fraudulentas, estas fotocopiadoras pueden hacer copia 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 alta calidad que sólo un experto puede diferenciarlos de los documentos auténticos.
DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS.	
SABOTAJE INFORMÁTICO	Es el acto de borrar, suprimir modificar sin autorización funciones o datos de computador con intención de obstaculizar el funcionamiento normal del sistema las técnicas que permiten cometer sabotajes informáticos;
VIRUS	Es una serie de claves programáticas que pueden adherirse a los programas legítimos 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, como utilizando el método de Caballo de Troya
GUSANOS	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de dato 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 maligno, ahora bien las consecuencias del ataque de un gusano puede ser tan grave como las de el ataque de un virus, por ejemplo un programa gusano que subsiguientemente es destruir puede dar instrucciones a un sistema Informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
BOMBA LÓGICA O CRONOLÓGICA	Existen conocimientos especializados ya que requiere la programación de la destrucción o modificación de los datos en un momento dado de futuro, ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten, por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño y ara 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.
ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS	Por motivos diversos, desde la simple curiosidad, como es el caso de muchos piratas informáticos (*Hackers*) hasta el sabotaje del 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 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 lo que los usuarios emplearon contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos, algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales, el problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas, al respecto, consideramos que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

3.3.- ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE)

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

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

La OCDE, es una organización Internacional Intergubernamental que reúne a los países más industrializados de economía de mercado, en la OCDE, los

representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objeto de maximizar su conocimiento económico y coadyuvar a su desarrollo y al de países no miembros.

De esta forma, la OCDE hizo toda una relación mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales autorizando, la intercepción y la reproducción no autorizada de un programa de computadora protegido, con objeto de que se finalizara la preparación del informe de la OCDE, el consejo de Europa inicio su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar que tipo de conducta debía prohibirse en la legislación penal y la forma en que debía de conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el consejo de Europa aprobó la recomendación 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.

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 elegir un marco de seguridad para los sistemas informáticos el mismo año.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que el seno de la Organización de las Naciones Unidas (ONU), en donde 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.

también la UNESCO, en sus pronunciamientos relativos a las Autopistas de la información, ha declarado que el aumento del acceso a redes y bases de datos interconectadas incrementa el valor de los principios éticos y legales, incluyendo:

- La privacidad de la información y el derecho que tiene cada individuo a chequear sus propios datos como derecho humano fundamental.
- La lucha contra la piratería internacional y otros delitos.
- La protección de los derechos de los creadores de software

En fecha muy reciente, la propia UNESCO se ha pronunciado en contra del uso que sé esta dando a estas redes de alcance global para la difusión de pornografía, y el comercio de mujeres, e incluso de niños.

Las posibles implicaciones 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 iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma, las conclusiones político-jurídicas desembocaron en una lista de 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 (lista mínima), 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.

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 (lista optativa o facultativa), espionaje informático, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el consejo de Europa inicio su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos o determinar que tipo de conducta debía prohibirse en la legislación penal y la forma en que debía de seguirse 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 ocupo también de otras, como la protección de la esfera personal, las victimas, 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"[106] 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 la intención de ofrecer las bases para que los estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos del mismo año.

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México y 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 universales, debe destacarse que en el seno de la organización de las Naciones Unidas, 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 burocracia de los distintos países y que por ello se había difundido la comisión de los actos delictivos.

---

[106] Sistemas informàticos. http://InformaticadeSistemas.com fecha de consulta 11 de julio del 2002.

Además, la injerencia 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 era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, 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 ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido la ausencia de medidas que pudieran contrarrestarlos, se considero que el uso deshonesto de las computadoras podría tener consecuencias desastrosas, a este respecto, el congreso recomendó que se establecerían 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, por ello surge la falta de una definición jurídica de la conducta delictiva, también hay carencia 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.

Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema, en consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada, durante la elaboración de dicho

régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Hamburgo en 1992, adoptó diversas recomendaciones respectó 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, sino hasta con la adopción de otras medidas (principio de subsidiaridad), además, las nuevas disposiciones deberán ser precisas, claras y con la fidelidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que estos queden circunscritos primordialmente a los actos deliberados.

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, especialmente a alteración de datos de computadora y el espionaje informático, así como que por lo que se refiere al delito de acceso no autorizado, es conveniente precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

3.4. - COMPARACIÓN CON LEGISLACIONES DE OTROS PAÍSES CON RESPECTO A EL DELITO DE FRAUDE INFORMÁTICO.

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras. Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos, todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Las personas que cometen el fraude informático y en general los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuente, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre si es la naturaleza de los delitos cometidos, de esta forma la persona que ingresa en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes, el nivel típico de aptitudes del delincuente informático,es tema de controversia ya que para algunos

el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas. , Motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

En los Estados Unidos como Europa y Norte América existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años. En el contexto internacional son pocos los países que cuentan con una legislación apropiada, entre los que se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile entre otros.

3.4.1. -ESTADOS UNIDOS

Este país adopto en 1994 e Acta Federal de Abuso Computacional que modifico el Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transición de un programa, información, códigos o comandos que causan daños a la computadora, a lo sistemas informáticos, a las redes, información, datos o programas, la nueva ley es un adelanto porque esta directamente en contra de los actos de transmisión de virus.

Estados Unidos sanciona los ataques tecnológicos (violencia tecnológica), las estafas electrónicas, defraudaciones y otros actos relacionados con los dispositivos de acceso a sistemas informáticos.

Así mismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática

"En el mes de julio del año 2000, el senado y la cámara de representantes de este país tras un año largo de deliberaciones establece el acta de firmas electrónicas en el comercio global y nacional, la ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el *B2B*) y entre empresas y consumidores (para *B2C*)"[107]

El objetivo de los legisladores al realizar dichas enmiendas es la de proteger a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente, asimismo los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo el auge a los delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y a las bases de datos y que la protección legal de todos sus tipos y formas lo cual es vital para la protección de los individuos tanto en su intimidad así como para el bienestar de las instituciones financieras, negocios agencias gubernamentales y otras relacionadas con el estado de California que legalmente utiliza esas computadoras, sistemas y bases de datos. Pero hay que hacer la mención que aquí se regulan los virus informáticos primordialmente en todo lo que tendría que ver con la modificación, destrucción copiado, o trasmisión de datos o alterar la operación normal de las computadoras, y los sistemas o las redes informáticas.

[107] Informatica Jurídica, http:// www.monografias.com. Fecha de consulta 11 de julio del 2002.

3.4.2. -ALEMANIA.

Este país sanciono en 1986 la Ley contra la Criminalidad Económica del 15 de mayo del mismo año, que contempla los siguientes delitos:

- Espionaje de datos,
- Estafa informática,
- Alteración de datos, es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje Informático. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos también es punible la tentativa.
- Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el trafico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos.
- utilización abusiva de cheques o tarjetas de crédito

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal hallar un equivalente análogo al triple requisito de acción engañosa, causan el error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

El legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos, de esta forma. Dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma calificada.

3.4.3. - AUSTRIA.

La ley de reforma del Código Penal sancionada el 22 de Diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas. y contempla además los siguientes delitos:

- destrucción de datos.- no sólo se regulan los datos personales sino también los no personales y los programas.

- Estafa informática.

La estafa informática sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos, además contempla sanciones para quienes cometen este hecho utilizando su profesión.

De igual forma se han publicado en las épocas de los 70's y 80's, en donde se establecieron sanciones de multa y de privación de la libertad hasta un año, para los

sujetos que incumplieran con las disposiciones relacionadas con la detención, almacenamiento y procesamiento de datos por medios informáticos.

3.4.4. - GRAN BRETAÑA.

Debido a un caso de *hacking* en 1991, comenzó a regir en este país la *Computer Misuse Act* (ley de Abusos Informáticos) mediante esta ley el intento exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas, Esta ley tiene un apartado que especifica la modificación de datos sin autorización. establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora y de esa manera":

- Impedir la operación de cualquier computadora, o
- Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos.
- Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos.

La ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación inglesa, posteriormente la ley fue reformada en 1994 para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos.

3.4.5. - HOLANDA.

El 1ª de Marzo de 1993 entró en vigencia la ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El *hacking*,

- El *phereaker* (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio)

- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría)

- La distribución de virus. Esta penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. si se demuestra que el virus se escapo por error, la pena no superara el mes de prisión, pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

3.4.6. - FRANCIA

En 5 de enero de 1988, reforma en su ley número 88-19 la ley relativa al fraude informático, en la que se consideran aspectos como:

- Intromisión fraudulenta que suprima o modifique datos, ya que en este articulo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

- Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos,

- Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que este contiene, o sus modos de procesamiento o de transmisión.

- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje), en este articulo se

sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

- Falsificación de documentos informatizados, en este articulo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

- Uso de documentos informatizados falsos, en este articulo se sanciona a quien concientemente haga uso de documentos falsos.

3.4.7. - ESPAÑA.

"El honor y la intimidad de las personas son derechos fundamentales para su ordenamiento jurídico, tal como queda recogido en el articulo 18 de la Constitución Española, y como ocurre en la totalidad de los ordenamientos considerados democráticos en la actualidad."[108]

Precisamente este objetivo garantista que persigue el legislador español, al desarrollar el articulado de la norma fundamental en sucesivas leyes, como señala Castán al referirse a estos derechos "son aquellos derechos fundamentales de la persona humana considerada tanto en su aspecto individual como comunitario, que corresponden a ésta por razón de su propia naturaleza y que deben ser reconocidos y respetados por todo poder o autoridad y toda norma jurídica positiva, cediendo, no obstante, en su ejercicio ante las exigencias del bien común"[109]

Lo anterior nos muestra dos características esenciales de este tipo de derechos; su vocación de universalidad y su subordinación a los intereses generales, a pesar de su consideración como derechos subjetivos, ambas características son

[108] Sánchez Goyanes, Enrique, ***Constitución Española Comentada***, 21ª edición, Editorial Paraninfo, Madrid, España, 2001, Pág. 300.

[109] Fernández Galiano, Antonio de Castro Cid Benito, ***LECCIONES DE TEORÍA DEL DERECHO Y DERECHO NATURAL***, Editorial Universitas, S, A, 1994, Pág. 423.

manifiestas en la adaptación de la intimidad, como derecho fundamental especialmente protegido, por la legislación informática.

"De este derecho inicial a la intimidad la doctrina ha diseñado un derecho a la privacidad con el que se pretende no sólo rechazar cualquier intromisión a la vida privada de cada cual, sino también introducir mecanismos de control del sujeto afectado sobre las informaciones relativas a su persona o a su familia, se prohíbe una conducta amenazando con una sanción el incumplimiento de esa prohibición"[110], a partir de aquí, hablar de responsabilidad es evidente.

En el nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicara pena de prisión o multa, en lo referente a:

1. La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

2. El nuevo Código Penal de España sanciona en forma detallada esta categoría delictiva (violación de secretos/ espionaje/ divulgación), aplicando pena de prisión y multa.

3. En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de algúna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Con Relación el fraude informático el articulo 248 de el Nuevo Código Penal Español (aprobado por la ley Orgánica 10/1995, de 23 de Noviembre/BOE número 281, de 24 de Noviembre de 1995) nos dice:

---

[110] Murillo, Pablo Lucas, ***EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA,*** Editorial Tecnos, 1990, Pág. 117.

" 1. - Cometen estafa los que, con ánimo de lucro, utilizan el engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. - también se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero."[111]

"Articulo 255. - será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1. - valiéndose de mecanismos instalados para realizar la defraudación,
2. - Alterando maliciosamente las indicaciones o aparatos contadores,
3. - Empleando cualesquiera otros medios clandestinos."[112]

3.4.8. - CHILE.

Chile fue el primer país latinoamericano en sancionar una ley contra delitos informáticos, la cual entro en vigencia el 7 de junio de 1993, esta ley se refiere a los siguientes delitos:

-La destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas de prisión, asimismo dentro de esas consideraciones se encuentran los virus,

-Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

---

[111] ***Nuevo Código Penal Español*** (aprobado por la ley Orgánica 10/1995, de 23 de Noviembre / BOE número 281, de 24 de Noviembre de 1995

[112] Idem..

-Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información

3.4.9. - CUBA.

Desde 1993 entró en vigor el reglamento de protección de datos y sistemas informáticos así como la articulación nacional de comisión de protección de Datos, que desde el año 1988 viene trabajando en el país y cuyo esfuerzo mereció el reconocimiento del PII-UNESCO al concedérsele a este en el año 1993, la realización del proyecto "Laboratorio Latinoamericano de Protección contra Virus Informáticos", institución que hasta la fecha ha formado especialistas del área y ha servido al desarrollo de sistemas autóctonos de protección informática, así como el diseño e implementación de políticas y estrategias de seguridad informática.

3.4.10. - COSTA RICA

En el aspecto legislativo sobre el derecho Informático tenemos que existe una propuesta de legislación del recurso de Habeas Data presentada a la asamblea legislativa por iniciativa del señor diputado Dr. Constantino Urcuyo, proyecto de ley que pretende reformar la ley de la Jurisdicción Constitucional, con el fin de incorporar dicho recurso del Habeas Data en Costa Rica, el cual resulta interesante debido a que se pretende recoger una necesidad de proteger la dignidad, intimidad y autodeterminación de los ciudadanos frente a los retos que ofrece el procesamiento automatizado de datos personales, lo cual a la fecha se encuentre instituido en legal forma.

3.4.11. - PERÚ.

El ordenamiento jurídico peruano tipifica los siguientes delitos, los cuales se encuentran dentro del concepto de delitos informáticos y son:

- "Delito de violación a la intimidad
- Delito de hurto calificado por transferencia electrónica de fondos,
- Delito contra los derechos de autor,
- Delito de falsificación de documentos informáticos,
- Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos,
- Delito de daños aplicable al hardware." [113]

De acuerdo al análisis anterior y conforme a todos estos ordenamientos, fuentes doctrinales y principios mencionados, se puede deducir finalmente la creación de una ley especial que regule y proteja el bien jurídico a tutelar en la seguridad patrimonial tanto al particular como al estado, derechos que se han visto violados, agredidos y ofendidos en distintas circunstancias por la realización de dicho delito informático como lo es el fraude informático.

3.5.- NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

La legislación Nacional en México no estatuye los llamados "delitos informáticos" y mucho menos el fraude informático, a excepción del Código Penal del Estado de Sinaloa, y ante tal situación todas las conductas ilícitas relativas al manejo de la computadora y a la informática, que se realicen en el país o en alguna entidad federativa quedaran impunes a falta de tipo penal a nivel local, acarreando consecuencias económicas, tanto en los sectores públicos y privados, abarcando el

[113] Código Penal, Edición 2000, Editorial Nueva Madrid, Perú, Pág. 41.

ámbito Internacional trayendo como consecuencia efectos internacionales relevantes en el ámbito informático.

Sin perjuicio de lo anterior, algunos países como Estados Unidos, Alemania, Francia, Austria y España entre otros, de los cuales analizamos con anterioridad consideran que tal problema debe atacarse de un nivel local hasta llegar al nivel Internacional debido al flujo de información electrónica en todos los países, y los efectos jurídicos, políticos y económicos que pueden causarse, sin embargo, tales países manejan gran cantidad de información y la mayoría de su población tienen computadoras propias, por ello, debe comenzarse a legislar en México a un nivel local, y posteriormente firmar tratados internacionales con los demás países para combatir los delitos informáticos y en especial y con mayor trascendencia el fraude informático.

En nuestro país a sido poca la legislación que regula sobre el tema de fraude informático, sino es que hasta nula, a pesar del enorme crecimiento de la tecnología informática, la conciencia que se ha dado a nivel mundial, ha dado enormes avances en sus respectivas legislaciones, como los países europeos y Estados Unidos, considerando que este tipo de problemas no tienen fronteras, y además de causar enormes daños económicos, sociales y políticos, y tomando en cuenta que hoy en día México cuenta con una red mundial de información en la que circula enormes cantidades de datos en sus sistemas informáticos, es urgente e imperiosa la necesidad de prevenir y sancionar todas aquellas conductas que lesionen bienes jurídicos tradicionales como bienes jurídicos de reciente tutelación.

La problemática de los delitos informáticos y en especial el tema que nos preocupa sobre el fraude informático requiere un estudio especial, en nuestro país con la finalidad de adecuar todas aquellas conductas ilícitas relacionadas, tomando todo tipo de medidas en nuestra legislación local y hasta federal. Los programas de computación, las bases de datos y las infracciones derivadas, en la actualidad este tipo de delitos se encuentran regulados en el Código Civil, pero no las regula

directamente sino reconoce la creación de la firma electrónica al igual que el código de comercio y dentro de la Ley Federal de Derechos de Autor, se encuentra contemplado el uso de los derechos de autor, pero nunca de una manera directa y real el uso de los medios informáticos y de la Internet como medios y objetos básicos e indispensables para la comisión de dichas conductas delictivas.

Dentro del Nuevo Código Penal para el Distrito federal, nos hemos podido percatar de las innumerables reformas, adiciones y derogaciones que el mismo ha venido sufriendo a través de la historia penal mexicana, aunque varias de esas reformas han demostrado una mejoría en nuestro sistema penal, también hay que considerar que otro tanto de esas reformas han demostrado que el aumento de penas no han servido como una forma de discusión, puesto que en nuestro Código Penal vemos el aumento de penas, como ya hemos mencionado, pero la delincuencia sigue creciendo conforme la tecnología va avanzando.

Para disuadir la comisión de delitos, lo eficaz es que no exista impunidad, que encontremos en servidores públicos, una labor eficiente en la procuración y administración de justicia para que se sancione a los responsables de los delitos, es por ello que es indispensable y urgente el crear unas cuantas medidas de prevención, más que nada porque si tomamos en cuenta que este tipo de personas toman la información como un arma indispensable para la comisión del delito del fraude informático, es de esta manera como nos encontramos, en la tarea de buscar y encontrar un forma o medida de prevenir los delitos informáticos, que como he venido señalando a lo largo de este trabajo de investigación a causado innumerables esfuerzos para definir, tipificar y sancionar dichos delitos.

Podemos observar la desproporción e inequidad entre las penalidades y sanciones pecuniarias enumeradas por esta norma, para sancionar intima y selectivamente las diferentes modalidades o hipótesis materiales, por lo que en estricto apego a la ley debería de ser un mismo delito, asimismo se han establecido criterios discriminatorios determinados arbitrariamente en atención a la calidad de las

personas físicas y morales, o bien de las entidades públicas que hayan sido victimas de los infractores cibernéticos.

Podemos darnos cuenta que en la Ley Federal de Derechos de Autor tipifique este tipo de delitos, mientras tanto en el ámbito penal las defraudaciones vía Internet tienen un auge impresionante, y lo más importante que hay que considerar con esto, es que en el ámbito de derechos de autor sean más rigurosos, ya que obviamente sabemos que solo son unas personas que tienen ese privilegio, lo que es contrario en el fraude informático donde cualquier tipo de individuos de cualquier clase social o estrato económico puede tener acceso a una computadora y hacerse de bienes por este medio cibernético, y aquí lo más importante que sucede con estos sujetos es que invierten sus ahorros en bienes de los cuales nunca reciben o simplemente son estafados por sujetos que sabemos que tienen una inteligencia superior al promedio de sujetos que Cometerían un robo común, Aquí se basan en conocimientos cibernéticos y bases de datos cuya finalidad es la de estafar a los usuarios, con ello no digo que una persona que trate de ingresar información de manera gratuita con el fin de transmitirla y hacer que se propague, sino lo que realmente debe de interesar es proteger a los usuario en su patrimonio en lo referente a las compras que se realizan por esta vía de comunicación para que no sean sujetos de engaños.

De esta manera aun siguen vigentes los principios que dieron lugar al nacimiento del Código Penal de 1931, hasta el Nuevo Código del 3 de Julio del 2002 que abroga a este código penal en sus reformas y demás leyes que se opongan al presente ordenamiento, pero hasta la fecha dichos principios que dieron vida a este ordenamiento siguen vigentes, pues podemos observar que no es una teoría, ni una escuela jurídica las que van a dar respuesta a las necesidades de contar con un Código Penal adecuado para el Distrito Federal, y esto se puede lograr si se recoge la practica y es minuciosamente analizado.

