UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL MEXICANA"

T E S I S

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO
P R E S E N T A:

MARCO ANTONIO ALONSO QUEZADA

ASESOR

LIC. HUMBERTO GAONA SANCHÉZ

SAN JUAN DE ARAGON ESTADO DE MÉXICO MARZO DE 2002

PAGINACION DISCONTINUA

Parte importante y fundamental del presente trabajo es mi escuela, mis maestros y mi asesor;
sin ellos como pensar en llegar a este punto si ellos forman parte del camino.
Por todo ello mil gracias:
"ENEP ARAGÓN 96-99"

Este trabajo podría ser dedicado a muchas personas:

a Sebastián por la gran admiración.

a Elvia por ser un reflejo de cariño.

a Pilar definición de carácter y lucha.

a Virginia y su alegría.

a mi novia Gisell, la primera mujer en verdad en mi vida.

Y claro al recuerdo de mi padre.

Pero más que un trabajo esto ha sido un esfuerzo,

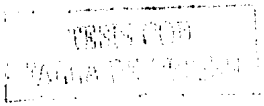
y este esfuerzo es de una sola persona: Mi Madre.

Por su ayuda y por sus golpes, por aguantar todo este tiempo y por darme un gran ejemplo de lucha y amor a la vida.

Espero que este pequeño esfuerzo recompense tantos años de lucha, por todo lo que me has dado:

GRACIAS MAMA

ÍNDICE



INTRODUCCIÓN

El cambio en la vida del hombre ha sido una constante en su vida diaria, en tan solo algunos años, los cambios en sus actividades diarias son imposibles de describir, el hombre de los años 20' no reconocería todos los cambios que se han originado de ese tiempo a la fecha, como decirle que en unas cuantas horas puede recorrer el mundo entero, que su voz, que su imagen puede llegar en segundos a lugares tan lejanos; y es que la explicación solo tiene una respuesta: "*La Evolución Tecnológica*".

Podemos entender esa evolución como la actividad del hombre que lo ha llevado desde la invención del fuego, hasta la conquista del la luna; pero en la actualidad el hombre ha logrado grandes avances tecnológicos trascendentales y sobre todo con un ritmo muy acelerado; estos avances transforman las relaciones del mismo, producen grandes cambios en su conducta y traen aparejados grandes riesgos con los beneficios creados por los mismos.

La aparición de una nueva era informática a traído consigo el surgimiento paralelo de nuevas conductas criminales relacionadas con la creación de los sistemas informáticos; con una nueva forma de realizar diversas transacciones que conllevan el traslado de grandes cantidades de valores, nace inmediatamente una nueva forma de realizar ilícitos para esta actividad, a estas conductas se les ha llamado comúnmente *Delitos Informáticos.*

El presente trabajo pretende hacer un análisis de la situación que guarda el Derecho Penal Mexicano frente a estas nuevas conductas (Delitos Informáticos), es necesario precisar si cuenta con la tutela necesaria para prevenir y en su caso castigar este tipo de conductas.

Para ello es necesario conocer los antecedentes de los sistemas informáticos, así como una serie de elementos fundamentales que le darán al lector la posibilidad de entender de forma plena el presente trabajo, y que van desde la situación en la que se encuentra el sistema informático en México, hasta conceptos de Derecho o Delito; todo esto se manejará en el **Capítulo I.**

En el **Capítulo II** tendremos a la vista un análisis de los Delitos Informáticos, su concepto, sus elementos y clasificación, así como las diversas posturas que se han adoptado a nivel internacional en cuanto a su naturaleza jurídica y las diversas organizaciones internacionales que trabajan en su problemática, a fin de entender plenamente a la figura jurídica que en cuestión abordamos.

En seguida es necesario analizar cada una de las conductas que tradicionalmente han sido consideradas como Delitos Informáticos, en la Legislación Penal Mexicana, con el objeto de determinar si estas conductas encuentran protección efectiva en nuestro país. El análisis de cada una de las figuras nos permitirá determinar, si con base en el principio del bien jurídico, nos encontramos ante una nueva figura delictiva con carácter autónomo respecto de otros delitos, que amerite desde luego protección jurídica, o si las mismas conductas no son más que medios para la comisión de figuras típicas tradicionales.

En el ultimo apartado se desprende la esencia de los Delitos Informáticos, los bienes jurídicos que se ven afectados con su comisión, lo que nos lleva al análisis de los cauces legislativos idóneos para brindar una adecuada protección a los bienes jurídicos conocidos, o al reconocimiento de un bien jurídico de nueva aparición que amerite tal protección.

ABREVIATURAS

CPDF.:	Código Penal para el Distrito Federal.
CPF.:	Código Penal Federal.
CPES.:	Código Penal del Estado de Sinaloa.
LVGC.:	Ley de Vías Generales de Comunicación.
LFT.:	Ley Federal de Telecomunicaciones.
LFDA.:	Ley Federal del Derecho de Autor.
CCDF.:	Código Civil para el Distrito Federal.
LPI.:	Ley de la Propiedad Industrial.