Nuestro Nuevo Código Penal para el Distrito Federal no se refiere al respecto ya que no hace mención en la última reforma del mismo acerca del tema, sin hacer

una clasificación o apartado especial para cada delito como lo es el fraude informático, y en los delitos en contra de las personas en su patrimonio, antes de la reforma del 16 de julio del 2002 en lo referente al fraude informático como a continuación muestro no hace ninguna referencia al tema, dentro de los numerales en donde debería de estar considerado:

"CAPÍTULO III

FRAUDE

ARTÍCULO 230. Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

I. De veinticinco a setenta y cinco días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el salario mínimo, o no sea posible determinar su valor;

II. Prisión de cuatro meses a dos años seis meses y de setenta y cinco a doscientos días multa, cuando el valor de lo defraudado exceda de cincuenta pero no de quinientas veces el salario mínimo;

III. Prisión de dos años seis meses a cinco años y de doscientos a quinientos días multa, cuando el valor de lo defraudado exceda de quinientas pero no de cinco mil veces el salario mínimo; y

IV. Prisión de cinco a once años y de quinientos a ochocientos días multa, cuando el valor de lo defraudado exceda de cinco mil veces el salario mínimo.

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

I. Por título oneroso enajene alguna cosa de la que no tiene derecho a disponer o la arriende, hipoteque, empeñe o grave de cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la gravó, parte de ellos o un lucro equivalente;

II. Obtenga de otro una cantidad de dinero o cualquier otro lucro, como consecuencia directa e inmediata del otorgamiento o endoso a nombre propio o de otro, de un documento nominativo, a la orden o al portador, contra una persona supuesta o que el otorgante sabe que no ha de pagarlo;

III. Venda a dos personas una misma cosa, sea mueble o inmueble, y reciba el precio de la primera, de la segunda

enajenación o de ambas, o parte de él, o cualquier otro lucro, con perjuicio del primero o del segundo comprador;

IV. Al que se haga servir alguna cosa o admita un servicio en cualquier establecimiento comercial y no pague el importe debidamente pactado comprobado;
V. En carácter de fabricante, comerciante, empresario, contratista o constructor de una obra, suministre o emplee en ésta materiales o realice construcciones de calidad o cantidad inferior a las estipuladas, si ha recibido el precio convenido o parte de él, o no realice las obras que amparen la cantidad pagada;

VI. Provoque deliberadamente cualquier acontecimiento, haciéndolo aparecer como caso fortuito o fuerza mayor, para liberarse de obligaciones o cobrar fianzas o seguros;

VII. Por medio de supuesta evocación de espíritus, adivinaciones o curaciones, explote las preocupaciones, superstición o ignorancia de las personas;

VIII. Venda o traspase una negociación sin autorización de los acreedores de ella o sin que el nuevo adquirente se comprometa a responder de los créditos, siempre que estos últimos resulten insolutos;

IX. Valiéndose de la ignorancia o de las malas condiciones económicas de un trabajador a su servicio, le pague cantidades inferiores a las que legalmente le corresponden por las labores que ejecuta o le haga otorgar recibos o comprobantes de pago de cualquier clase, que amparen sumas de dinero superiores a las que efectivamente entrega;

X. Valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usurarias por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los vigentes en el sistema financiero bancario;

XI. Como intermediarios en operaciones de traslación de dominio de bienes inmuebles o de gravámenes reales sobre éstos que obtengan dinero, títulos o valores por el importe de su precio a cuenta de él o para constituir ese gravamen, si no los destinaren al objeto de la operación concertada por su disposición en provecho propio o de otro.

Para los efectos de este delito se entenderá que un intermediario no ha dado su destino o ha dispuesto del dinero, títulos o valores obtenidos por el importe del precio o a cuenta del inmueble objeto de la traslación de dominio o del gravamen real, si no realiza su depósito en cualquier institución facultada para ello dentro de los treinta días siguientes a su recepción en favor de su propietario o poseedor, a menos que lo hubiese entregado dentro de ese término al vendedor o al deudor del gravamen real o devuelto al comprador o al acreedor del mismo gravamen.

El depósito se entregará por la institución de que se trate a su propietario o al comprador.

XII. Construya o venda edificios en condominio obteniendo dinero, títulos o valores por el importe de su precio o a cuenta de él, sin destinarlo al objeto de la operación concertada.

En este caso, es aplicable lo dispuesto en el párrafo segundo de la fracción anterior.

Las instituciones y organismos auxiliares de crédito, las de fianzas y las de seguros, así como los organismos oficiales y descentralizados autorizados legalmente para operar con inmuebles, quedan exceptuados de la obligación de constituir el depósito a que se refiere la fracción anterior.

XIII. Con el fin de procurarse ilícitamente una cosa u obtener un lucro indebido libre un cheque contra una cuenta bancaria, que sea rechazado por la institución, en los términos de la legislación aplicable, por no tener el librador cuenta en la institución o por carecer éste de fondos suficientes para su pago de conformidad con la legislación aplicable. La certificación relativa a la inexistencia de la cuenta o a la falta de fondos suficientes para el pago deberá realizarse exclusivamente por personal específicamente autorizado para tal efecto por la institución de crédito de que se trate;

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

XV. Por sí, o por interpósita persona, sin el previo permiso de las autoridades administrativas competentes o sin satisfacer los requisitos señalados en el permiso obtenido, fraccione o divida en lotes un terreno urbano o rústico, con o sin construcciones, propio o ajeno y transfiera o prometa transferir la propiedad, la posesión o cualquier otro derecho sobre alguno de esos lotes. "

Como vemos el delito de fraude esta ampliamente tipificado pero no concibe en ninguna de sus fracciones al fraude informático, es por ello que es prudente que dentro de toda esta clasificación se haga un apartado especial para que sea tipificado como delito dentro de nuestro Nuevo Código Penal del Distrito Federal.

Por otro lado tenemos que la Ley Federal de protección al Consumidor se refiere:

" ***CAPITULO VIII BIS.***
DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVÉS DEL USO DE MEDIOS ELECTRÓNICOS, ÓPTICOS O DE CUALQUIER OTRA TECNOLOGÍA

Articulo 76 Bis.- las disposiciones del presente Capitulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, en la celebración de dichas transacciones se cumplirá con lo siguiente:

I.- El proveedor utilizara la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II.- El proveedor utilizara alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informara a este, previamente a la celebración de la transacción, de las caracterlsticas generales de dichos elementos,

III.- El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones,

IV.- El proveedor evitara las practicas comerciales engañosas respecto de las caracterlsticas de los productos que desea recibir, así como la de no recibir avisos comerciales, y

V.- El consumidor tendrá derecho a conocer toda a información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor,

VI.- El proveedor respetara la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como de no recibir avisos comerciales,

VII.- El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara suficiente obre los servicios ofrecidos, y cuidara las practicas de mercadotecnia dirigidas a población vulnerable, con niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población."[114]

[114] Legislación. WWW.INFORMATICA-JURIDICA.COM/LEGISLACIÓN.ASP. Fecha de consulta 13 de julio del 2002.

Por otra parte teniendo en cuenta que el estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia verdad de los mismos y estableciendo las sanciones correspondientes consideramos que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, este deberá legislar en materia penal federal, tales ilícitos, dada la naturaleza y consecuencias de los mismos y otros elementos indispensables para su ejecución como son las vías generales de comunicación; quedando así la jurisdicción federal como única competente para conocerlos en juicio.

Sinaloa es la única entidad federativa de México que estatuye especifica y concretamente a los delitos informáticos, y ante la importancia que tiene que el Congreso Local de tal Estado haya legislado sobre la materia de delitos, considero importante y pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

"TITULO DÉCIMO
DELITOS CONTRA EL PATRIMONIO
CAPITULO V
DELITO INFORMÁTICO

Art. 217: Comete delito Informático, la persona que dolosamente y sin derecho:
I.- 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
II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis a dos años de prisión y de noventa a trescientos días multa".[115]

Al respecto podemos decir que se engloba bastante bien lo que seria el tipo delictivo, pero en lo correspondiente a la sanción que debe merecer se me hace muy exagerada, lo cual no debe de ser así, en este aspecto lo mejor seria solo hacer la multa y trabajo en favor de la comunidad, y dentro de nuestro del Código Federal debería considerarse este tipo dentro de los delitos patrimoniales. A mi parecer se

[115] ***Código Penal para el Estado de Sinaloa***, Editorial Porrúa, México, 2002.

ubico al delito informático en general en el Código Penal de Sinaloa bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez cabe destacar que los delitos informáticos son una eminente violación al patrimonio de los sujetos, y en especifico el fraude informático.

CAPITULO IV

IV.- PROBLEMÁTICA SOBRE EL FRAUDE INFORMÁTICO EN LA ACTUALIDAD MEXICANA.

4.1. – PROBLEMÁTICA QUE CONLLEVA LA CARENCIA DE UNA REGULACIÓN DEL FRAUDE INFORMÁTICO EN EL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

La principal limitante para poder encontrar la problemática sobre esta investigación es la débil infraestructura legal que posee nuestro país con respecto a la identificación y ataque a este tipo de delito, no obstante se poseen los criterios suficientes sobre la base de la experiencia de otras naciones para el adecuado análisis e interpretación de este tipo de acto delictivo.

El desarrollo del presente capitulo, tiene como fin el de incorporar la figura jurídica de los delitos informáticos y en especifico el del fraude informático a la legislación penal mexicana, y por ello es importante vincular tal delito con las instituciones jurídico-penales existentes en nuestro Código Penal para el Distrito Federal.

La red mundial *Internet,* esta favoreciendo la comisión de infracciones de diferente índole en materia informática, el submundo que se crea por dicha red hace que las conductas ciertamente contra derecho sean difíciles de perseguir, no sólo por la complejidad del entorno donde se produce sino por la ausencia de tipificación de las modalidades y de los medios utilizados para cometer tales conductas. En el primer caso se esta ante conductas cometidas por sujetos que a diverso titulo regulan el acceso a la red definiendo los protocolos y distribuyendo las direcciones *IP.* En el segundo caso, se refiere esencialmente a la actividad de los usuarios los cuales dañan la red y a sus operadores con comportamientos ostensiblemente desviados, los comportamientos indebidos pueden ser la difusión en la red de virus que generan daños permanentes, provocando inconvenientes para los usuarios de la red. En la última categoría de ilícitos influyen subespecies diversas entre los derechos que resultan violados por la utilización de la red Internet, estando sobre esa modalidad los derechos sobre las marcas, derechos de autor y los derechos de la personalidad.

Siempre la electrónica, la informática y la telemática han participado activamente en la economía contemporánea efectivamente, en una economía globalizada como la de hoy, la producción en dichos sectores junto con el reconocimiento del valor de la información hacen sin duda que los recursos resultantes de esas actividades, asuman una importancia estratégica y competitiva tanto para el Estado como para la comunidad, y que estas deban de protegerse.

Cabe hacer mención a las distintas etapas por las que a atravesado la denominación de nuestro cuerpo legal punitivo en una breve remembranza y así una vez explicado poder entrar en la materia que nos concierne.

"La norma jurídica abarca tanto la conducta humana hipotizada *ingenere* como la consecuencia jurídica, aquélla adquiere relevancia en merito de la amenaza de coerción estatal determinada por el precepto legal como resultado del maleficio; sin aquélla, este no puede prevalecer, y una pena sin conducta referible pierde toda significación, en ocasiones, al legislador se le olvida prever los caracteres de la conducta, o por inadecuada técnica incurre en el error de no configurarla, para que pueda estimarse como típica.... y entonces aun, unida a la imprecisa enunciación que quiso crear el tipo, la pena no podrá aplicarse porque faltaron los requisitos de la tipicidad que el derecho liberal exige."[116]

De lo anterior se desprende del mismo modo, que en ciertas formas típicas carecen de una pena congruente con el delito que se comete, y solo para los efectos del análisis doctrinario se puede hablar de delito sin pena y de pena sin delito; pero en la realidad jurídica y de la concepción unitaria de la norma de derecho positivo, seria un disparate hablar de delincuente sin delito, y de delito al que no le sobreviene pena y de pena sin un tipo.

"La norma jurídica no existe sin sus elementos sustanciales, imprescindibles, la actividad jurisdiccional se detiene ante una conducta no hipotizada como

---

[116] PALACIOS VARGAS, J. Ramón, ***DELITOS CONTRA LA VIDA Y LA INTEGRIDAD CORPORAL***, 2ª edición, Editorial Trillas, México, 1985. Pág. 11.

delictuosa, y lo mismo frente a la conducta a la que se subsigue la coerción estatal propia del derecho penal..."[117]

Sin embargo seria indebido considerar que en la sistemática jurídica no puede practicarse la deserción de elementos de la norma, de los elementos del delito, aunque no exista pena, y de los caracteres de esta sin el delito en la ley. Lo que pretendo con este análisis es que el estudio analítico lo exige la doctrina para la correcta interpretación de la ley, para los fines dogmáticos, y lo que se trata de lograr es destacar que sin la existencia de la tipicidad, resulta inútil cualquier esfuerzo de legislar, ya que todo se convertirá en un estudio de fines restringidos a la dogmática, sin repercusiones en el derecho, ya que no podemos crear sin estructuras o bases un nuevo tipo de delito si no tenemos los fundamentos necesarios para poder crear las raíces necesarias para que pueda realmente funcionar la pena que se le aplique, y no solo se convierta en un esfuerzo mas del legislador para solo crear leyes sin fundamento y sin repercusión legal, y que solo se busque como finalidad la evasión de esa misma ley. Yo considero que para que se pueda tipificar el delito de fraude informático y en especifico la estafa informática debe de basarse esa ley en fundamentos lógicos, teóricos y prácticos, en como solucionarlo, y no ir con la mentalidad de como sancionarlo sin poner remedio a ese mal, yo no estoy de acuerdo en que en los delitos de orden patrimonial se imponga pena de prisión como exclusiva, lo más congruente y sensato, seria que el sujeto que hizo ese mal lo pague con su trabajo el tiempo que se estime sea el necesario.

"Es toda una herejía hablar hoy de delitos naturales, ya sea con el significado de Garófalo o con el de Carrara; es revivir el iusnaturalismo bajo el velo del racionalismo si se toman las ideas carrarianas, el sociologismo superado si se entiende con el pensamiento de Garófalo, ...para una filosofía general y jurídica cobijada bajo su amparo, resulta innegable y se ha de afirmar que hay ciertos bienes a los que el Estado debe la tutela del derecho, independientemente de que lo reconozca así lo desprende dentro del marco de la positividad de sus preceptos

[117] Idem.

legales, precisamente, la supresión de estos derechos naturales del hombre, por parte de ciertos regímenes, pone en su sitio la importancia de su reconocimiento y su vida anterior a la norma."[118]

A lo largo de la historia de nuestra legislación mexicana y de la legislación internacional se han encontrado diversas disposiciones con el propósito de regular la conducta del hombre, para así poder convivir en armonía y en beneficio de la sociedad, es a través del tiempo de las costumbres y de la tecnología, como las necesidades del mismo van creciendo, de modo que es imperativo e importante crear legislaciones y procedimientos que regulan las distintas actividades del ser humano de manera que el proceso con el que el hombre se va desarrollando sea conforme a derecho y con las regulaciones que esta ofrece.

"El carácter sancionatorio del Derecho Penal, el Código Penal de ayer y del hoy, lo tutelan a través de la prohibición que entraña el tipo sancionado con una de las más intensas penas, pues bien, los bienes, o los intereses, jurídicos que más significación tienen dentro de esa concepción son los del hombre mismo, los del individuo, el maestro de Pisa los clasifica en orden decreciente, así; la vida, la integridad corporal, la libertad, el honor, la familia y la propiedad (propiedad y posesión)."[119]

El derecho penal totalitario coloca en primer lugar la organización del Estado, y los peores delitos son los que atentan contra ese orden, y los delitos sociales serian aquellos que no afectaran al individuo, sino a la colectividad, al grupo, en sus derechos o intereses, pero si analizamos un poco la cita anterior podemos ver que el tema que nos interesa en el desarrollo de nuestro trabajo es el fraude informático, y si lo localizamos en el ámbito de la libertad, y en el ámbito de la propiedad y la posesión, tomando en cuenta que en esta ultima localizaríamos el patrimonio de los sujetos, entonces si analizamos detenidamente que si no hay libertad en este sentido

[118] Ibidem, Pág. 12.
[119] Ibidem, Pág. 13.

la entenderíamos como el libre acceso a programas de computo, información, y la propiedad y posesión las entendemos como el patrimonio de cada uno de los sujetos que navegan en la Internet y requieren de servicios o bienes, con esto podemos ver que este no es el problema esencial, el problema fundamental es que se tenga acceso a todo tipo de información, pero sin lucrar con ella y que en el momento que entramos a bases de datos para obtener una remuneración mediante un engaño a los consumidores estamos en presencia del fraude informático, que en el presente trabajo de investigación, ofrezco para aportar los lineamientos necesarios para que sea regulado en nuestro Código Penal para el Distrito Federal.

Jiménez de Azúa ha dicho " Este hecho grandioso y terrible, que pone en manos del Estado el *ius punendi*, debe ser sometido a investigación, empezando por su pretendida legitimidad, no es suficiente afirmar que se trata de un derecho subjetivo del Estado, es preciso calar hondo en los fundamentos, a pesar del famoso apotegma *homines non requirunt tiones carum rerum quas semper vident*, (no basta que haya existido siempre para que se le estime como justo, y tampoco es licito)- como creyeron algunos de los partidarios del tecnicismo jurídico, con Manzini a la cabeza, trato de apartar estos problemas de la preocupación del penalista, afirmando que la investigación filosófica es repudiada por superflua y aún dañina, o decir, con Francisco Magri, que la penalidad no se justifica por otras filosofías, sino por un criterio de necesidad."[120]

Es cierto que la razón de muchos de los delitos tipificados que existen han sido producto de la necesidad de que sean penalizados, pero esa misma necesidad esto nos lleva a que sin fundamentos lógicos y congruentes se legisle solo por legislar, y que a la larga esa finalidad sea contraproducente, porque esa penalización va generando deficiencia y peor aun nuevos delitos, que tienen que ser penalizados, y no solo esto sino que también en ello influye mucho el avance tecnológico como es el caso de nuestra investigación, ya que nuevos adelantos científicos y tecnológicos acarrean nuevas acciones que deben ser calificadas como conductas típicas, pero el

[120] Carranca Y Rivas, Raúl, ***EL DRAMA PENAL***, Editorial Porrúa, México, 1982, Pág. 103.

problema no es una ni otra sino la finalidad que se le de a cada una. Y si tomamos la idea de que se legisla por necesidad, debemos partir también de que esa necesidad debe estar bien fundamentada, valorando los argumentos a favor y en contra que conlleve dicha toma de decisión para legislar cierta conducta típica.

La importancia para que se pueda concretar una iniciativa de ley que regule al fraude informático, se ve reflejada en otras legislaciones pero nunca de una manera directa en lo que se refiere a el fraude informático, en el Código Penal del Distrito Federal y ahora con el Nuevo Código Penal para el Distrito Federal no se regula. La propuesta que se hace de la tipificación de este tema como delito, ya que busca más que nada la protección a los usuarios, y más que buscar un castigo privativo de libertad para los que cometen dicho delito, la propuesta seria resarcir el daño, pero para que pueda resarcirse este, deben implementarse métodos, mecanismos, técnicas, para que una vez que sean descubiertos estos tipos de sujetos, paguen un monto económico a el sujeto victima del fraude además de hacer que trabaje en favor de la comunidad, además de que en determinados casos se dé la privación de la libertad, y esta última tomarla solo en los casos donde se amerite debido al monto que se defraudo y tomando en cuenta la seguridad de que el individuo no llegare a querer evadirse de la pena impuesta.

El crimen informático aumenta con delitos que van desde robos de computadoras portátiles hasta millonarios fraudes a través de la Internet, y debido al potencial de aprovechamiento de Internet para la información, la educación, el entretenimiento y la actividad económica a escala mundial es muy importante; por ello, es necesario garantizar un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público. Los suministradores de acceso a Internet y los suministradores de servicios de ordenador central desempeñan un papel decisivo para dar acceso a los usuarios a los contenidos de Internet, sin embargo no debemos de olvidar que la responsabilidad primordial de los contenidos recae sobre los autores y los suministradores de contenidos, por ello es

imprescindible señalar con exactitud la cadena de responsabilidades con el fin de situar la responsabilidad de los contenidos ilícitos en sus creadores.

Algunos países como Alemania, han introducido una legislación muy amplia para bloquear todo acceso directo a Internet a través de los suministradores de acceso mediante la introducción de la exigencia de servidores "*proxy*" análogos a los que analizan las grandes organizaciones por razones de seguridad, junto con "listas negras" centralizadas.

Debido a esto se han formado dos vertientes la primera que esta a favor de una regulación en general de la Internet abarcando:

a) Acceso no autorizado,
b) Destrucción de datos
c) Infracción de los derechos de autor
d) Infracción del *Copyright* de bases de datos
e) Intercepción de *e-mail*
f) Fraudes electrónicos
g) Transferencias de fondos
h) Espionaje
i) Espionaje industrial
j) Terrorismo
k) Narcotráfico
l) Trafico de armas
ll) Proselitismo de sectas
m) Propaganda de grupos extremistas.

Y la segunda vertiente que proporciona argumentos en contra a la regulación informática son en tres tipos de casos:

a) El derecho a la intimidad

b) La libertad de Expresión
c) La libertad de acceso a la información.

Con respecto a el punto anterior, puedo decir que podemos tener un derecho a la intimidad, una libertad de expresión, y una libertad de acceso a la información sin que ello caiga en un abuso, que nos perjudique, tanto en nuestros derechos de autor como en nuestro patrimonio, la cuestión es que podemos tener acceso a todo ello con la debida responsabilidad de nuestra parte, considero que toda persona que maneja una computadora exceptuando el caso de los menores, sabe delimitar, por lo menos de manera esencial el fin que le esta dando a esa información, lo que yo pretendo es que las personas que requieran un bien o servicio vía Internet tengan la seguridad de que las empresas que se supone están ofreciendo ese bien o servicio sean legales y que realmente existan y que no sean solo creadas para que se aprovechen de los usuarios en lo que están requiriendo, y estafen a los sujetos, con productos o servicios que nunca recibirán, y lo peor aun que proporcionen sus cuentas, teniendo la seguridad de recibir ese bien ó servicio y que después ya no tengan nada en sus cuentas de tarjetas de crédito ó bancarias.

La problemática que se ha venido suscitando a través de los tan comentados delitos informáticos dentro de los sistemas computacionales, ha generado como lo he comentado, un desastre internacional que en ocasiones a traído consigo consecuencias catastróficas implicando la seguridad internacional, y a pesar de que haya ordenamientos que contengan dichos delitos tienen severas lagunas con relación a la materia informática, ya que como hemos venido mencionando se protegen aspectos de suma importancia como lo es la intimidad, seguridad patrimonial, dignidad e inclusive daños morales.

Esta posibilidad se abre cuando lo que actualmente se aprecia son las regulaciones fragmentarias que han surgido en otros Estados de nuestra República Mexicana, algunas relativas a la libertad personal, buscando sancionar las agresiones a la intimidad y a la vida privada, y otras dirigidas a tutelar la información simple y llanamente, la doctrina sobre el tema se concreta, en tutelar el derecho de la

información en sus tres formas que son: "en primer lugar, el derecho de informar, en el sentido de buscar y suministrar información, (derecho activo), el derecho a ser informados (derecho pasivo) y el derecho definido por la doctrina como "reflexivo" y que es el derecho de toda persona a informarse sobre si mismo, es decir, a controlar, rectificar o negarse a difundir los datos introducidos en un archivo electrónico".[121]

La problemática de las bases de datos y de las relaciones entre el derecho de información y tutela de la reserva de los datos, aparece estrictamente conectada a la potencial lesividad de la elaboración informática, que acentúa los objetivos de peligrosidad intrínsecamente conexos a cada forma de recolección y conservación de la información.

A falta de una legislación especifica en el ámbito Internacional, en Internet existen códigos de ética cuyo cumplimiento esta castigado con la censura popular, lo cual acaba siendo en algunos casos, más eficaz que una norma de derecho positivo, si sabemos que podemos ser juzgados por nuestros compañeros, y somos consientes de que nuestro comportamiento podría ser calificado de novato, informal ó no agradable, entonces tendremos que acatar ciertas normas éticas que la misma sociedad cibernética nos impone, ello hace que la tónica normal en Internet sea de respeto entre los usuarios de la red, siendo los demás casos la excepción.

Otro tipo de sanción son los sistemas de seguridad informática, los propios sistemas de control implementados en la red, garantizan la seguridad aceptable, aunque no impiden que los archivos que circulen por la red puedan tener algún virus, o acceso ilimitado a códigos de tarjetas de crédito y en muchos casos puedan ser neutralizados por un programa generador de passwords, hay algunos organismos y corporaciones como la NSA, FIRST (*forum of incident Response and Security Teams*) y CERT (*Computer Emergency Response Team)* tienen equipos de especialistas dedicados a la localización de *crakers* y protegen contra sabotajes e

---

121 Guerrero, M, Fernanda María, Santos, Jaime Eduardo, Sánchez, César Julio, Zuluaga, Víctor, Cuervo, Abel. ***PENALIZACIÓN DE LA CRIMINALIDAD INFORMÁTICA***, proyecto académico, Editorial Ediciones Jurídicas, Colombia, 1998, pp. 51.

intervención en caso de siniestros informáticos, por otra parte algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

4.1.1. - SUJETO ACTIVO

Las personas que cometen los "Delitos Informáticos". Son aquellas que poseen ciertas características que no presenta el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter especial, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades que faciliten la comisión de este tipo de delitos.

"La criminalidad informática es una forma nueva de criminalidad denominada de cuello blanco o de calzones cortos, esta modalidad ha sido calificada como una subespecie de la llamada *criminalidad económica*, "[122]

Este tipo de delitos forman parte de la llamada cifra negra de la criminalidad, es decir son conductas cuya comisión no se denuncia, especialmente porque las entidades afectadas no aceptan, ni se arriesgan a poner en tela de juicio su credibilidad y la confianza del público en general.

El sujeto activo: "el hombre es sujeto activo del delito, porque únicamente el se encuentra provisto de capacidad y voluntad y puede, con su acción u omisión, infringir el ordenamiento jurídico penal, se dice que una persona es sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible, ya sea como autor intelectual, material, participe, cómplice o encubridor."[123]

---

[122] Ibidem, pp. 24.

[123] Pavón Vasconcelos, ***DERECHO PENAL MEXICANO***, 10a Edición, Editorial Porrúa, México, 1991, Pág. 17.

Con el tiempo se ha podido comprobar que los que son autores de los delitos informáticos en general son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos, de esta forma la persona que ingresa en un sistema Informático sin intenciones delictivas es muy diferente de cualquier sujeto con una actividad común, el nivel de aptitudes del delincuente Informático trae aparejada una controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos o un sujeto que tenga bastante familiaridad con el mundo cibernético.

Desde finales de la década de los 70's, cuando se introdujo al mercado la computadora personal (PC), la acción de estos sujetos ha crecido en proporciones asombrosas, y en una proporción semejante, también han crecido quienes los catalogan de tecno criminales, así también como aquellos que los consideran rebeldes positivos, que luchan para que los adelantos tecnológicos en materia de la informática y computación lleguen a las manos no solo de los poderosos, sino también a cualquier tipo de usuario de una computadora.

De acuerdo al profesor Mario Garrido Montt, entiende por sujeto activo del delito de fraude informático: "quien realiza toda o una parte de la acción delictiva que lleva a la conclusión del ilícito".[124]

La primera cuestión se presenta al determinar si el sujeto activo debe ser considerado como un sujeto calificado técnicamente, o bien, puede tratarse de cualquier persona contrario a la mayoría de los delitos que se encuentran tipificados en las leyes penales de todos los países del mundo, el perfil del delincuente Informático posee cierta configuración y virtudes que lo hacen único dentro de este enfoque, esto es los sujetos activos tienen habilidades para el manejo de los

[124] Huerta Miranda, Marcelo, Libano Manssur, Claudio, ***DELITOS INFORMÁTICOS***, 2ª edición, Editorial Jurídica Cono Sur, Chile, 1998, pp. 185.

sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de sistemas informatizados, aun cuando en muchos de los casos no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, todo ello en razón a las características siguientes:

" a) hasta cierto grado, se han descubierto una serie de patrones que van desde la apariencia hasta sus hábitos de lectura, es el sujeto típico inteligente, abstraído y apasionado por la ciencia informática y computacional,

b) Su conducta delictiva no tiene un alto grado de peligrosidad, como en los delitos donde existe una violencia física o moral, ya que un delincuente Informático al realizar la comisión de un delito, no utiliza violencia.

c) Su personalidad es original y única, es decir, poseen una inteligencia superior a la normal, y además tienen una gran preparación especial en la materia informática y computacional.
d) Poseen una imaginación extraordinaria, compleja y muy exuberante, es decir, son muy despiertos, impacientes, audaces y aventureros,

e) Son personas que generalmente no tienen antecedentes penales, y que llevan una vida laboral y estable,

f) La gran mayoría de ellos son personas de un nivel económico muy elevado,

g) así también físicamente poseen similitudes como:

1) Tienden a ser delgados
2) Su piel es pálida,
3) En su mayoría son varones,

4) Normalmente son de ascendencia sajona y oriental,
5) Visten de manera informal,
6) La mayoría tienen cabello corto, barba y bigote,
7) Usan lentes,
8) Como complemento a su imagen, siempre traen consigo un portafolios,

h) Todos poseen una educación universitaria y el manejo de herramientas técnicos, pero la mayoría de ellos son autodidactas."[125]

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos, de esta forma, la persona que entra en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes, o que mediante la compraventa de bienes muebles o inmuebles, se apodera del patrimonio de los individuos que tienen la necesidad de adquirir dichos bienes vía Internet por las diversas razones que estos tengan., con esto no pretendo que caigamos en una clasificación como la que realizó Lombroso en su debido momento, y encasillemos a un cierto tipo de sujetos, que reuniendo ciertas características físicas puedan considerarse indiscriminadamente como delincuentes informáticos, sino por el contrario, con ello pretendo que analicemos que muchos de los sujetos que pueden cometer algún tipo delictivo en el ámbito informático, no necesariamente reúnen esas características, como en la actualidad los podemos encontrar de muy diversos tipos, tanto físicamente como de diversos estratos sociales.

El nivel típico de aptitudes del delincuente Informático es un tema de controversia, ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática, en tanto que otros traducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto

[125] REVISTA MECÁNICA POPULAR, Año 55, núm. 4, Abril 1998, Televisa, S. A, México, p 51.

tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Las tecnologías de la información han facilitado la aparición de nuevas conductas que, con independencia del mayor o menor reproche social generado, han obligado a los países avanzados a adoptar en sus legislaciones lo que yo en este trabajo de investigación también persigo, con respecto al fraude informático.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos en general y el fraude informático en lo particular los estudiosos en la materia los han categorizado como "DELITOS DE CUELLO BLANCO" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland, este conocido criminólogo señala un sin número de conductas que considera como delitos de cuello blanco, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y marcas, de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros. De esta misma manera este autor nos dice que tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete, entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto estatus socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por su baja educación, ni mucho menos por poca inteligencia, y ni por inestabilidad emocional.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la victima estén sujetos a leyes nacionales diferentes además, si bien los acuerdos de cooperación

internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionales por los delitos informáticos, sus posibilidades son limitadas.

Existe un sin número de formas de clasificación de los delitos, ya que estos tienen una subdivisión atendiendo a diversos factores como lo son:

1. - LA CONDUCTA	delitos de acción, y de omisión estos a su vez se clasifican en delitos de simple omisión y delitos de comisión por omisión.
2. - LOS SUJETOS QUE PARTICIPAN	delitos unisubjetivos y plurisubjetivos
3. - EL RESULTADO	delitos formales y delitos materiales
4. - SU CULPABILIDAD	delitos dolosos, delitos culposos, y preterintencionales
5. - SU DURACIÓN	delitos instantáneos, delitos permanentes, y delitos continuados
6. - EL DAÑO QUE PRODUCEN	delitos de lesión, y delitos de peligro
7. – FORMA DE PERSECUCIÓN	delitos por querella y de oficio
8. - SU GRAVEDAD	faltas, delitos y crímenes.

Existen otros tipos de clasificaciones atendiendo a los enfoques que se presentan:

1. - POR EL TIPO DE DELITO:	a.- Fraude, b.- Robo, c.-Abuso de confianza, d.- Daños en propiedad ajena, e.- Extorsión,

	f.- Sabotaje
2. - POR EL TIPO DE CONDUCTA.	a.- De destrucción, b.- De modificación, c.- De alteración, d.- De creación, e.- De diseño, f.- De ejecución, g.- De uso,
3. - POR LA FORMA DE OPERAR.	a.- En ataque físico, b.- Técnica salami, c.-Virus Informático, d.- Manipulación de datos falsos, e.- Por el uso de símbolos o códigos secretos.
4. - POR EL RESULTADO OBTENIDO.	a.- Afectación a la propiedad intelectual, b.- Daño físico y destrucción, c.- La ganancia o el lucro indebido.

4.1.2. - SUJETO PASIVO.

En primer lugar tendríamos que distinguir entre sujeto pasivo o victima del delito, sobre el que recaería la conducta de acción que realiza el sujeto activo y en el caso del fraude informático, las victimas son todos los individuos, instituciones crediticias, estados, etc., que usan sistemas automatizados de información, generalmente conectados a servidores que proporcionan las llaves a toda la información que pueda contener un procesador, mientras este conectado.

El sujeto pasivo del delito que nos ocupa es sumamente importante para el estudio de nuestro tema ya que mediante el podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones que anteriormente analizamos.

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo, el sujeto pasivo puede ser

una o varias personas naturales o jurídicas en el caso de las empresas u organizaciones y particulares, la gravedad que revisten estos ilícitos permite que sus consecuencias recaigan no sólo sobre el sujeto pasivo directo de la acción típica, sino también sobre los Estados y la sociedad en la que nos encontramos.

Por lo expuesto, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar un análisis minucioso sobre la criminalidad informática en general y en lo particular sobre el fraude informático, tomando en cuenta el análisis objetivo de las necesidades de protección y de las fuentes de peligro, una protección contra los criminales, que se valen de la buena fe de los individuos que realizan sus compras vía Internet aportando sus números de tarjetas de crédito, y esto presupone ante todo que las victimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales victimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las victimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de victimas y estimulando la denuncia de los delitos se promovería la confianza publica en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para destacar, investigar y prevenir los delitos informáticos.

En primer termino tenemos que distinguir que sujeto pasivo o victima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso del fraude informático las victimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa es sumamente importante, ya que mediante él podemos conocer el ilícito que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que en el ámbito Informático muchos de los delitos son descubiertos casuísticamente por el desconocimiento del *modus operandi* de los sujetos activos. Por lo anterior se reconoce que la mayor parte de este tipo de delitos no son descubiertos o no son denunciados a las autoridades, muchas veces porque no hay autoridades competentes que puedan hacer algo contra estos maleantes, se reconoce que 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 que presupone ante todo que las victimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

Debemos destacar que los organismos internacionales han adoptado métodos similares en el sentido de que educando a la comunidad de victimas y estimulando la denuncia de los delitos se promovería la confianza publica en la capacidad de los encargados de hacer cumplir la ley y de las autoridades para detectar, investigar y prevenir los delitos informáticos.

De lo anterior tenemos que el sujeto pasivo del fraude informático, es la persona o entidad sobre la cual recae la conducta que realiza el sujeto activo, la mayoría de los fraudes informáticos que no son descubiertos, como ya se menciono, pero es importante que se debe en gran parte a que los mismos no son denunciados, debido al miedo al desprestigio y a su consecuente pérdida económica, derivada de

la duda que se sembraría debido a la inseguridad que ofrecen sus sistemas de seguridad al proporcionar un servicio a un usuario cualquiera.

Pero el derecho a la información tutelado inclusive por nuestra Constitución también se ve afectado por los delitos informáticos y que es practica común entre los delincuentes informáticos el romper barreras de seguridad de diversas bases de datos privadas y gubernamentales, para sustraer información que tenga determinado valor personal para el delincuente, Es debido a esta bifuncionalidad de bienes jurídicamente tutelados que las leyes que se han creado en México hasta el momento no han resultado lo suficientemente eficaces para prevenir el delito del fraude informático pues los Códigos Penal del Estado de Sinaloa y el Penal Federal se han enfocado ha tutelar el derecho a la información por sobre el patrimonio.

4.2. - PARA UN USUARIO REPRESENTA UNA GRAN VENTAJA QUE SE REGLAMENTE EL USO DE LA INFORMACIÓN Y MÁS AÚN REGLAMENTARLA PARA LOS FINES A QUE VA DESTINADA, PARA QUE NO QUEDE IMPUNE ESTE TIPO DE DELITO COMO LO ES EL FRAUDE INFORMÁTICO.

Visto así el panorama, las situaciones detectadas que favorecen la comisión de las infracciones antes mencionadas; y, desde luego que conocen y utilizan los delincuentes, que entre otros son los siguientes:

1. *LA MALA CALIDAD DE LAS TARJETAS*, el *pvc* no es el de mejor calidad o las entidades financieras por ahorrar costos, adquieren al que no ofrece garantías mínimas de durabilidad y de resistencia.

2. *LA COMERCIALIZACIÓN LIBRE Y SIN CONTROL DE MAQUINAS Y MATERIAS PRIMAS PARA OFRECER SERVICIOS FINANCIEROS,* Los cajeros adquiridos por las entidades financieras, son en la mayoría

de los casos máquinas obsoletas que ya han salido del mercado en otros países.

3. *LA FALTA DE CUANTIFICACIÓN DE LOS RIESGOS CUANDO NO SE PROPORCIONAN LAS DEBIDAS SEGURIDADES,* cuando las empresas deciden ofrecer a la clientela productos y servicios a través de sistemas electrónicos, televisión y teléfono.

4. *LA VERIFICACIÓN DE DATOS,* en el comercio esta procede vía telefónica, y en este evento se protege más al comerciante que al cliente, en la medida en que se revelan datos de este que el establecimiento comercial no debe saber como saldos en tarjetas de crédito.
5. *LA SELECCIÓN DEL PERSONAL,* estadísticamente aquí y en cualquier parte del mundo se ha detectado que en un alto porcentaje las infracciones se deben a la mala conducta de los funcionarios de las entidades defraudadas, en el caso de instituciones financieras.

6. *CARENCIA EN INVERSIÓN DE SEGURIDAD DE TIPO INFORMÁTICO, DIGITALES O DE CARÁCTER BIOMÉTRICO y ENCRIPTACIÓN,* y a ello se suma el bajo nivel de investigación tecnológica o la falta de un minucioso esfuerzo por encontrar buenos productos y proveedores, ya que para muchas empresas es más importante dar una imagen atractiva de un producto o de un servicio, antes de adoptar las correspondientes medidas de seguridad.