CAPÍTULO I

ANTECEDENTES Y CONCEPTOS FUNDAMENTALES

CAPÍTULO I

1.1 Historia de la informática.

La historia de la informática, para muchas personas es reciente, creen que esta nace a partir de la aparición de las computadoras, pero la informática es mucho más que eso y por supuesto tiene mucha historia tras de si, la cual, es necesaria conocer para entender la presente investigación.

Podemos encontrar el primer antecedente de la informática aproximadamente hace unos 2 500 años, siendo el *ábaco*, cuya aparición se encuentra plenamente documentada en China; aportando también el primer escrito binario, conocido como: "*I Ching*" o el "*Libro de las Mutaciones*".

En Occidente las principales referencias las encontramos en Grecia, **Tales de Mileto** describía algunos aspectos de la electricidad estática (de ese mismo texto se desprende la palabra electrón); la construcción del primer robot lo encontramos en Alejandría, realizado por **Heron**, un experto en hidráulica; dicho robot simulaba ser un actor de teatro.

En 1642 el francés **Blas Pascal** fabrica la primera máquina sumadora mecánica la cual es perfeccionada en 1666 por **Samuel Morland**; este instrumento es de suma importancia ya que realizaba operaciones que hasta ese entonces se creían exclusivas de la mente humana.

Una mención especial requiere el desarrollo de un *telar automático* por el francés **Joseph Jacquard**. En efecto, analizando las operaciones repetitivas que requería la producción de telas, este inventor imaginó conservar la información repetitiva necesaria bajo la forma de perforaciones en tarjetas. Estas perforaciones eran detectadas mecánicamente, asegurando el desplazamiento adecuado de las guías del hilado (tal como aún hoy ocurre en las máquinas caseras).

El hecho más importante del siglo XIX es la concepción de una máquina procesadora de información, capaz de autocontrolar su funcionamiento, esto se debe al ingles **Charles Babbage**, él cual crea la máquina denominada "*máquina de diferencias*", capaz de resolver ecuaciones polinómicas mediante el calculo de diferencias sucesivas entre conjuntos de números.

El segundo hecho fundamental del Siglo XIX corresponde a **George *Boole***, fundador de una nueva álgebra. En 1847 "*El Análisis Matemático del Pensamiento*", en 1854 publica "*Las leyes del pensamiento*". Su álgebra consiste en un método para resolver problemas de lógica que recurre solamente a los valores binarios "1" y "0" y a tres operadores: *"AND" (y), "OR" (o) y "NOT" (no)*. A partir de esta se ha desarrollado posteriormente lo que conocemos hoy como *"código binario"*, que utilizan todos los computadores actuales.

En 1937, **Claude Shannon** y **Warren Weaver**, desarrollaron lo que se llamó "*teoría matemática de la comunicación*" hoy más conocida como "*Teoría de la Información*", estableciendo el concepto de "negentropía" (la información reduce el desorden) y la unidad de medida del *"bit"* (*binary digit*), aplicada hoy día tanto en telecomunicaciones como en informática.

Alan Turing, científico ingles crea a "*Colossus*" (1943), computador que permitía descifrar en pocos segundos los mensajes cifrados generados por la máquina "*Enigma*" alemana. Esta era en realidad un computador *"dedicado"*, es decir, con una única función, descifrar los códigos de la máquina *Enigma*.

Funcionaba con 2.400 válvulas y 5 paneles de lectura óptica de cintas perforadas, capaz también de imprimir los mensajes descifrados.

John P. Eckert y John W. Mauchly construyeron en 1947, en la Universidad de Pennsylvania, el *ENIAC (Electronic Numerical Integrator and Calculator)*, *primer computador electrónico*, compuesto de 17.468 válvulas o "tubos" (más resistencias, condensadores, etc.), con 30 toneladas de peso, en 1,5 segundos podía calcular la potencia 5000 de un número de 5 cifras.

En 1949 fue publicado el resultado teórico de los trabajos del equipo de **Wiener** bajo el título de *"Cybernetics"*. La naciente cibernética se definió como "*teoría de la comunicación y autorregulación en sistemas probabilistas extremadamente complejos*".

Las máquinas con válvulas constituyeron la llamada *"primera generación"* de computadores.

En 1947, tres científicos - **Bardeen, Brattain y Shockley** de los laboratorios *Bell* habían inventado un semiconductor de tamaño reducido capaz de realizar funciones de bloqueo o amplificación de señal: nacía el *transistor*. Más pequeños, más baratos y mucho menos calientes que las válvulas de vacío,

los transistores desplazaron rápidamente a éstas en todos los aparatos electrónicos, especialmente en los computadores.