7. *NO EXISTE LA POSIBILIDAD DE COTEJAR DATOS MEDIANTE EL INTERCAMBIO DE DATOS A TRAVÉS DE REDES CON LOS REGISTROS O BASES DE DATOS PÚBLICOS O PRIVADAS NACIONALES O INTERNACIONALES.*

8. A LOS VACÍOS DE LA LEGISLACIÓN SE SUMA LA FALTA DE CONOCIMIENTO DE LAS AUTORIDADES.

Muchas veces y como ya lo hemos referido en el análisis de esta investigación acerca de las características de los delitos informáticos el desconocimiento de que una acción conforma un delito lleva a personas de conducta honorable a cometerlos, ahora bien si el delincuente no tiene conciencia de que cometió un delito como el sujeto pasivo de una conducta criminógena atípica se va ha enterar de que fue víctima de la misma y peor aún en el supuesto de que el sujeto pasivo estuviera conciente de dicha conducta delictiva, como denunciaría la misma, si los ministerios públicos encargados de integrar las averiguaciones previas no tienen los conocimientos técnicos necesarios para encuadrar estas conductas.

Podemos encontrar dentro de este análisis dificultades técnicas para poder detectar a un delincuente de fraude informático, imaginemos a un delincuente invisible el cual no deja ningún tipo de huellas y el cual va a obtener beneficios de sus acciones en formas en que el sujeto pasivo difícilmente se va ha enterar y si este no llegase no tiene forma de conocer la identidad del delincuente, y más aún si en nuestro país no se cuenta con una ciberpolicía encargada de rastrear y perseguir delincuentes informáticos, de esta manera no se tienen ninguna base para proceder a la denuncia que seguridad se tendría de que se castigara al comisor de un delito de este tipo, esta sería una de las razones por las que hay todavía un tremendo atraso en la sanción en la comisión del fraude informático.

"La Ciudad de México- México cuenta ya con una policía especial para detectar delincuentes cibernéticos en un tiempo no mayor de 15 minutos, público un periódico nacional que citó a fuentes de la Secretaría de Gobernación, ...los recursos son escasos, el personal todavía lo están seleccionado y el equipo técnico no ha quedado totalmente instalado esta cibérpolicía dependerá de la PFP (Policía Federal Preventiva), esta policía nació ante la ausencia de mecanismos para detectar a los "*HACKERS*", que tienen la capacidad de invadir los sistemas informáticos del

gobierno, empresas y particulares, entre los delitos que combatirá esta organismo será, el evitar el robo de números de tarjetas de crédito, la sustracción de información especial, la creación de empresas fantasma, y falsificación de documentos entre otros."[126]

Desde hace dos años, aproximadamente, este proyecto ya está materializado, desde luego, este proyecto solo abarca el aspecto de denuncias contra menores, todavía no ha desarrollado su sistema dentro de los delitos informáticos, este se encuentra dentro de la Secretaria de Seguridad Pública, por la Policía Federal Preventiva, a cargo de la coordinación de inteligencia para la prevención.

"Ejerciendo sus atribuciones legales, la Policía Federal Preventiva ha desarrollado en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en policías de países desarrollados. Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo. Internet ha sido utilizado por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; así mismo, se han detectado bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento. Mención aparte, lo constituye el incremento de casos de niños desaparecidos en México, que son robados por extraños o sustraídos por padres en proceso de separación, lo que provoca un severo daño psicológico al menor. En el peor de los casos, la victimización del menor apartado del seno familiar alcanza niveles de alarma cuando se observan patrones de alimentación a redes internacionales de prostitución y/o de abuso sexual. Se mantiene patrullaje en la red mediante software convencional para rastreo de *Hackers* y sitios de Internet, comunidades y *chat rooms* en los que promueven la pornografía y el turismo sexual infantil. Asimismo, se utiliza Internet

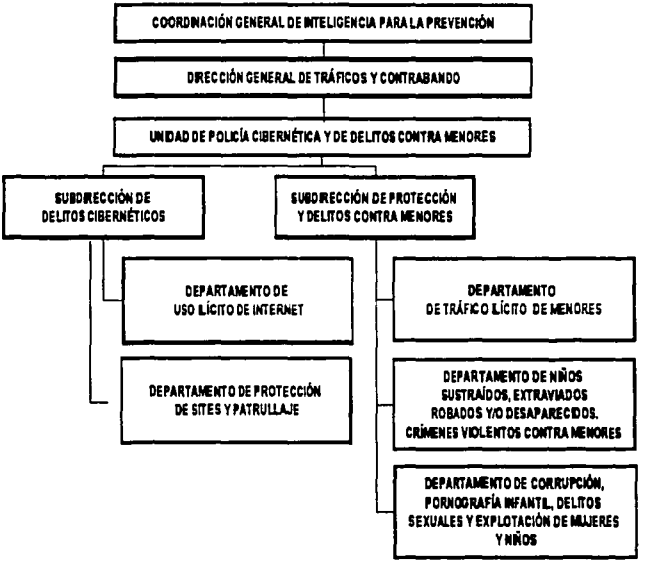
[126] "***Tarjetas Súper fraudes***", EL SOL DE MÉXICO, mediodía, México, Lunes 21 de Abril de 1997.Primera Plana.

como un instrumento para detectar a delincuentes que organizan sus actividades en la red. Se realiza análisis sobre actividades de organizaciones locales e internacionales de pedofilia así como de redes de prostitución infantil y redes de tráfico de menores que los explotan o prostituyen en otros países. Se desarrolla una Base de Datos Nacional para la identificación de patrones, rangos, preferencias y *modus operandi* de los casos reportados de menores extraviados, desaparecidos, abusados sexualmente, explotados, traficados y prostituídos, además de la integración de un Banco Nacional de Datos sobre pedofilia y agresores sexuales. Se cuenta con proyectos bilaterales con el Sistema Nacional para el Desarrollo Integral de la Familia, DIF, además, se tienen convenios con ONG's nacionales que reportan casos de niños robados como son la Asociación Pro Recuperación de Niños Extraviados y Orientación a la Juventud de México A.C., (APRENEM); la Asociación Mexicana de Niños Robados y Desaparecidos A.C.; la Fundación Nacional de Investigación de Niños Robados y Desaparecidos I.A.P. Se tienen proyectos bilaterales con "*International Center for Missing & Exploited Children*", "*National Center for Missing & Exploited Children*", "*U.S. Customs Cybersmuggling Center*", "Oficina de Asuntos de Menores" del Departamento de Estado de Estados Unidos e Interpol. Se tienen contactos con otras instituciones y *ONG's* que nos están ayudando a combatir los delitos que se cometen contra menores: *Tecnológico de Monterrey, Casa Alianza, Unicef, Adivac, A.C.* México Ciudad Humana, A.C., Espacios de Desarrollo Integral, A.C. (*ediac*), La Neta, Juegos sin Terminar. "[127]

La policía cibernética se constituye de la siguiente manera, atendiendo en exclusiva los casos en que se involucra a menores de edad y alimenta el banco nacional de datos sobre delincuentes en México:

---

[127] SECRETARIA DE SEGURIDAD PUBLICA, SSP. POLICÍA FEDERAL PREVENTIVA. Coordinación de Inteligencia para la Prevención. http://www.ssp.gob.mx/cibernética/INDEX/htm. Fecha de consulta viernes 11 de octubre del 2002.



El logotipo de La Unidad de Policía Cibernética es el siguiente:

La función que tiene esta coordinación es la de identificar y desarticular las organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio. Con esto nos damos cuenta que este tipo de ciberpolícia solo se encarga de todo lo relacionado con los menores, dejando una vez más aun lado muchos de los delitos que son calificados en otras legislaciones como delictivos, como sería en nuestro caso el fraude informático.

Respecto a la iniciación de procesos, es importante señalar que el único organismo que se ha dedicado a denunciar y a perseguir delitos que se pueden considerar incluidos dentro de los denominados informáticos es el Instituto Nacional de Protección a los Derechos de Autor, el cual fundamentándose en la ley Federal del Derecho de Autor se ha encargado de perseguir y sancionar a todo tipo de usuarios de programas reproducidos ilegalmente sin importar la magnitud de la empresa u organización policíacos que han instrumentado operativos tendientes a el decomiso de este tipo de material, esto nos hace ver que lo que protegemos en este país es el interés por los derechos de autor, pero no nos preocupábamos anteriormente por el patrimonio de los individuos que de una u otra forma realizamos transacciones, compramos o vendemos vía Internet, el patrimonio solo se restringía al de los derechos de autor en su beneficio o en su perjuicio pero nunca se dejaba de ver como una prioridad, ahora en la actualidad debido a los avances computacionales, se abarca más este ámbito tanto con los delitos informáticos y en específico el fraude informático.

Evidentemente el artículo que resulta más atractivo robar es el dinero o algo de valor, por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan pagos, como los de nominas, ventas, o compras, en ellos es donde es más fácil convertir transacciones fraudulentas en dinero y poder transferirlo a cuentas con el mismo medio con el que se obtuvieron (la computadora, vía Internet).

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

- "tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.

- Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos,

- A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un periodo de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando solo los efectos,

- Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden o no les afecta, el significado de los datos que manipulan,

- En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir, los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos, esto puede llegar a ser otra fuente de "agujeros".

- Solo parte del personal de proceso de datos conoce todas las implicaciones del sistema y el centro de cálculo puede llegar a ser un centro de información, al mismo tiempo, el centro de calculo procesara muchos aspectos similares de las transacciones

- En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión,

- El error y el fraude son difíciles de equiparar, a menudo los errores no son iguales al fraude, cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión, se tiende a empezar buscando errores de programación y del sistema, si falla esta operación se buscan fallos técnicos y operativos, solo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude."[128]

De lo anterior se desprende que las diversas razones por las cuales se puede cometer un fraude generalmente es porque son inducidas y muy pocas de las veces es porque se cometa un error, las empresas como vimos, son las principales fuentes de donde emanan los fraudes informáticos, debido a que la continua utilización de programas y sistemas computacionales proveen de los medios idóneos a los individuos que conocen de este tipo de mecanismos, o también aquellos individuos que hacen uso de los archivos de información como el de legislaciones que por no tener derechos de autor no cometen un ilícito, pero si consideramos que para hacer la compilación de toda la legislación de la República Mexicana, se contrata personal que estamos pagando de nuestros impuestos y además de esto pasan mucho de su tiempo recopilando información, revisando legislación, publicándola, no es conveniente que sujetos se alleguen de esta información una vez que esta ya ha sido cotejada, revisada y formalmente presentada, este es un problema muy importante ya que la misma fuga de información comienza desde dentro de la misma institución, ya que cualquier sujeto con conocimientos de computación puede acceder, y hacer uso indebido de la información lucrando con ella, pero también no hay que hacer a un lado a las personas que podríamos enunciar como cualquier individuo que solo desea realizar pagos, compras o ventas utilizando la Internet como el medio primordial, desde la comodidad de su casa, es allí donde se encuentra el sujeto que comete el delito de fraude informático ya que abusando del desconocimiento o de la

[128] Fraude. http: //www.monografias.com/especiales/mecanografia fecha de consulta 22 de Agosto del 2002.

buena fe del individuo ó sea sujeto pasivo, lo induce al error al manifestar mediante una página de Internet que obtendrá tal o cual bien o servicio, y para poder detectar si una página es realmente confiable necesitaríamos ser verdaderamente conocedores, y aún así caeríamos en el engaño al que fuimos inducidos, por lo cual esto en ciertas ocasiones es imposible de detectar porque los *crackers* tienen tal nivel de conocimientos, que no solo crean una página, común y corriente en la red sino que la hacen tan visualmente confiable que sin más los individuos somos presas fáciles para estos sujetos.

Aunque nosotros como consumidores tendemos a agrupar nuestros intereses juntos por debajo del término de la seguridad general, hay realmente varias partes de la seguridad que se confunden, la seguridad significa guardar "algo" que puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactivo, "seguro" los medios son protegidos desde el acceso, el uso o alteración no autorizada, hoy en día muchos de los usuarios no confiamos en la seguridad de la Internet, pues de alguna u otra forma tememos que alguien consiga el número de las tarjetas de crédito mediante el uso de la red, por otro lado otros temen que localicen su código de acceso de la cuenta del banco y entonces transfieran fondos a la cuenta del hurtador, pero esto no solo es lo único que nos puede preocupar sino también los conocidos robos hormiga, esto es más común de darse y proliferar, debido a que son pequeñas cantidades que son obtenidas mediante el engaño a los consumidores que efectúan operaciones mediante la red, y como son pequeñas cantidades las que se sustraen, el consumidor no presta tanta atención para denunciarlo o buscar una solución al respecto, por otro lado también tenemos a los individuos que venden bienes o servicios en la red, muchas de estas páginas como no requieren un requisito específico para ser realizadas, pueden ser de diversos productos en los cuales se hacen promesas falsas de entregas, posteriores a efectuar el pago, o simplemente requiere él número de tarjeta de crédito y su *NIP* para que sea saldado el pago, y en menos de 30 días uno recibirá el producto según la localización del domicilio, y al plazo señalado, se cumplió con el precio o

costo estipulado, pero la mercancía nunca fue recibida, y si uno accesa a la página nuevamente ya no existe, o ha caducado, sin que podamos hacer algo al respecto para exigir nuestro derecho.

Para poder guardar objetos seguros, refiriéndome a contraseñas o claves, dónde yo sepa como usuario que realmente son lugares en la red que existen y que no van a caducar o van a defraudarme y pueden ser confiables necesitamos que exista:

A. *La autenticación* (promesa de identidad) es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.

B. *La autorización*, (se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sancioné si las realiza), en este caso cuando se trate de empresas que tengan este tipo de funciones y sean blanco fácil para la realización de este tipo de fraudes informáticos utilizando su nombre.

C. *La privacidad o confidencialidad*, es el más obvio de los aspectos y se refiere a que la información solo puede ser conocidas por individuos autorizados, existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos, la transmisión de un medio presenta múltiples oportunidades para ser interceptada y copiada; las líneas "pinchadas" la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

D. *La integridad de datos*, la integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., ya sea durante el proceso de transmisión o en su propio equipo de origen, es un

riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

E. *La disponibilidad de la información*, se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

F. *No rechazo* (la protección contra alguien que niega que ellos originaron la comunicación o datos)

G. *Controles de acceso*, esto es quien tiene autorización y quien no para acceder a una zona de información determinada.

Estos intereses no solo son exclusivos de la Internet sino también del mundo físico, la autenticación y el asegurar los objetos es una parte de nuestra vida diaria, la compresión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar como estos requerimientos se encuentran en el mundo de la red y donde se sitúan las dificultades, existen numerosas técnicas para proteger la integridad de los sistemas, lo primero que se debe de hacer es diseñar una política de seguridad, en ella se debe de definir quienes son los que tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente, evitando los *passwords* (por defecto o demasiado obvios).

Muchos de los métodos utilizados se basan en abrir una cuenta bancaria a nombre de uno de los miembros del grupo y solicitar uno o dos terminales que es utilizado en el punto de venta virtual conocido como *TPV*, "el *TPV* es el método más usado para realizar transacciones económicas a través de la Internet., para ello se

utiliza la tarjeta de crédito, cargando cantidades determinadas a una cuenta bancaria asociada".[129]

Para realizar la compra en Internet sólo hace falta saber el número de tarjeta y la fecha de caducidad, debido a que no se realiza una compra físicamente y que la única comprobación que se realiza es a través de *TPV*, el cual contacta con la entidad bancaria que lo tiene dada de alta para verificar únicamente que el número de tarjeta que se introduce para realizar la compra está en vigor y tenga importe suficiente para realizar la misma. Durante un cierto período de tiempo, el comercio virtual realizaba múltiples ingresos utilizando número de tarjetas de crédito una vez que se encontraba el efectivo en la cuenta realizaban transferencias de dichas cuentas a otras en las que hay otros titulares, todos ellos miembros de la organización. Y al banco de cierto tiempo los cargos se realizaban en las cuentas de los titulares, y estos al comprobar que le habían cargado cantidades que en ningún momento habían aceptado, ya nada podían hacer pues no se podían detectar a estos individuos.

En algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906, otro método es aquel en el que se hace que la víctima haga una llamada a un teléfono de cobro para reclamar un servicio, cobro inexistente, premios fantasmas, etc, mediante datos bancarios, cobro de la tarjeta de crédito.

LAS SUBASTAS: algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos, y una vez que el consumidor ha enviado el dinero, puede ocurrir que reciban algo con menor valor o peor aún todavía, que no reciban nada.

---

[129] Noticias Sobre Delitos informáticos. http//delitosinformáticos.com/noticias/102426093181806.shtml. fecha de consulta 5 de julio del 2002.

ACCESO A SERVICIOS DE INTERNET.- el consumidor recibe una oferta de servicios gratuitos, la aceptación lleva implícita el compromiso de contrato a largo plazo con altas penalizaciones en caso de cancelación.

LAS TARJETAS DE CRÉDITO.- en algunos sitios de la Internet, especialmente para adultos se pide el número de tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años, el verdadero objetivo en cobrar cargos no solicitados.

OPORTUNIDADES DE NEGOCIO.- convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera, en la Internet abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en un fraude.

INVERSIONES.- Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y ocasionan grandes riesgos para los usuarios, como norma general no es recomendable fiarse de las páginas que garantizan inversiones sin seguridad del 100%.

PRODUCTOS Y SERVICIOS MILAGRO.- Algunas páginas de la Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias, y hay quienes de forma crédula ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

En las compras por la Internet utilizando tarjeta de crédito existe un plazo de reclamación, en el cual te devuelven el dinero sino estás satisfecho, este tipo de compras son consideradas como ventas a distancia, por lo que el régimen jurídico aplicable es el mismo que el aplicado a las realizadas en el medio tradicional. pero no solo es el cliente el que desea que el servicio se preste de una manera legal, sino que el propio comerciante en ocasiones se ve desprotegido ante hechos fraudulentos.

El problema principal que tiene el comercio electrónico es la desconfianza del consumidor. Por tanto habrá que descubrir cuál es la causa de esta desconfianza y contrarrestarla. Como ya se habrá intuido, la base de esta desconfianza es el desconocimiento; ¿quién hay detrás de esto?, ¿qué hacen con mi número de tarjeta...? Ante esto sólo se puede actuar de una forma; *CON INFORMACIÓN.*

Habrá que informar al consumidor de cuáles son los principales aspectos (positivos y negativos) de la compra por Internet. Para las tiendas es básico informar, dar confianza, seguridad. Porque si al hecho demostrado de la desconfianza, añadimos el hecho de que quien vende es una pantalla de ordenador, el rechazo se puede convertir todavía en mayor de lo que era antes.¿Cómo se consigue esto? Por un lado, informando de qué es una zona segura y cómo se produce la certificación por una agencia externa de esa seguridad. Y por otro, con un fuerte servicio de atención al cliente. Si el consumidor sabe que una agencia externa ha auditado esa tienda -su seguridad- y, por tanto, da fe de que la tienda es segura y de que esa tienda existe, también sabrá que el servicio de atención al cliente es totalmente fiable. A la tienda le tocará luego seguir una política de marketing que tenga como principal estrategia el servicio de atención al cliente, ya que el cliente es su mayor activo, y su principal objetivo debe ser fidelizar a éste, para que tenga la seguridad de que realmente este contratando con una empresa honesta y confiable y que en cualquier momento el comprador, pueda: *REALIZAR RECLAMACIONES* ante la misma empresa en el domicilio donde físicamente este ubicada, *y EXIGIR CALIDAD DE SERVICIOS Y PRODUCTOS.* En caso de que los productos que le hayan sido enviados no satisfagan sus exigencias o simplemente no sean de la calidad que esperaba.

En la actualidad existe un organismo Internacional dedicado a denunciar los abusos en la Internet este organismo recibe el nombre de *ECONSUMER.GOV*, el cual surge "el 24 de abril de 2001, en respuesta a los retos que supone el fraude internacional por Internet, y como parte del trabajo que se lleva a cabo con objeto de

fortalecer la protección al consumidor y la confianza del consumidor en el comercio electrónico, 13 países presentaron econsumer.gov, un esfuerzo conjunto para reunir y compartir quejas sobre comercio electrónico transfronterizo.

El proyecto tiene dos componentes: un sitio Web público en diversos idiomas y un sitio Web gubernamental de acceso restringido y protegido con clave. El sitio público provee información general en torno a la protección al consumidor en todos los países que pertenecen a la *IMSN* (*Red Internacional de Supervisión de Prácticas de Mercadeo*), información para establecer contacto con las autoridades de protección al consumidor de dichos países y un formato de queja electrónico. Toda la información está disponible en inglés, francés, alemán y español. *Utilizando la red Consumer Sentinel* (una base que contiene datos con las quejas de los consumidores y otra información de investigación y que es manejada por la Comisión Federal de Comercio de los Estados Unidos (*FTC*, por sus siglas en inglés), las quejas que se reciban serán compartidas a través del sitio Web gubernamental con las autoridades participantes responsables de aplicar la ley en materia de protección al consumidor". [130]

Además es importante que cuando se vaya a realizar una compra o venta vía Internet se verifique lo siguiente:

ACERCA DE LA COMPAÑIA.

- ¿Qué tipo de empresa es y qué vende?
- ¿Dónde está ubicada, incluyendo el país?
- ¿Cómo se puede contactar a la empresa?

ACERCA DEL PRODUCTO O SERVICIO:

- ¿Qué es lo que vende?, incluyendo detalles suficientes para que sepamos exactamente y no tengamos duda del producto.
- ¿Qué estamos comprando?, el costo del producto o servicio y la moneda utilizada.

[130] Econsumer.Gov.http://econsumer .gov/spanish/index.html. fecha de consulta 20 de marzo del 2002.

ACERCA DE LA VENTA:

- Los costos adicionales al precio del producto o servicio, tales como los costos de envío y manejo. Impuestos y aranceles.
- Cualquier restricción o limitación en la venta,
- Cualquier garantía o fianza,
- La disponibilidad de opciones de pago seguras y convenientes,
- Una estimación de cuándo recibirá el producto.

ACERCA DE SU PROTECCIÓN A LOS CONSUMIDORES:

- La posibilidad de que el cliente conserve una copia de la factura,
- La seguridad de que la información personal estará protegida en el caso de pago en línea,
- Políticas sobre el tipo de información personal que sé esta almacenando sobre, que es lo que hace la compañía con ella y con quién la comparte.
- La posibilidad para el cliente de elegir que no se almacene su información personal.
- Políticas sobre el envío de correos electrónicos (e-mail) no solicitado, incluyendo la posibilidad de rechazar esta propuesta.
- La política de devolución, incluyendo una explicación de cómo puede devolver un artículo o hacer un cambio. Donde debe de llamar, escribir o acudir para reclamar o enviar quejas o problemas derivados de el producto adquirido.

Por otro lado encontramos los fraudes informáticos cometidos mediante manipulación de datos, con esto me refiero a que no hay exclusividad en este tipo de delitos, como anteriormente ya he hecho referencia con los delitos cometidos contra los usuarios de la Internet en la compra y venta de bienes y servicios, sino que también contempla otro tipo de acto delictivo, como es la sustracción de información de diversos tipos que podemos considerar como clasificada o confidencial.

Klaus Tiedman clasifica la criminalidad mediante computadores para obtener información o base de datos en cuatro grupos los cuales son:

" **Manipulaciones**.- estas pueden afectar tanto la fase de suministro o alimentación (imput) de datos, como a la fase de salida (output) y la de su procesamiento (bajo la forma de manipulaciones en el programa o en la consola), resultan poco importantes las manipulaciones en el *hardware*, al cual pertenecen los elementos mecánicos del equipo de procesamiento de datos.

Espionaje.- En el ámbito del procesamiento de datos el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin ningún problema a otro soporte.

Sabotaje.- La destrucción total de programas y datos, puede poner en jaque la continuidad de toda una empresa. Estos resultan favorecidos debido a la concentración de información en un mínimo espacio.

Hurto de tiempo.- Se trata de la utilización indebida de instalaciones de cómputo por parte de empleados desleales o de extraños, lo que puede ocasionar pérdidas considerables, lo reprochable no consiste tanto en el escaso consumo de energía eléctrica, ni en el mínimo desgaste del equipo de cómputo, sino en el notable enriquecimiento del autor proveniente del uso indebido del computador."[131]

En lo referente a las manipulaciones de ordenador consisten en modificaciones de datos practicadas especialmente por empleados de las empresas perjudicadas, con el fin de obtener un enriquecimiento personal, los métodos en los que se puede llevar a cabo estas manipulaciones son mediante la introducción de datos falsos en el ordenador (manipulaciones de imput) puede alterar el orden del proceso (manipulaciones de programa y la consola), o bien puede posteriormente falsear el resultado, inicialmente correcto, obtenido del ordenador (manipulaciones del output).

---

[131] Markovicth Magliona, Claudio Paul, López Medel, Macarena. ***DELINCUENCIA Y FRAUDE INFORMÁTICO***, Editorial Jurídica Chile, 1999. pp. 52.

En el espionaje informático constituye en el ámbito de la criminalidad por ordenador la segunda forma más frecuente del delito, además de ser muy lucrativa y para la empresa o institución es muy peligroso, y el objeto de el espionaje informático lo constituirán en primer lugar los respectivos programas, a este tipo de delitos también se le denomina hurto de software, y el método más frecuente es la obtención de copias de archivos de datos.

Las posibilidades de manipulación del ordenador son aprovechadas, no solo por personas externas a una institución o a una empresa, o solo por empleados que perjudican a la propia empresa, sino también por la gerencia de empresas, y coordinaciones en instituciones gubernamentales que trabajan fraudulentamente para obtener de cierto tipo de información un beneficio, y en el caso de empresas poder perjudicar a la competencia y hasta organismos estatales.

CAPITULO V

V.- PROPUESTA PARA TIPIFICAR EL FRAUDE INFORMÁTICO EN EL DISTRITO FEDERAL.

5.1. - FRAUDE INFORMÁTICO EN NUESTRO CÓDIGO PENAL VIGENTE

En la actualidad han surgido muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a individuos como a empresas, la proliferación de la computadora como la principal herramienta, así como la creación de la red global Internet ha provocado que cada vez mas personas se las ingenien para lucrar, hacer daño o causar perjuicios a través del uso de estos medios.

El acceso no autorizado a un sistema Informático, consiste en acceder de manera indebida, sin autorización, a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual y/o económica por el desciframiento de los códigos de acceso o *password*, como fin u objetivo, se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas. Teniendo en cuenta también la gravedad que implica el fraude informático, es necesario que el Código Penal para el Distrito Federal incluya esta figura delictiva, ya que de no hacerlo, la ausencia de esta figura en concreto, daría lugar a que los autores de esos hechos queden impunes ante la ley, o bien, obligaría a las autoridades jurisdiccionales a aplicar preceptos que no se ajusten a los hechos cometidos.

Un claro ejemplo del uso de las telecomunicaciones, se puede representar en la página de la Suprema Corte de Justicia de la Nación, quién posee su propia página de internet, red jurídica nacional y red interna[132]. En la página de internet, se presenta la información a la que tiene acceso cualquier persona, en cualquier parte del mundo. En la Intranet Nacional, es aquella dónde sólo tienen acceso los funcionarios del Poder Judicial de la Federación, a efecto de proporcionar información que es sólo para consulta de la administración de justicia. Y finalmente la Intranet de la Suprema Corte de Justicia de la Nación, es aquella, donde se presenta

[132] Ver anexo I

la información que es de interés para las actividades de los señores Ministros y del personal que se ubica sólo en las oficinas de Pino Suárez y 16 de septiembre.

Para poder entender la naturaleza de mis propuestas, es necesario que analicemos el fraude informático desde dos puntos de vista, tomando como referencia nuestra legislación Penal del Distrito Federal, primero como se encuentra regulado el delito de fraude y posteriormente como lo acoplaría al ámbito Informático, ya que nuestra legislación lo regula efímeramente y de manera muy general este ámbito en especifico, y se asemeja con los delitos en materia de vías de comunicación y correspondencia como a continuación se muestra:

A continuación se trascribirán los artículos legales respectivos para alcanzar los fines de esta investigación para un mejor desarrollo metodológico.

" TITULO QUINTO
DELITOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y DE CORRESPONDENCIA.

Articulo 167. - Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:

V.- Al que dolosamente o con línea de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales por medio de las cuales se transfiera señales de audio, de video o de datos..." [133]

En este párrafo solo se nos menciona al que interrumpa o interfiera, las comunicaciones (sobre este punto me referiré más adelante, ya que es el punto medular de el artículo legal en referencia), pero en ninguna parte nos hace hincapié de forma directa a la Internet sobre algún medio o sistema informático, sin embargo nos menciona los medios como, comunicación alámbrica, inalámbrica e incluso de fibra óptica, y las diversas especies como lo es vía satélite, telegráficas, telefónicas, podría en algún aspecto al referirse en el aspecto telefónico, lo que nos haría pensar que tal vez se refiere a la Internet, pero no podríamos suponer, ya que debe estar

[133] AGENDA PENAL FEDERAL, 2002. Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia. Editorial ISEF. Págs 40, 41, 42

bien descrito, dicho tipo, ya que este tipo al querer abarcar un gran ámbito de aplicabilidad quiere generalizar, y suponiendo sin conceder, debemos hacer referencia que muchos de los datos no únicamente son transferidos de una computadora a otra por así decirlo, sino que también hay que contemplar a los individuos que crean dichos archivos y lucran con ellos, sin transferirlos a otra computadora, o simplemente no transfieren datos, ni de audio, ni de video, sino simplemente crean empresas falsas que hacen que individuos incautos caigan en un engaño, y en este caso como podríamos sancionarlos si de ningún modo el Código Penal para el Distrito Federal ni mucho menos el Nuevo Código Penal para el Distrito Federal lo describe y lo que llega a describir es de una forma tan general, que cualquier persona entonces que transfiera datos, es un delincuente informático, es bien claro que nos menciona que con una línea de lucro, entonces cualquiera que cree su propio trabajo en una base de datos y quiera venderlo es según este tipo penal un delincuente, debido a que no especifica en este sentido directa y formalmente el aspecto que estudio en la presente Investigación, debido a que no podemos interpretar en ningún sentido este tipo para querer aplicarlo, adecuarlo a algún tipo penal actual, es por ello que es una necesidad el crear un tipo penal en el que se contemple de manera concreta y clara al fraude informático, y como al principio nos señala la parte medular de este tipo penal, al que interrumpa o interfiera, esto analizándolo en el origen de los términos, de una manera más concreta al respecto tenemos que:

"Interrumpa.- impedir la continuación o prosecución de algo, suspender, cesar momentáneamente o durante cierto lapso, para reanudar ulteriormente una actividad, ..."[134]

Y también a su vez la palabra Interfiera comprende: "apoderarse de una cosa o de una noticia antes de que llegue a su destino o al destinatario."[135]

---

[134] Op, Cit, CABANELLAS, Guillermo, Tomo II, pp. 424.
[135] Idem. Pp. 407.

Con esto vemos claramente que en ninguno de sus puntos podría encuadrar el fraude informático, debido a que además de que en el fraude informático no se interrumpe ningún tipo de dato, o comunicación, y es más aún ni siquiera se nota que en ningún aspecto haga mención a el engaño, o aprovechándose de la poca experiencia, conocimiento, o que como producto del error se haga uso de estos datos, señales, por cualquiera de los medios ya descritos anteriormente. Y si utilizáramos en este aspecto la analogía e interpretación, los cuales quedan estrictamente prohibidos en materia penal, por otro lado, el término interferir, podríamos utilizarlo en cuestión como la obtención de las contraseñas de las tarjetas de crédito, pero si cualquier individuo entra en la red, como cualquier usuario, podría tener acceso a las mismas de una manera indiscriminada en ciertos portales o páginas de compras, y más que nada el párrafo legal en comento del artículo antes citado, por cuestiones cronológicas se referiría entonces a las señales telegráficas, al espionaje, en donde se interferían líneas telefónicas para conocer las conversaciones, o para obtener cierta información privilegiada.

> **"Artículo 168 Bis.- Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:**
>
> *I.- Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas; o*
>
> *II.- Transmita la propiedad uno o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas...."*[136]

De lo anterior podemos deducir que no reconoce ni siquiera el ámbito Informático, debido a que la legislación penal quiere ser tan general, que da ha entender que cualquiera que accese a una vía de comunicación sea del tipo o de la forma que fuere es delincuente, y con respecto a la sanción que se le impone, no compensa, ni repara ningún daño que haya sido ocasionado, la manera más fácil que veo, que se le impone en este tipo penal es el sancionar con la pena de prisión como

[136] AGENDA PENAL FEDERAL, 2002. Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia. Editorial ISEF. Págs 40, 41, 42.

única solución, en lo cual no concuerdo, debido a que debe de haber forzosamente una rehabilitación, pero si tenemos que el fraude informático no es un tipo delictivo común, no se le debe de aplicar una sanción común, como cualquier otro delito.

Con respecto al análisis anterior como se sabe en materia penal el tipo debe encuadrar perfectamente no puede interpretarse como nos señala nuestra Constitución en su articulo 14 párrafo tercero "... En los juicios de orden criminal queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata."[137]

Según el manual de las Naciones Unidas para la prevención y control de delitos informáticos, señala que cuando el problema se eleva a la escena internacional se magnifican los inconvenientes y las insuficiencias, por ello los delitos informáticos y en particular el fraude informático constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada, pero para que esto pueda funcionar debe primero, tenerse una regulación a nivel local y posteriormente a nivel federal sobre el problema a combatir ya que si no se tienen los medios para ello, resultaría ineficaz cualquier esfuerzo para combatirlo, aunque se tuviera mucha voluntad para tratar de erradicarlo.

Para ello se requiere un apoyo que nos especifique acerca de que tipo de conductas deben constituir delitos informáticos, tomando en cuenta al fraude informático como uno de los primordiales.

Que se elabore un acuerdo entre estados y a nivel global acerca de las definiciones legales de dichas conductas delictivas, debido a que tanto a nivel local como federal y mundial encontramos que existe una falta de consenso sobre la definición jurídica clara y precisa, así como la falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, por lo cual se debe de adiestrar funcionarios

---

[137] Idem, Pág. 3.

judiciales en el campo de los delitos informáticos en específico en la detección de los fraudes informáticos, debido a que la clara ausencia de la especialización en este ámbito, por parte de las autoridades legislativas, crean una insuficiente, enorme y clara realidad legislativa, ya que gracias a esta ausencia dicha legislación encuentra en su práctica una muy deficiente solución.

Estamos de acuerdo en que la informática concierne a todos los sectores de la vida económica y social en una forma que ya hemos analizado y es muy destacada, pero esta expansión hace surgir problemas jurídicos nuevos de carácter general y muy técnicos, por ello los dominios del derecho se modifican así bajo la influencia de la informática en forma muy numerosa, y tomando en cuenta que es interdisciplinaria puesto que abarca diversos dominios del derecho siendo evidente la vocación de la informática para ser aplicada a los más diversos sectores.

Y podemos señalar que en el Nuevo Código Penal para el Distrito Federal, no contempla ningún apartado especial para este tipo de fraude informático, solo hace mención y no de forma directa en el apartado referente a la pornografía infantil al decir "artículo 187. - al que por cualquier medio..." y esto no nos aclara, ya que si aplicamos el principio de exacta aplicación de la ley en materia penal, vemos que los delitos informáticos y en particular el fraude informático, no nos aclara nada la frase manifestada anteriormente, por lo cual sino esta expresamente mencionado en la ley no es punible.

Ya previamente en los capítulos II, III y IV, de la investigación se estableció que el fraude informático reúne a una multiplicidad de conductas defraudatorias realizadas por medio de comportamientos astutos, engañosos, en este caso manipulaciones informáticas fraudulentas, lesivas de intereses económicos diversos, realizadas con animó de obtener una ventaja económica, y aprovechando las características de los sistemas informáticos y su funcionamiento, en consecuencia el fraude informático comprendería entonces todas aquellas conductas de manipulaciones defraudatorias en el funcionamiento de un sistema de tratamiento

automatizado de datos, con la intención maliciosa de lograr un provecho, produciendo un perjuicio económico.

Para enfrentar estos comportamientos primero analizamos la aptitud del delito de fraude tipificado en la legislación penal para el Distrito Federal, frente a las conductas constitutivas del fraude informático, concluyendo que el fraude presentaba dificultades insalvables para poder castigar estos comportamientos, luego nos enfrentamos con la inexistencia en nuestro ordenamiento jurídico de un apartado especial o más aun una ley relativa a los delitos informáticos, Pero no es la historia de nuestro Código Penal para el Distrito Federal y ahora con las reformas de nuestro Nuevo Código Penal para el distrito Federal, lo que justifica mi aseveración, sino que en dicho análisis del articulado de dicho Código pude llegar a esta proposición.

Por ello a continuación propongo que se cree un artículo dentro del capítulo III delitos en contra del patrimonio de las personas, FRAUDE, al que le denominare FRAUDE INFORMÁTICO de la siguiente manera:

CAPITULO III
FRAUDE INFORMÁTICO

ARTÍCULO 232. **- SE ENTIENDE POR FRAUDE INFORMÁTICO, AL SUJETO QUE POR MEDIO DE COMPORTAMIENTOS ASTUTOS, ENGAÑOSOS, O APROVECHÁNDOSE DEL ERROR DE OTRO, MEDIANTE MANIPULACIONES CONTRARIAS A EL ORIGEN DE LOS SISTEMAS INFORMÁTICOS, APROVECHE LAS CARACTERÍSTICAS DE LOS MISMOS Y SU FUNCIONAMIENTO COMO LO ES LA INTRANET E INTERNET, TENIENDO COMO FINALIDAD LA OBTENCIÓN DE UN LUCRO EN BENEFICIO PROPIO O DE UN TERCERO, CAUSANDO UN DAÑO O PERJUICIO EN EL PATRIMONIO O INFORMACIÓN DE CUALQUIER ÍNDOLE SIENDO ESTOS LÍCITOS, SE LE IMPONDRÁN:**

I. **DE VEINTICINCO A SETENTA Y CINCO DÍAS MULTA, Y TRABAJO EN FAVOR DE LA COMUNIDAD, CUANDO EL VALOR DE LO DEFRAUDADO NO EXCEDA DE CINCUENTA VECES EL SALARIO MÍNIMO, O NO SEA POSIBLE DETERMINAR SU VALOR.**

II. **DE SETENTA Y CINCO A DOSCIENTOS DÍAS MULTA Y REPARACIÓN DEL DAÑO, CUANDO EL VALOR DE LO**

DEFRAUDADO EXCEDA DE CINCUENTA PERO NO DE QUINIENTAS VECES EL SALARIO MÍNIMO.

III. DE DOSCIENTOS A QUINIENTOS DÍAS MULTA Y REPARACIÓN DEL DAÑO, CUANDO EL VALOR DE LO DEFRAUDADO EXCEDA DE QUINIENTAS PERO NO DE CINCO MIL VECES EL SALARIO MÍNIMO.

IV. DE QUINIENTOS A OCHOCIENTOS DÍAS MULTA Y REPARACIÓN DEL DAÑO, CUANDO EL VALOR DE LO DEFRAUDADO EXCEDA DE CINCO MIL VECES EL SALARIO MÍNIMO.

Art. 232 BIS.- SE IMPONDRÁ LA PENA CORRESPONDIENTE SEGÚN EL MONTO DE LO DEFRAUDADO EN ÉL ARTICULO ANTERIOR, AL SUJETO QUE COMETA FRAUDE INFORMÁTICO CUANDO ACTUÉ EN CALIDAD DE USUARIO, YA SEA PERSONA FÍSICA O MORAL, INTERMEDIARIO, PRESTADOR DE SERVICIOS, BANCO, EMPRESA PROVEEDORA, UTILIZANDO SUS HABILIDADES TÉCNICAS SOBRE INFORMÁTICA, Y UTILICE LA INTERNET PARA OBTENER CON ENGAÑOS GANANCIAS INDEBIDAS, DINERO, VALORES, BIENES O SERVICIOS, ADQUIRIENDO, ENAJENANDO, TRANSFIRIENDO, DEPOSITANDO O DANDO EN GARANTÍA PRODUCTOS, SERVICIOS DE CUALQUIER ÍNDOLE

La propuesta anterior como artículo 232 para el Código Penal para el Distrito Federal sobre FRAUDE INFORMÁTICO lo baso en el siguiente análisis como a continuación expongo:

A. SE ENTIENDE POR FRAUDE INFORMÁTICO, AL SUJETO QUE POR MEDIO DE COMPORTAMIENTOS ASTUTOS, ENGAÑOSOS, O APROVECHANDO EL ERROR DE OTRO,

En esta primera parte del concepto propuesto, me refiero a lo que entenderemos por fraude informático, y hago el señalamiento de que la conducta ilícita es lo primero que debe de ser castigado, en este caso del fraude informático, que cualquier sujeto sea una persona física o moral que se base en comportamientos, procedimientos, actos que sean engañosos, o astutos, debido a que en el análisis del sujeto activo de este delito mencionamos que no se trata de cualquier sujeto que tenga una computadora y este conectado a la red, sino que

requiere de conocimientos en informática, computación etc, para poder lograr su finalidad ilícita, y que conozca mucho más las técnicas cibernéticas, y haga caer o se aproveche del error de los individuos que hacen uso de la Internet, y a los cuales en ciertos aspectos podríamos considerar "incautos" que deciden hacer una transferencia, adquirir información, realizar alguna compra, etc. Sin tener los conocimientos, la información necesaria para no ser víctimas de fraudes informáticos.

B. MEDIANTE MANIPULACIÓN CONTRARIA A EL ORIGEN DE LOS SISTEMAS INFORMÁTICOS,

En esta segunda parte hago referencia que el fraude informático para que se considere como tal, debe de basarse en la utilización de sistemas informáticos, los cuales desde un inicio fueron creados solo y con la finalidad de servir al individuo, disminuyendo el trabajo, aminorar errores, hacer más veloz el tiempo de transferencia de la información, realizar transacciones en menor tiempo, facilitar información de manera gratuita, etc, para que el ser humano tuviera a su alcance información de cualquier parte del mundo, de cualquier tema, sin que saliera de una habitación para ello, pero la naturaleza del ser humano es buscar el modo de sobrevivir, y eso no esta mal, lo malo y lo ilícito es que se utilice este medio para sobrevivir de manera que ciertos individuos se basen en el engaño, en el trabajo arduo de otras personas, en el error de otras personas, para obtener un lucro, o un beneficio, simplemente con accesar a la red.

C. APROVECHE LAS CARACTERÍSTICAS DE LOS MISMOS Y SU FUNCIONAMIENTO COMO LO ES LA INTRANET E INTERNET,

En este párrafo me refiero a que no solo los individuos que accesan a Internet son los únicos que cometen fraudes informáticos, sino también los que se encuentran en una red privada como lo es la intranet, ya que muchos de los ilícitos que se cometen son por los mismos empleados de las instituciones, ya que tienen

que se cometen son por los mismos empleados de las instituciones, ya que tienen acceso a todo tipo de información dentro de la institución, empresa, etc, y ellos son los que propagan ciertos datos, información privilegiada, claves, etc, como es el caso de la legislación en la Suprema Corte de Justicia de la Nación, ya que en esta Institución se contrata a personal capacitado para que realice cotejos, correcciones de las legislaciones que reciben para que sean publicadas, y estamos de acuerdo que la legislación no tiene propiamente derechos de autor, pero uno como habitante de esta Ciudad paga sus impuestos y el personal que se contrata para dicha actividad es pagada de los mismos, y muchas de las veces esta información es filtrada, una vez estando lista para su publicación, para que a cambio de una remuneración económica la faciliten a librerías, la fotocopien y la vendan etc, cuando el esfuerzo que se invirtió en su revisión es extremo, y la misma institución proporciona le legislación ya sea de manera gratuita en forma impresa o a bajo costo para que en discos compactos se pueda distribuir.

D. TENIENDO COMO FINALIDAD LA OBTENCIÓN DE UN LUCRO EN BENEFICIO PROPIO O DE UN TERCERO, CAUSANDO UN DAÑO O PERJUICIO EN EL PATRIMONIO O INFORMACIÓN DE CUALQUIER ÍNDOLE SIENDO ESTOS LÍCITOS.

En este párrafo me refiero a el lucro indebido que se obtiene, al acceder a estos medios como son la intranet, e Internet, obteniendo información, bases de datos, realizando ventas engañosas, cometiendo robos hormiga, utilizando números de tarjetas de crédito, y hasta clonando las tarjetas de crédito, etc, todo ello encaminado a beneficiarse económicamente a costa de uno o varios sujetos en forma indebida, aclarando que dicha información deberá ser licita, refiriéndome a ello en que no vaya en contra de la moral, probidad y buenas costumbres.

Con respecto a la sanción además de la pena de prisión y la multa en la primera fracción propongo trabajo a favor de la comunidad, ya que a mi parecer el tipo de individuos que cometen esta clase de delitos no son pertenecientes al común

de los demás individuos, por lo que sus habilidades en computo y conocimientos deben de ser aprovechadas al máximo en beneficio de la sociedad.

Y en lo referente a las tres fracciones siguientes además de la multa propongo, la reparación del daño, la reparación se diferencia de otros vocablos que se han utilizado a veces como sinónimos; indemnización, resarcimiento, etc. Este uso indebido ha creado muchas confusiones al respecto. Si profundizamos al análisis veremos que la reparación del daño entraña una idea más amplia, más compleja que cualquier otro sinónimo u otro concepto semejante. En consideración a lo expuesto la reparación del daño persigue tres objetivos que son:

1. COMPONER EL DAÑO O PERJUICIO QUE ALGUIEN HA SUFRIDO EN LO MATERIAL O EN LO PATRIMONIAL, lo que se expresa con el empleo de los términos "material o patrimonialmente", es la exclusión de la persona, ya que cuando hay daño a la persona, en ningún caso es posible la "recomposición" o la vuelta a un status anterior con esto hago referencia a la vida humana, razón por l cual se habla de un desagravio o satisfacción. Por lo tanto es imprescindible, que el bien dañado sea de características tales que pueda, por su esencia y función componerse *in natura*, por lo cual es necesario determinar si, después de lesionado el bien, existe interés en el ofendido por ese tipo de reparación, ello hace posible que exista una composición de la misma cosa o una composición por sustitución, la primera para que sea posible que se de, habrá que admitir que el deterioro ocasionado por la conducta sea susceptible de recomposición, que el damnificado tenga interés en ello, y que la cosa una ve recompuesta conserve intactos sus elementos esenciales y sus facultades esenciales. Con respecto a la segunda la reparación por sustitución, guarda evidentemente relación con la misma esencia y función de las cosas para lo cual resulta de vital importancia subordinar estas situaciones a

tres principios; el de la autonomía de la voluntad, el de la buena fe, y el de la del ejercicio abusivo del derecho

2. DESAGRAVIAR O SATISFACER AL OFENDIDO, el patrimonio moral es un bien inescindible y autónomo que goza de genuina protección en nuestro derecho, las personas poseen algo más valioso que su patrimonio material; su rectitud, sus valores morales, su respeto por los otros y la consideración que estos les guardan, su fuerza espiritual, etc. Esto es un conjunto de realidades individuales y sociales que configuran su "patrimonio moral".

3. EVITAR UN DAÑO O PERJUICIO IRREPARABLE Y TOTAL, con esto me refiero que si el damnificado, ya ha sufrido la perdida de su patrimonio, que esta no se de una forma total, debido a que si se hace que el ofensor repare el daño, en las medidas que le sea impuesto de acuerdo a el monto que haya sido capaz de defraudar informáticamente, lo cual deberá establecerse en su momento procesal respectivo cuando se haya levantado la denuncia, basándose y del monto que haya defraudado por vía informática.

Con respecto a lo anterior propongo la reparación del daño debido a que el control de la criminalidad se ha visto directamente afectada por la acelerada transformación de los valores sociales, que implican una anhelada redistribución de bienes y oportunidades, esta es una idea fundamental que forma parte de la justicia en la actualidad, la idea de la reparación del daño, la expongo como una especie de tratamiento consistente en impulsar a que el indiciado trabaje de manera casi autónoma, y resuelva en cierta manera la causa del problema que lo llevo a delinquir, pagando los daños que ocasiono, y que logre con ello una verdadera readaptación social, esto lo propongo con el fin de que las personas afectadas, muchas de las veces solo pueden tener el consuelo de que sean encarcelados los individuos de la comisión del acto

delictivo, porque jamás llegan a ver nada de lo que perdieron económicamente, y me parece justo que el individuo que cometió dicho ilícito, remunere al sujeto pasivo o a el agredido en su patrimonio a pagar el monto de la cantidad defraudada por vía Informática.

De acuerdo a lo anterior sólo lo que es factible de preverse es, a la vez susceptible de penalización, de esta forma quedan excluidos los casos fortuitos y la fuerza mayor, por lo cual los casos previsibles pueden ser de dos clases; dolosos y culposos. Esto es lo que determina la fase subjetiva del tipo penal, debido que en los actos dolosos, además de ser previsible, el sujeto había realizado en su mente la configuración de un objetivo o finalidad, es decir, el sujeto quería el resultado, por otra parte en los actos culposos, el sujeto no previó el resultado y no lo deseaba, a pesar de que era previsible su realización, sobre el fraude informático estriba en determinar la clase de un dolo directo especial.

La segunda parte de mi propuesta que menciono como artículo ***232 BIS*** para el Código Penal para el Distrito Federal sobre FRAUDE INFORMÁTICO lo analizó como sigue:

A. *SE IMPONDRÁ LA PENA CORRESPONDIENTE SEGÚN EL MONTO DE LO DEFRAUDADO EN ÉL ARTICULO ANTERIOR, AL SUJETO QUE COMETA FRAUDE INFORMÁTICO CUANDO ACTUÉ EN CALIDAD DE USUARIO, YA SEA PERSONA FÍSICA O MORAL, INTERMEDIARIO, PRESTADOR DE SERVICIOS, BANCO, EMPRESA PROVEEDORA,*

Hago mención en este párrafo a todo usuario que siendo servidor público o teniendo la calidad que sea dentro de una institución y teniendo acceso a Internet o a intranet, o sin pertenecer a una empresa o Institución, incluso siendo persona física o moral haga uso indebido por medio de la red para obtener un lucro, ya sea de los

datos internos o externos que se contengan, se le impondrá la pena correspondiente según el monto de lo defraudado por esta vía.

B. UTILIZANDO SUS HABILIDADES TÉCNICAS SOBRE INFORMÁTICA, Y UTILICE LA INTERNET PARA OBTENER CON ENGAÑOS GANANCIAS INDEBIDAS, DINERO, VALORES, BIENES O SERVICIOS,

Hago referencia que no importando que los sujetos fueren servidores públicos, particulares, personas físicas o morales mencionados en el párrafo anterior, pertenezcan o no a una empresa o institución, utilicen sus conocimientos para que mediante engaños informáticos, obtengan un lucro indebido, que es el aspecto fundamental del tipo que se propone, y que puede constituirse ese lucro de diferentes formas como en dinero, valores, bienes o servicios.

C. ADQUIRIENDO, ENAJENANDO, TRANSFIRIENDO, DEPOSITANDO O DANDO EN GARANTÍA PRODUCTOS, SERVICIOS DE CUALQUIER ÍNDOLE

Y que todo ese lucro que se obtuvo mediante fraude informático, sea adquiriendo, enajenando, transfiriendo, depositando, o dando en garantía productos o servicios como pago, sea este de cualquier otra índole incurrirá en lo que es el fraude informático.

Un problema crucial con que se debe enfrentar la sociedad decidida a poner atajo a la delincuencia informática es el que se relaciona con la modernización y mejoramiento de los equipos técnicos de prevención y, por otro lado, la formulación de criterios de defensa comunes en este sentido. Sin embargo el fondo del problema consiste en que para lograr una relativa protección frente a la amenaza de la mala utilización de la informática, debe nuestra sociedad, conjugar ciertos elementos de notable trascendencia, en primer término debe existir una tipificación como la que

anteriormente se presenta, que comprenda lo que el fraude informático supone e implica, en el marco de una regulación global de la actividad informática.

Sin embargo no basta solo con tener un cuerpo legal privilegiado si no se entiende la necesidad de determinar un procedimiento penal especial relativo a esta forma novedosa de delincuencia, debido a que el juez no es un técnico en informática, y por lo tanto se requiere flexibilizar el clásico procedimiento penal con miras a entregar al magistrado las herramientas jurídicas tendientes a la substanciación adecuada de un proceso de esta naturaleza.

En lo relativo a las pruebas, el juez determinara la forma en como ha de dejarse constancia en el proceso de estas pruebas y cuando se hicieren necesarias operaciones técnicas especiales para ello o para su realización, para tal efecto podrá designar a un asesor técnico que desarrolle y explique la prueba, de entre los que ejercieren los oficios especializados, en dado caso que la prueba fuere ofrecida por una de las partes y el juez lo estimare conveniente, éste suministrara el personal e instrumentos necesarios para llevar a cabo la demostración, sin perjuicio de lo que se resuelva sobre costas, en todo caso, si el tribunal contara con los instrumentos requeridos y no es necesaria la cooperación de un técnico, procederá a realizar la prueba por si mismo, posteriormente se certificara, después de verificada la operación, el día y hora en que se verificó, el nombre y dirección de los que intervinieron en ella, la persona, cosa suceso, o fenómeno en que se produce o explica, y el juez deberá tomar las medidas necesarias para evitar que puedan ser alterados los originales de estas pruebas.

Es también fundamental la existencia de una policía adiestrada en este tipo de conductas delictivas, por lo que propongo a la par de una adecuada tipificación del fraude informático, la tecnificación de los aparatos policiales en su roll de colaboradores de la acción de la justicia.

CONCLUSIONES

Una vez finalizado el trabajo de investigación, se llega a las siguientes conclusiones:

PRIMERA.- En la actualidad existen una gran variedad de conceptos, respecto a la palabra delito, sin embargo en la presente investigación se determino que delito es aquélla acción del hombre, típica, antijurídica y culpable, de la cual se desprenden tres elementos fundamentales, la acción, el tipo, y la tipicidad este último el cual se fundamenta en la justificación.

SEGUNDA.- Como se menciona en el cuerpo de la tesis en la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática, tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática esta hoy presente en casi todos los campos de la vida moderna, con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

TERCERA.- El derecho tiene como finalidad normar la conducta humana, debido a que los actos del hombre cambian de acuerdo a la época, en la actualidad

no existe institución, incluso hogar en el que no se encuentre un ordenador o un sistema informático.

Hasta hace pocos años era imposible pensar en una red de comunicación mundial como es la *INTERNET*, por lo tanto es menester que todos los países del mundo unan sus esfuerzos a fin de evitar la propagación de los delitos informáticos.

CUARTA.- La información, hoy en día, constituye una forma de poder, el cual como todo poder puede ser objeto de control y de dominio sobre quien lo posee, por lo que, la nueva tecnología informática nos ha llevado a que junto con el *boom* del ordenador, se haya abierto en torno a éste, un nuevo foco de criminalidad por lo que no son las máquinas las que delinquen, sino los hombres.

QUINTA.- El uso de la red mundial de información permite realizar negocios por vía telemática, realizar transferencias de fondos, utilizar datos en forma rápida, casi inmediata, y a la par de todos estos adelantos científicos trae aparejado que aparezcan nuevas formas de delinquir, creándose una nueva figura como lo es el *fraude informático*.

SEXTA.- El delito informático en este caso en particular lo es el *Fraude informático*, es difícil de perseguir por las cualidades del sujeto activo de este tipo de infracciones, debido a que las huellas del mismo son borradas con cierta facilidad, y sobre todo que en nuestro país por la novedad en la comisión de este tipo de delito, no se cuenta con el personal con conocimientos suficientes para que pueda investigarlos y puedan ser detectados, y si a eso aunamos que no existe sanción alguna en nuestro Código Penal del Distrito Federal y mucho menos en el Nuevo Código Penal para el Distrito Federal, para el sujeto que comete esta conducta ilícita, nos vemos perdidos ante un mar de impunidad.

El problema parte del hecho de que nuestra legislación se basa en el principio del Derecho Romano "*nullum crimen nullum poena sine lege*", precepto que consagra en nuestra Legislación, de que no existe delito si previamente no se encuentra determinada la conducta típica antijurídica en la ley, por lo tanto, en nuestro Código Penal del Distrito Federal no existe el delito de Fraude informático.

SÉPTIMA.- Tenemos que en nuestro país, el denominador común ha sido la falta de conocimientos teóricos y jurídicos que peritos en estas materias prefieren prestar en auxilio de los legisladores y magistrados en general quienes carentes de ley y herramientas no han podido, pese a que necesitamos, como todos, hacer frente a este fenómeno cuya gravedad es inconmensurable. Como es costumbre en nuestro país llevamos varios años de retraso en el desarrollo del Derecho Informático, debido a que la preocupación radica fundamentalmente en legislar acerca de la piratería, de la propiedad Intelectual y de la propiedad Industrial respectivamente, pero esta rama del derecho abarca muchos campos más aún que no se encuentran legislados apropiadamente como lo es el del *Fraude informático*.

OCTAVA.- El *fraude informático* es una conducta en que el sistema informático es el objeto del delito, y sería solucionable mediante un esquema legal que se implantara en nuestro Nuevo Código Penal del Distrito Federal que abroga el anterior Código Penal de 1931, como se propone.

NOVENA.- El *fraude informático* comprendería en consecuencia todas aquellas conductas realizadas por medio de comportamientos astutos, engañosos, en este caso manipulaciones informáticas fraudulentas, lesivas de intereses económicos diversos, realizadas con ánimo de obtener una ventaja económica, y aprovechando las características de los sistemas informáticos y su funcionamiento.

En consecuencia, el *fraude informático* comprende todas aquellas conductas de manipulación defraudatoria en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención maliciosa de lograr un provecho, produciendo a un tercero un perjuicio económico, refiriéndome con esto tanto a la manipulación de información como (legislaciones) utilizando la intranet, al uso de claves de tarjetas de crédito vía Internet, y a la compraventa de bienes y servicios por esta vía.

DÉCIMA.- Estimamos como novedoso y correcto considerar a la pureza e idoneidad de las técnicas de la informática como el bien jurídico protegido en este delito, debemos entender que tal valor jurídico se afecta de manera directa cada vez que se cometa un ilícito informático, sin embargo en el momento que se comete un ilícito en el ámbito informático se afectan de manera indirecta otros bienes jurídicos tradicionales los cuales no debemos de perder de vista, es imprescindible la creación inmediata de una regulación dentro del Nuevo Código Penal para el Distrito Federal que regule la actividad del fraude informático desde un punto de vista globalizador e interconectado donde lo penal y lo civil se encuentre incluido, es necesario a su vez avanzar en un procedimiento penal especial para la tramitación de causas sobre delitos informáticos en general, fijando, previamente, un tribunal competente.

DÉCIMA PRIMERA.- El fraude informático se comete en general por dos tipos de personas, en primer término por aquellos que tienen autorizado el acceso al sistema y que, por ende, conocen legítimamente los códigos de seguridad, de bancos, empresas u organismos del estado, En segundo lugar están aquellos que tienen el acceso prohibido o cerrado y que ingresan al sistema a través del desciframiento malicioso del *password*, es en este último caso donde el agente comete *hacking* indirecto.

DÉCIMA SEGUNDA.- La criminalidad informática es un reto tanto para la economía, el derecho y los estados y la ciencia en general, solo superable con un

estudio dedicado, específico y unitario de esta materia, lo que me lleva a postular que el fraude informático junto con todos los delitos informáticos, un delito de futuro, por la expansión que de él se prevé al amparo de los desatados avances tecnológicos y de la insuficiencia del derecho tradicional para caminar a un ritmo tan desenfrenado.

DÉCIMA TERCERA.- Las políticas criminales precisarán de un ámbito de prevención y de seguridad aportada por los particulares, a través de la formulación de planes generales y particulares de control destinados a impedir la comisión de los delitos en base, fundamentalmente, a la anticipación de conductas, de cara a la insuficiencia del aparato represivo del estado

DÉCIMA CUARTA.- En cuanto a que el *fraude informático* sea un delito de oportunidad especial, estimo que tal situación no es una característica que distinga a los delitos informáticos en general de otros hechos ilícitos, en efecto en los ilícitos informáticos siempre habrá algún grado de premeditación, dentro del cual el delincuente debió elucubrar acerca del momento preciso en que cometerá el delito, esta situación no difiere de los delitos de homicidio cuando este ha sido premeditado, el fraude, etc; el delincuente en general siempre buscara el momento más oportuno para cometer el delito, en todos los casos la oportunidad estará determinada por factores como el que sea posible cometer el delito, la obtención asegurada de sus pretensiones, y la ponderación de las posibilidades de poder detectarlo.

FUENTES DE CONSULTA

BIBLIOGRAFÍA

AMUCHATEGUI REQUENA, Irma G. ***DERECHO PENAL***, Curso Primero y Segundo Colección de Textos Jurídicos Universitarios, Editorial Harla, México, 1990.

AZPILCUETA, Hermilio Tomás, ***DERECHO INFORMÁTICO***, Editorial Abeledo Perrot, Buenos Aires,

BAÓN RAMÍREZ, Rogelio, ***VISIÓN GENERAL DE LA INFORMÁTICA EN EL NUEVO CÓDIGO PENAL***, en ámbito jurídico de las tecnologías de la información, cuadernos de derecho judicial, Escuela Judicial / consejo General del Poder Judicial, Madrid

BARRAGÁN, Julia, ***INFORMÁTICA Y DECISIÓN JURÍDICA***, Editorial Fontamara, México, 1994.

CARRANCA Y TRUJILLO, Raúl, ***DERECHO PENAL MEXICANO***, México, Editorial Porrùa, 15ª Edición, México 1988.

CARRANCA Y RIVAS, Raúl, ***EL DRAMA PENAL***, Editorial Porrúa, México, 1982.

CARNELUTTI., Francesco, ***TEORÍA GENERAL DEL DELITO***, Editorial ARGOS, Colombia, 1960. p16.

CASTELLANOS TENA, Fernando, ***LINEAMIENTOS ELEMENTALES DE DERECHO PENAL***, 20ª Edición, Editorial Porrùa, S, A México 1984.

COLÍN SÁNCHEZ, Guillermo, ***DERECHO MEXICANO DE PROCEDIMIENTOS PENALES***, 14ª Edición, Editorial Porrùa, s, a, México, 1988.

CORREA M. ***DERECHO INFORMÁTICO***, Buenos Aires, Editorial Depalma, 1987.

CUELLO CALÒN, Eugenio, ***DERECHO PENAL,*** 14 Edición, Barcelona, 1964.

C. MEJAN, Luis Manuel, ***EL DERECHO A LA INTIMIDAD Y LA INFORMÁTICA***, Editorial Porrùa, México, 1994.

DAVARA, RODRÍGUEZ,, Miguel Ángel, ***MANUAL DE DERECHO INFORMÁTICO***, Editorial Aranzadi, Pamplona, España, 1997.

FERNÁNDEZ CALVO, Rafael, ***EL TRATAMIENTO DEL LLAMADO DELITO INFORMÁTICO EN EL PROYECTO DE LEY ORGÁNICA DEL CÓDIGO PENAL***, reflexiones y propuestas de la LI (Comisión de Libertades e Informática) en Informática y Derecho pp. 1150,.

FERNÁNDEZ GALIANO, Antonio De Castro Cid Benito, ***LECCIONES DE TEORÍA DEL DERECHO Y DERECHO NATURAL***, Editorial Universitas, S, A, 1994.

FIX FIERRO, Héctor, ***INFORMÁTICA Y DOCUMENTACIÓN JURÍDICA***, 2ª, Edición UNAM, México, 1996.

GONZÁLEZ QUINTANILLA, José Aguirre Arturo, ***DERECHO PENAL MEXICANO***, Parte General, Editorial Porrùa, México 1991.

GHERSI, Carlos Alberto, ***REPARACIÓN DE DAÑOS,*** 2ª edición, Editorial Universidad, Buenos Aires 1992.

GUERRERO M. Fernanda María, SANTOS, Eduardo Jaime, SÁNCHEZ, Julio César, ZULUAGA Víctor, CUERVO, Abel, ***PENALIZACIÓN DE LA CRIMINALIDAD INFORMÁTICA***, Editorial Ediciones Jurídicas, Colombia, 1998. pp. 169

H. AIKEN, Ch Babbage, J. Von Neumann, C. E. Shannon, A.m. Turing, W. G. Walter y otros. ***PERSPECTIVAS DE LA EVOLUCIÓN DE LOS COMPUTADORES***, Selección y Comentarios de Zenon, W. Pylyshyn, Editorial Alianza.. 1994.

HANCE, Oliver, ***LEYES Y NEGOCIOS EN INTERNET***, Editorial Mc Graw Hill sociedad Internet, México, 1992

HUERTA MIRANDA, Marcelo, LIBANO MANSSUR, Claudio, ***DELITOS INFORMÁTICOS***, 2ª edición, Editorial Jurídica Cono Sur, 1998. pp. 377

JIMÉNEZ DE ASÚA, Luis, Principios del Derecho Penal, ***LA LEY PENAL Y EL DELITO***, Editorial, Sudamericana Abeledo Perrot, Buenos Aires, 1990.

——, ***LA LEY Y EL DELITO***, 10 ª Edición, Editorial Sudamericana, Buenos Aires, 1980.

——, ***LECCIONES DE DERECHO PENAL***, Volumen 7, Editorial Harla, México, 1997.

JOYANES AGUILAR, Luis, ***PROGRAMACIÓN BÁSICA PARA COMPUTADORAS***, 3ª Edición, Editorial McGrawHill, México, 1990.

LEDESMA, Julio, C, ***DERECHO PENAL INTELECTUAL***, Editorial Universidad, Buenos Aires, Argentina, 1992.

MAGLIONA MARKOVICTH, Claudio Paul, LÓPEZ MEDEL, Macarena, ***DELINCUENCIA Y FRAUDE INFORMÁTICO***, derecho comparado, Editorial Jurídica de Chile, Chile, 1999. pp. 273.

MIR PUIG, S, (comp.) ***DELINCUENCIA INFORMÁTICA***, Promociones y Publicaciones Universitarias, Barcelona, 1992.

MURILLO Pablo Lucas, ***EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA***, Editorial Tecnos, 1990,.

ORELLANA WIARCO, Octavio Alberto, ***TEORÍA DEL DELITO***, sistemas casualista y finalista, 8ª Edición, Editorial Porrùa, México, 1999.

PALACIOS VARGAS, J. Ramón, ***DELITOS CONTRA LA VIDA Y LA INTEGRIDAD CORPORAL***, 2º edición, Editorial Trillas, México, 1985.

PAVÓN VASCONCELOS, ***DERECHO PENAL MEXICANO***, 10a Edición, Editorial Porrùa, México, 1991,

PÉREZ LUÑO, Antonio Enrique, ***MANUAL DE INFORMÁTICA Y DERECHO***, Editorial Ariel, S, A, Barcelona, 1996

REYNOSO DÁVILA, Roberto, ***DELITOS PATRIMONIALES***, Editorial Porrùa, México, 1999,.

RIBAS, Alejandro Javier, ***ASPECTOS JURÍDICOS DEL COMERCIO ELECTRÓNICO EN INTERNET***, Editorial Aranzadi, España. 2000.

RÍOS ESTAVILLO, Juan José, ***DERECHO E INFORMÁTICA EN MÉXICO***, Instituto de Investigaciones Jurídicas de la UNAM, México, 1997.

SÁNCHEZ GOYANES, Enrique, ***CONSTITUCIÓN ESPAÑOLA COMENTADA***, 21º edición, Editorial Paraninfo, Madrid, España, 2001.

SOTO GÁLVEZ, Gerardo, ***LA NECESIDAD DE REFORMA DE LA LEY FEDERAL ANTE LA IMPUNIDAD DE LOS DELITOS INFORMÁTICOS***, Tesis de licenciatura, Guadalajara Jalisco, 1997, según cita de lic. Alberto Rafael Horacio Buendía Madrigal " El Derecho Penal y los Delitos informáticos", Pág. 209.

TÉLLEZ VALDÉS, Julio, ***DERECHO INFORMÁTICO***, 2ª Edición, Editorial Mc Graw Hill, 1996.

TIEDMAN, KLAUS, ***CRIMINALIDAD MEDIANTE COMPUTADORAS, EN PODER ECONÓMICO Y DELITO***, Editorial Ariel, S, A. Barcelona 1995.

ZAFFARONI, Eugenio Raúl, ***MANUAL DE DERECHO PENAL***, Parte General, 2ª Edición, Editorial Cárdenas, México, 1998.

ENCICLOPEDIAS

ENCICLOPEDIA MULTIMEDIA SALVAT , Editores , 1999.

ENCICLOPEDIA JURÍDICA OMEBA, Tomo XII, Fama-Gara, Editorial Driskill, s,a. Buenos Aires, Argentina, 1977,

ENCICLOPEDIA DE INFORMÁTICA Y COMPUTACIÓN, INGENIERÍA DEL SOFTWARE E INTELIGENCIA ARTIFICIAL, Editorial Cultural S, A. España, 1997.

ENCICLOPEDIA DE INFORMÁTICA Y COMPUTACIÓN, Tomo HARDWARE, Madrid, España, 1997

ENCICLOPEDIA ENCARTA, MICROSOFT, 1999, "INFORMÁTICA".

ENCICLOPEDIA LAFER, Editorial Reymo, España, 1988 Págs. 3435.

ENCICLOPEDIA DE INFORMÁTICA Y COMPUTACIÓN, TELEINFORMÁTICA, Editorial Cultural, s, a. España, 1997

DICCIONARIOS.

CABANELLAS,, Guillermo, ***DICCIONARIO DE DERECHO USUAL***, Tomo I, 10 edición, Editorial Heliasta, Buenos Aires, 1976. Pág., 423

LEXIS 22, ***DICCIONARIO ENCICLOPÉDICO VOX***, Circulo de Lectores, HOMS/JOLO, Tomo 11, Barcelona 1976

LEGISGRAFIA.

AGENDA PENAL FEDERAL 2001, Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia, 9ª edición del 2001, Editorial Grupo ISEF.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, Editorial Porrùa, 138ª edición, México, 2001.

COMPILA VI, Compilación de leyes, Investigación y Automatización Legislativa, Suprema Corte de Justicia de la Nación, Dirección General de Documentación y Análisis, poder judicial de la Federación, legislación Federal y del Distrito Federal, 2002.

NACIONES UNIDAS, Revista Internacional de Política Criminal Manual de las Naciones Unidas sobre Prevención del delito y control de delitos informáticos, Oficina de las naciones Unidas en Viena, Centro de Desarrollo Social y Asuntos Humanitarios Naciones Unidas, Nueva York, números 43 y 44.

CÓDIGO PENAL , Edición 2000, Editorial Nueva Madrid, Perú, Pág. 41.

NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL, gaceta oficial del Distrito Federal, 16 de julio de 2002.

NUEVO CÓDIGO PENAL ESPAÑOL (aprobado por la ley Orgánica 10/1995, de 23 de Noviembre / BOE número 281, de 24 de Noviembre de 1995

HEMEROGRAFIA

CALLEGARI, Lidia, *DELITOS INFORMÁTICOS Y LEGISLACIÓN* revista de la facultad de derecho y ciencias políticas de la Universidad Pontificia Boliviana Medellín, Colombia, N° 70, Julio-Agosto -Septiembre, 1985.

LIMA MALVIDO, María de la Luz *DELITOS ELECTRÓNICOS*, en criminalia, México, Academia Mexicana de Ciencias Penales, Editorial Porrúa, N° 16, Año L, Enero-Junio, 1984.

SARZANA, Carlos, *CRIMINALITA E TECNOLOGÍA*, en computers crime, Rassagna Penitenciaria e Criminologia, traducción Juan Carlos Hernández Sotelo) N° 12, Año 1 1979, Roma Italia

GÓMEZ PERALS, Miguel, *LOS DELITOS INFORMÁTICOS EN EL DERECHO ESPAÑOL*, informática y derecho, N° 4 UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de informática y Derecho 2125, septiembre 1992, Mérida, 1994, Editorial Aranzadi.

ROMEO CASABONA, Carlos Maria, *LOS LLAMADOS DELITOS INFORMÁTICOS*, Revista de informática y derecho, UNED, Centro Regional de Extremadura, Mérida.

RUIZ VADILLO, Enrique, *RESPONSABILIDAD PENAL EN MATERIA DE INFORMÁTICA*, N° 9, 10 y 11, UNED, CENTRO REGIONAL DE EXTREMADURA, Mérida 1996,

REVISTA MECÁNICA POPULAR, Año 55, N°4, Abril 1998, Televisa, S, A, México,

"*Tarjetas Súper fraudes*", EL SOL DE MÉXICO, mediodía, México, Lunes 21 de Abril de 1997.

RECURSOS ELECTRÓNICOS.

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ, Facultad De Ingeniería De Sistemas computacionales, http:://www.Fisc.utp.ac.pa/museo/historia.htm.

http://uny.uasnet.mx/prof/cln/der/silvia/lexis.htm.

http://w3.mor.itesm.mx/~lssalced/histo1.html, *Última actualización 27/08/98Por Eduardo Salcedo*, Referencia: Long Larry; "Introducción a las Computadoras y al Procesamiento de la Información"; Cuarta Edición; Prentice Hall; México 1995.

WWW. Geocities.com, "Generaciones de Computadoras", Informática,.

http://w3.mor.itesm.mx/~lssalced/histo3.html,

http://www.pàginas.com%2fdetalle.php3%Fidioma%3DCastellano%26secciòn%3Dtrab%26categoria%3D41trabajos de informática,

http://www.com/html/paginas/ficha.php3?zip=conInternet.zipfichaydescargadeldoc.

http://Internet.fiestras.co.../Render&inifile=futurentese.ini&c=Articulo&cid=983562480 99,

INFORMÁTICA DE SISTEMAS, Derechos y Delitos informáticos, www.infòrmaticadesistemás.com,

http: //angelfire.com/ga/metalsystem/terminologia_T`tecnica_del_*Hacker*.html,

HELEN PEÑA, SILVIA PALAZUELOS, ROSALÍA ALARCÓN, División de Estudios de Postgrado, Facultad de Derecho, UNAM, 21 mayo 1997. fecha de consulta 25 de agosto del 2002. sgpalazu@themis.derecho.unam.mx

http//delitosinformaticos.com/noticias/102426093181806.shtml. fecha de consulta 5 de julio del 2002.

http://econsumer .gov/spanish/index.html. fecha de consulta 20 de marzo del 2002.

http://www.Informática y derecho/régimen jurídico de los bancos de daos de buenos aires

http: //www.geocities.com/Area51/Vault/3230/artiseguridad y privacidad.html.

http://www.monografias.com . EL DELITO.

Secretaria De Seguridad Publica, Ssp, Policía Federal Preventiva, Coordinación de Inteligencia para la prevención, Policía Cibernética, http://www.ssp.gob.mx/cibernética/INDEX/htm.

GLOSARIO

ActiveX.- Concepto de arquitectura de sistemas desarrollado por Microsoft como sucesor de OLE y COM y presentar una alternativa al lenguaje Java para el desarrollo de programas para la red Internet. Presenta mayores flexibilidad y rendimiento que el java pero no es independiente de la plataforma pues sólo funciona en los sistemas operativos de Microsoft.

ADN.-Traducido literalmente como Red Digital Avanzada, se refiere a las líneas dedicadas de 56 Kbps.

Anfitrión.- [En inglés, Host.] Una computadora en una red. Se aplica en vez del término en desuso "nodo" que se utiliza en el lenguaje de definición de documentos.

Applet.- Programa en lenguaje java que se utiliza en las páginas de Internet para conseguir efectos especiales que el lenguaje html no puede realizar.

Arañas.- [Spiders] Programa automatizado que busca en el Internet.

Archie.- Herramienta de software para localizar archivos almacenados en sitios FTP anónimos.

ARPANet.- Siglas de la expresión inglesa Advanced Research Projects Agency Network (Red de la Agencia de Proyectos Avanzados de Investigación), red precursora a la Internet. Se desarrolló a finales de la década de los años 60 por parte del Departamento de Defensa de los Estados Unidos en la experimentación de una amplia red funcionara tras un ataque o guerra nuclear.

ASCII.- Siglas de la expresión inglesa American Standard Code for Information Interchange (Codificación Americana Normalizada para el intercambio de Información). Es la norma mundial para la codificación usada en las computadoras a fin de representar los caracteres requeridos para la comunicación entre máquinas. Hay 128 códigos normalizados ASCII, cada uno de los cuales se puede representar con un número binario de 7 dígitos.

Autoridad de Certificación.- En inglés "Certificate Authority". Un emisor de Certificados de Seguridad para las conexiones SSL.

ASP.- [Active Server Pages]. Sistema de programación desarrollado y propiedad de Microsoft para realizar las tareas antes realizadas por los CGI.

Atado.- En inglés Attachment, también llamado Anexo, es un documento adicional incluído en un correo electrónico.

Banner.- Pequeño anuncio promocional colocado intencionalmente en una página de Internet.

Banner dinámico.- Banner con imágenes en movimiento para atraer la atención del usuario de la página.

B2B.- Del inglés "Business to business", de negocio a negocio, o bien, de empresa a empresa.

B2C.- Del inglés "Business to consumer", de negocio al consumidor.

Baud.-Unidad que representa la velocidad de transferencia de la información. Es equivalente a bytes por segundo.

bit.- Unidad elemental de la información. El nombre proviene del inglés, "binary digit" o dígito binario. Originalemente explicada por Sócrates en los Diálogos de Platón, habiéndole llamado "diada" que sería su denominación óptima.

byte.-Conjunto de 8 bits. Puesto que 8 bits es la mínima cantidad requerida para representar los símbolos alfanuméricos

bps.-Iniciales de bits por segundo. Ver también byte, baud

Buscador.- [Search site] Sitio de Internet que contiene una amplia base de datos sobre las páginas que se encuentran en la red. El mas popular es Yahoo, que opera por afinidad semántica, aunque sean más efectivos otros buscadores como Altavista o Excite que operan por afinidad textual. Para lograr su objetivo los buscadores utilizan arañas.

Cache.-Espacio de almacenamiento temportal que el navegador emplea para almacenar los archivos (textos e imágenes) que recibe del Internet. Cuando se vuelve a visitar una página, el navegador rápidamente obtiene los archivos desde el cache en lugar de obtenerlos de la localidad remota donde origininalmente los encontró. Se habla del cache de disco cuando los datos se guardan en el disco duro y de cache de memoria cuando se almacenan en la RAM de la computadora.

Certificado de Seguridad.- Archivo de texto usado por el protocolo SSL para establecer una conexión segura. La información en los certificados de seguridad incluye a quien pertenecen, al emisor, un número único de identificación, fechas de validéz y una "huella" encriptada que se puede usar para verificar el contenido del certificado.

Para que exista una conexión SSL ambas partes deben poseer un Certificado de Seguridad válido.

Cliente- [Client] Máquina que conectada a una red solicita acciones a otra que actua como servidor.

CGI.- Interface de la Compuerta Común (Common Gateway Interface). Es un conjunto de reglas que describe como se comunica un servidor de la red con otros programas en la misma máquina y como otros programas (programas CGI) se comunican con el servidor. Cualquier programa se puede considerar como CGI si maneja la entrada y salida de información de acuerdo con la norma CGI. Un programa CGI es aquél que se ejecuta en el servidor y no en el navegador del cliente. De esta manera el programa tiene acceso tanto a los datos del servidor como a todos los archivos que hay en él.

CGI-BIN- Nombre común del directorio del servidor en el que se almacenan los programas CGI

Código de retorno- [Return Code] El estado de respuesta a una solicitud especificando el resultado de una solicitud.

Los más comunes son los códigos de error:

- 400 = Failed: Bad Request (Mal requerido)
- 401 = Failed: Unauthorized (No autorizado)
- 402 = Failed: Payment Required (Se requiere pagar)
- 403 = Failed: Forbidden (Prohibido)
- 404 = Failed: Not Found (No encontrado)
- 500 = Failed: Internal Error (Error interno)
- 501 = Failed: Not Implemented (No implementado)
- 502 = Failed: Overloaded Temporarily (Sobrecargado temporalmente)
- 503 = Failed: Gateway Timeout (Tiempo terminado para el "gateway")

Compatibilidad.- (De un navegador) Este término se refiere a que la página por su creación (programación) contiene instrucciones que pueden interpretarse por cualquier navegador.

Compresión.- [Compression] El proceso de reducir el tamaño en bytes de un archivo para reducir el tiempo de su transferencia entre máquinas. Ver también Tiempo de Carga

Cuartilla.- Página de papel de tamaño carta, a doble espacio, con 12 caracteres por pulgada y los cuatro márgenes de una pulgada de ancho.

Ciberespacio.- Del término en inglés cyberspace, originado por el escritor William Gibson en su novela "Neuromancer the word Cyberspace" y que se usa para describir la totalidad de los recursos informáticos disponibles a través de las redes de cómputo.

CSS.- [en inglés Cascading Style Sheets, literalmente hojas de estilo en cascada.] Método que permite definir por separado las reglas para definir las características de los elementos HTML, DHTML y XML. Sus versiones se distinguen por el número de edición: CSS1, CSS2, etc.

Daemon.-Programa que corre independientemente del navegador. Los Daemones pueden realizar varias tareas administrativas como las de construir índices, resumenes y retroenlaces. En Unix se utiliza el término por el de servidor debido a que los servidores operan independientemente.

DHTML.-[Dynamic html o html dinámico]. Combinación de html, hojas de estilo y Javascript que permiten modificaciones automáticas en los elementos de las páginas Ver por ejemplo la Galería de diseño.

DOM.-[Document Object Model o Modelo de objetos en documentos]. Es una interface independiente de la plataforma y del lenguaje que permite que los programas y scripts tengan acceso dinamicamente y actualicen el contenido, la estructura y estilo de los documentos.

Dominio.- [Domain] El nombre asociado a una dirección IP de una computadora en el Internet. Por ejemplo, hermosillovirtual.com

Espinazo.- (En inglés Backbone). Una línea de alta velocidad o serie de conexiones que forman una trayectoria principal en una red.

FAQ.- De la frase en inglés Frequently Asked Questions (o Preguntas más frecuentemente contestadas). Son documentos que listan las preguntas más comunes sobre un tema asi como las respuestas a las mismas. Las FAQ generalmente se escriben por gente cansada de contestar una y otra vez las mismas preguntas.

Finger.- Herramienta de programación utilizada para comprobar la presencia de una persona atendiendo una cuenta de Internet.

Extranet.- La red usada por una empresa para conectarse con sus clientes y socios de negocios.

Ver también el término Intranet

Firewall.- En español, barrera de fuego. Programa o equipo que separa a una red local (LAN) en dos o más partes con propósitos de seguridad.

FTP.- [File Transfer Protocol] Protocolo de transferencia de archivos. Es el método normal de enviar archivos entre computadoras en el Internet.

Galletas.- [Cookies] Son archivos que contienen información respecto a los visitantes de un sitio (por ejemplo, el nombre del usuario y sus preferencias). Esta información la proporciona el usuario en su primera visita al servidor. El servidor registra esta información un un archivo de texto y la guarda en el disco duro del usuario. Al regresar al sitio, el servidor busca la galleta y la utiliza.

Gateway.- O compuerta es un programa o equipo que se encarga de traducir la información contenida en dos protocolos diferentes.

Hit.- Acción de solicitar una acción a un servidor, tal como requerir la visualización de una página o la transferencia de un archivo.

Hipertexto.- [Hypertext] es el término que se dio al enlace que permite el salto rápido entre dos textos por afinidad conceptual. El hipertexto permite por ejemplo, saltar desde la frase *"Cristóbal Colón descubrió América....."* (Con los términos *Colón* y *América* como hipetextos) enlazando a una frase tal como *"Cristóbal Colón nació en Génova...."* o bien a *"América es uno de los cinco continentes.....".*
Para mayor detalle lea el artículo ¿Qué es el hipertexto?

html.- Abreviación del término en inglés HyperText Marking Language (Lenguaje de marcado de hipertextos), es el lenguaje de programación que permite la inclusión de textos, imágenes fijas y móviles, video, archivos, etc. y su enlace mediante hipertexto por el usuario de la computadora, independientemente de la estructura de la máquina o del sistema.

HTTP.- Abreviación de la designación inglesa para Protocolo de transferencia de hipertexto. Se trata del protocolo más utilizado para transferir datos entre un servidor y otra máquina.

Internet.- [De inter, internacional y net, en inglés, red].- Todas las computadoras del mundo conectadas entre si. como si se tratara de una enredadera o red. En su primera etapa la conexión de las computadora es a través de la red telefónica existente. En su última étapa la conexión será por medio de fibra óptica, si es que no aparecen tecnologías que le permitan hacerlo vía inalámbrica.

IGU.- [En inglés, GUI. Interface gráfica del usuario.] Presentación en pantalla del programa en cuestión que permite que el usuario interactúe con éste. Lo constituyen las imágenes, los íconos y los menús.

Internic.- [Internet Network Information Center. Centro de Información de la Red Internet]. Organización privada responsable del registrar los nombres de los dominios de la red.

Intranet.- [De intra, interno y net, en inglés, red].- Red interna de una empresa, que parcialmente puede exponer información al exterior via Internet. Es el concepto moderno con el que se manejan los sistemas internos de una empresa, tales como inventarios, requisiciones, liberaciones; ordenes de entrada y salida de almacen; ordenes de trabajo, de venta y de compra; facturación, requisiciones; documentación MRP I y II, SPC; documentación técnica y de producto, etc. permitiendo que los empleados accedan al sistema a través de un sistema de accesos controlados. Ver también el término Extranet

IP o dirección IP.- [IP Address] Dirección en el protocolo del Internet que identifica a una máquina conectada.

ISP.- Siglas de Internet Service Provider (Proveedor del servicio de Internet). Empresa que proporciona el servicio de acceso a la red Internet.

Java.- Lenguaje de programación de computadoras, cuyo creador, la compañía Norteamericana Sun, ideó como un lenguaje que puede usarse en todas las computadoras, independientemente de sus diferencias o plataformas. El lenguaje java permite que el mismo programa que se ejecuta en una Apple se pueda ejecutar también en una máquina compatible con las PC (Personal Computer), originalmente desarrolladas por IBM. En las páginas se pueden incluir programas escritos en el lenguaje java como applets

Javascript.- Lenguaje para realizar programas que logran efectos especiales en las páginas desarrollado por la compañía Netscape. Hoy en día tiene soporte suficiente para ser interpretado por una gran cantidad de navegadores de Internet. Ver también CSS y html dinámico

LOG (Archivo).- [Log File] Archivo creado por un servidor que contiene toda la información relativa al acceso a un sitio.

Macromedia.- Empresa que desarrolla programas multimedia de gran espectacularidad por los efectos combinados de sonidos, movimiento y transformación de imágenes para alcanzar efectos especiales en las páginas del Internet. Requiere que el usuario halla instalado una extensión especial a su navegador para observar estos efectos. Estos programas entran en decadencia con el desarrollo del formato SVG.

Marcos.- [En inglés frames]. Procedimiento por el cual se divide una página en varias secciones, cada una de las actúa como una página por separado.

META (Etiquetas META).- Elementos de programación HTML que permiten clasificar el contenido de las páginas en los sitios. Se definen así el lenguaje a utilizar, la descripción del contenido de la página, el conjunto de carácteres a utilizar, entre otros datos útiles.

MIME.-. Siglas de la expresión inglesa Multipurpose Internet Mail Extensions (Extensiones de correo Internet multipropósito). Norma para anexar archivos no textuales a los mensajes de correo normales de la Internet. Tales archivos pueden ser gráficos, hojas de cálculo, documentos de procesadores de texto con formato, audio o video.

Se dice que un programa de correo es compatible con MIME si puede enviar y recibir archivos usando esta norma. Al enviar estos archivos se codifican como si se tratara de texto, aunque este no sea legible. La norma MIME se usa también para que los navegadores identifiquen los archivos enviados al buscarlos en una lista de tipos MIME que los relaciona con los programas específicos para manejar cada tipo de archivo.

Multimedia.- El término, creado fundamentalmente para propósitos comerciales, se refiere a la utilización de los diferentes medios de comunicación con el usuario que tiene una computadora, permitiéndo combinar imágenes en movimiento con sonidos.

Navegador.- [Browser, literalmente "paginador"] Es el programa de computadora que permite interpretar y presentar la información en lenguaje html.

Netiqueta.-. Ver el artículo La netiqueta para una explicación de fondo.

NIC.- Siglas de la designación en inglés Networked Information Center (Centro de Información de Red). Cualquier oficina que maneje la información sobre una red. La más famosa es la InterNIC, encargada de la administración de los nombres de dominio registrados.

P3P.- [Platform for Privacy Preferences Project o Proyecto de plataforma para preferencias privadas]. Norma del WC3 para proporcionar a los usuarios una manera automatizada por la que los usuarios toman mayor control sobre el uso de su información personal en los sitios que visitan.

Página.- [Page] Documento de computadora que se presenta mediante un navegador.

Página Principal.- [Home Page, que literalmente significa "página del hogar".] Se trata de la página más importante de un sitio. Proporciona un resumen y los enlaces al resto del sitio. Frecuentemente contiene una tabla del contenido del sitio o el enlaces a la tabla.

Plataforma.- [Platform] El sistema operativo de la máquina, tal como Windows 95, Windows NT, UNIX, LYNUS, etc.)

Plug-in.- Programa de computación que se agrega al Navegador para manejar en éste cierto tipo de archivos.

PICS.- [Platform for Internet Content Selection o Plataforma para la selección de contenido en la red Internet]. Esta especificación permite etiquetas (metadatos) que asocian el contenido de la red Internet. Originalmente se diseñó para controlar el acceso infantil a la red, pero también facilita la utilización de firmas y otros aspectos de privacidad. Más información en www.netparents.org

POP.- [Post Office Protocol o Protocolo de Oficina Postal]. Un protocolo por el que un servidor de correo permite recoger los mensajes electrónicos y descargarlos en su computadora. Un servidor POP es la computadora en la que se encuentran los mensajes de correo electrónico.

Portal.- Página utilizada para comenzar una sesión de Internet. Los portales se caracterizan por incluir información útil tal como noticias, el clima, servicio de correo electrónico y en general cualquier información relevante para el usuario.

Protocolo.- [Protocol] El conjunto de reglas que permite intercambiar datos entre dos máquinas.

Puente.- En inglés Bridge, es un dispositivo que se usa para enlazar dos redes dando como resultado una sola red.

RDF.- [Resource Description Framework o Marco de trabajo para la descripción de recursos]. Esquema que integra diversos metadatos, incluyendo mapas de sitios, calificación de contenido, definiciones de los canales con flujo (streaming), las colecciones de datos para los buscadores y otros conceptos, empleando la sintaxis del XML.

Retroenlace.- [Back link.] Un enlace en una dirección implica la existencia de un enlace correspondiente en la otra dirección.

Ruteador.- [En inglés, Router]. Dispositivo que enruta los paquetes de información electrónica tomando decisiones de tráfico, en base a las condiciones de la red.

Script.- Pequeño programa para realizar efectos especiales en las páginas.

Servidor.- [Server] Máquina conectada a otras que ejecuta una acción a solicitud de las otras (clientes).

Servlet Aplicación Java que opera como un módulo en un servidor. Ver también .

SGML.- [Standard Generalized Markup Language o Lenguaje de marcado normativo generalizado] Es la recomendación general (ISO 8879) de la ISO (International Organization for Standardization, u Organización Internacional de Normas) para la creación de métodos de representación de textos en forma electrónica independientes de la máquina o plataforma (1986).

Sitio .- [Site] Este término se aplica a la ubicación donde se encuentra la información personal (sitio personal) o de la compañía (sitio empresarial). A todo sitio está asociada cuando menos una dirección de Internet (url) y una IP.

SMIL.-[Synchronized Multimedia Integration Language o Lenguaje de integración sincronizado de multimedia]. Es un lenguaje basado en XML que permite mezclar presentaciones en varios medios y sincronizarlas. Aunque puede parecer complicado, es relativamente sencillo para alguien familiarizado con html y javascript.

SMTP.- [Simple Mail Transfer Protocol o Protocolo Sencillo de transferencia de correo.] El protocolo con el que se transmite un mensaje de correo electrónico de una máquina a otra.

SSL.- Protocolo para permitir comunicaciones encriptadas y autentificadas a través de la red Internet. La aplicación del protocolo se inicia generalmente con la llamada a una página con el protocolo "https". El protocolo propociona privacidad, autentificación e integridad en el mensaje. En una conexión segura o SSL cada una de las partes envía información a la otra del Certificado de seguridad propio, que se utiliza para codificar la información. Para decodificar esta información se requiere por lo tanto dos claves, una del emisor y otra del receptor, garantizando la seguridad de los mensajes.

Streamer.- Servidor modular, esto quiere decir que las características del mismo se pueden ampliar con "módulos" externos programados por los propios creadores de la aplicación o por cualquier usuario para satisfacer una necesidad concreta. Este programa realiza las funciones de servidor web de alto rendimiento con características en cuanto a rendimiento y estabilidad similares a otros servidores del mercado como Apache o Microsoft IIS. En lo referente a compatibilidad, soporta la mayoría de estándares del mercado: Wap, "streaming multimedia" mediante la configuración de los tipos MIME adecuados, etc... además soporta tecnologías propias de otras plataformas com SSI (Server Side Includes), CGI, etc. Además de todas estas tecnologías soportadas de otros programas servidores, aporta tecnologías propias como scripts en Pike y lenguaje RXML (RoXen Marcro Language)

Sufijo del dominio.- [Suffix of Domain Name.] Sufijo de tres dígitos para identificar el tipo de organización.

- .com = Comercial
- .edu = Educacional
- .int = Internacional
- .gov = Gubernamental
- .mil = Militar
- .mx Usado solo identifica a una organización gubernamental mexicana. Acompañado por otro sufijo explicita que se encuentra en México.
- .net = Red
- .org = Organization

SVG.- [Scalable Vector Graphics o Gráficos vectoriales escalables] es un formato de imagenes basado en el XML desarrollado por el W3C que permite transferir las imágenes más rapidamente, hacerlas escalables y buscables, además de otras características.

TCP/IP.- Tomado de la expresión en inglés Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisiones y protocolo de la Internet). Es el conjunto de Protocolos que definen la comunicación Internet.

Tiempo de carga.- [Load Time] El tiempo requerido, generalmente expresado en segundos, para que el contenido total de una página de Internet se transmita por entero al usuario. Los

tiempos de carga deben ser reducidos a fin de no impacientar al usuario. La regla de que suceda algo antes de 5 segundos después de la acción del usuario proviene de la especificación del antiguo sistema operativo MS-DOS.

T1.- Norma norteamericana para líneas de transmisión de señales telefónicas que operan a 1.544 Millones de bps.

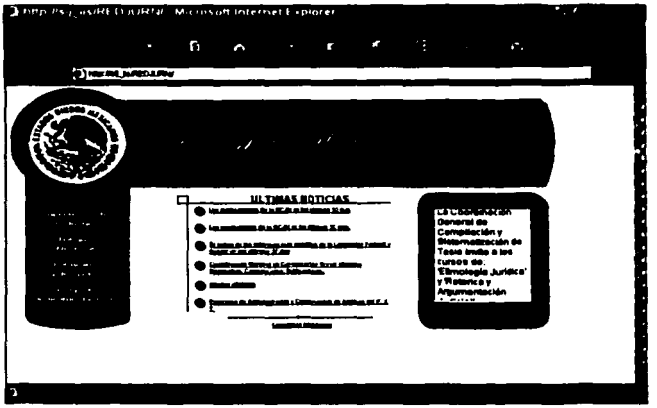
URI.-[Uniform Resource Identifier o Identificador Uniforme del recurso] Es el conjunto generico de todos los nombres y direcciones en forma de denotaciones cortas que se refieren a un recurso.

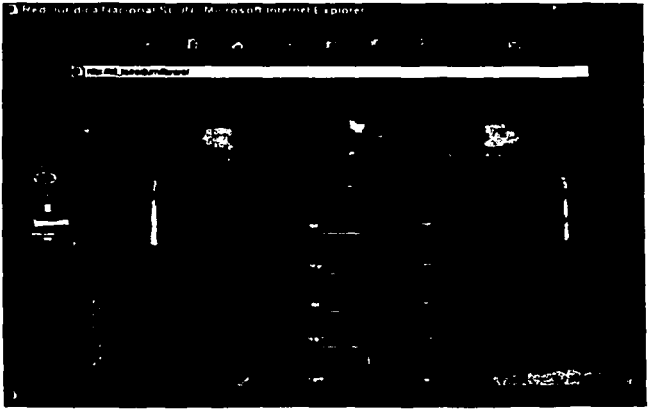
URL.-[Uniform Resource Locator o Localizador uniforme del recurso] Es el mecanismo para identificar una ubicación exacta en el Internet. Por ejemplo, *http://www.hermosillovirtual.com/servicios/glosario.htm* define la ubicación de la página *glosario.htm* en el directorio *servicios* en la máquina *hermosillovirtual.com* con un protocolo específico (*http, ftp, etc.*.

URN.-[Uniform Resource Name) o nombre uniforme del recurso.

ANEXO 1

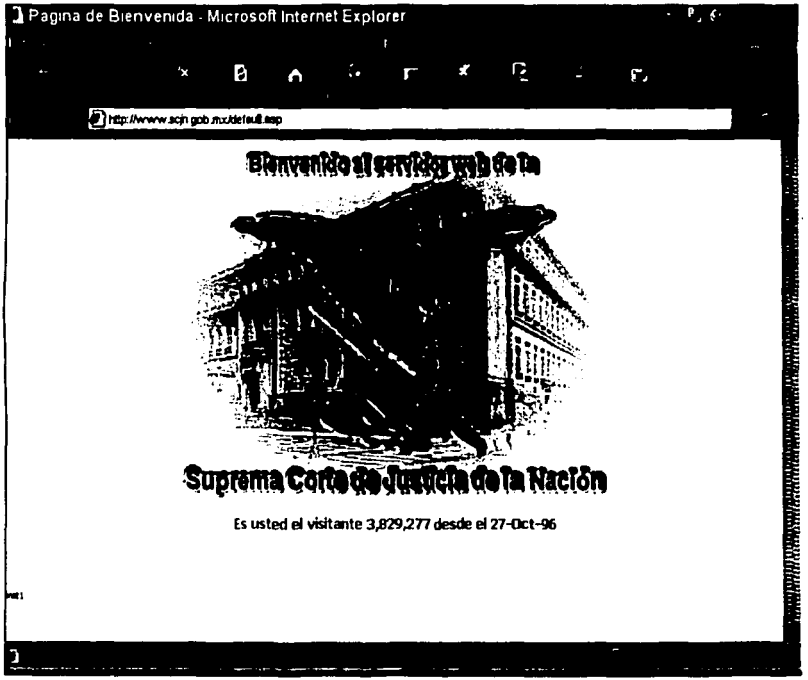
RED JURÍDICA NACIONAL.





ANEXO 2

PAGINA INTERNA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN.



ANEXO 3

RED JURÍDICA INTERNA.