En los años 60, técnicos de varios laboratorios se dieron cuenta que la técnica de fabricación de los transistores posibilitaba la producción de unidades más pequeñas con múltiples componentes cumpliendo las diversas funciones electrónicas requeridas. Así nacieron los *circuitos integrados*, los cuales permitieron una nueva disminución del tamaño y del costo de los aparatos.

Con lo anterior nace la *"segunda y tercera generación"* de computadoras.

En 1971, la compañía *Intel* lanza el primer microprocesador: un circuito integrado especialmente construido para efectuar las operaciones básicas ya señaladas por **Babbage** y conforme a la arquitectura definida por **Von Neumann**, que conocemos como *"Unidad Central de Procesos" (CPU)*.

En 1984, la compañía *Apple* lanzó una máquina que introduciría nuevamente una revolución: el *Macintosh*. Éste era el sucesor de un modelo llamado "*Lisa*" pero que no tuvo aceptación debido a su costo y escasa capacidad en que se introducía por primera vez el concepto de interfaz gráfica, la analogía del

los transistores desplazaron rápidamente a éstas en todos los aparatos electrónicos, especialmente en los computadores.

En los años 60, técnicos de varios laboratorios se dieron cuenta que la técnica de fabricación de los transistores posibilitaba la producción de unidades más pequeñas con múltiples componentes cumpliendo las diversas funciones electrónicas requeridas. Así nacieron los *circuitos integrados*, los cuales permitieron una nueva disminución del tamaño y del costo de los aparatos.

Con lo anterior nace la *"segunda y tercera generación"* de computadoras.

En 1971, la compañía *Intel* lanza el primer microprocesador: un circuito integrado especialmente construido para efectuar las operaciones básicas ya señaladas por **Babbage** y conforme a la arquitectura definida por **Von Neumann**, que conocemos como *"Unidad Central de Procesos" (CPU).*

En 1984, la compañía *Apple l*anzó una máquina que introduciría nuevamente una revolución: el *Macintosh.* Éste era el sucesor de un modelo llamado "*Lisa*" pero que no tuvo aceptación debido a su costo y escasa capacidad en que se introducía por primera vez el concepto de interfaz gráfica, la analogía del

"escritorio" y un nuevo periférico: el *"mouse"* o *ratón*, como herramienta para controlar al computador.

Así han podido fabricarse nuestros microcomputadores y los sistemas portátiles, al mismo tiempo que se aumenta permanentemente la capacidad de memoria interna de la máquina, para conservar más datos mientras se procesan. La velocidad, a su vez, superó ampliamente los diez millones de operaciones por segundo, llegando actualmente a cerca de 100 millones en los microprocesadores más avanzados utilizados en computadores grandes o *"mainframes"*.

Por todo lo anterior podemos definir a la informática como el la *herramienta* más importante de nuestros días, soporte de los conocimientos en relación a los sistemas computarizados y sus aplicaciones.

1.1.1 Informática en la actualidad.

Es indudable que hoy día la computación ha revolucionado *todas* las actividades del hombre, no existe ninguna conducta humana donde no se encuentre presente la informática; y es que al hablar de informática, no debemos pensar solo en las computadoras.

Al hablar de informática, debemos hablar de los circuitos y procesadores de todos y cada uno de los aparatos con los que convivimos a diario, así tenemos: las televisiones, radios, hornos de microondas, cámaras de video, celulares, relojes digitales, equipos de comunicación, automóviles, aviones, radiolocalizadores, y en general todas las piezas "*informáticas*" que hacen trabajar de una o de otra manera los diversos aparatos que usamos en nuestra vida diaria.

Los nuevos adelantos en el campo de la informática nos permiten mejorar muchas de las actividades del hombre, como ejemplo claro tenemos las comunicaciones; hablar de *Internet* es hablar de un acercamiento global, las distancias se acortan inimaginablemente al igual que los tiempos.

Este medio de comunicación nos permite transferir datos en diversos formatos, en audio, en video o de forma escrita, las empresas tienen una mayor facilidad

de publicitar y vender sus productos, los usuarios tiene la información al instante y de los puntos más alejados del planeta, se puede enviar y recibir información de manera instantánea sin importar el tamaño o el formato de la misma a cualquier parte del mundo.

A continuación se mostraran algunas de las estadísticas más importantes a nivel internacional con relación a este fenómeno:

PAÍSES CON EL MAYOR NÚMERO DE COMPUTADORAS EN USO 1998 *1*

Lugar	País	Computadoras en uso (miles)
1	Estados Unidos	121,030
2	Japón	28,760
3	Alemania	18,900
4	Reino Unido	16,540
5	Francia	13,700
6	Canadá	10,560
7	Italia	9,250
8	Australia	6,880
9	China	6,240
10	Corea del Sur	5,760
11	España	5,030
12	Rusia	4,720
13	Países Bajos	4,550
14	Brasil	4,010
15	México	3,960

1 Juliussen, Egil; Internet Industry Almanac; marzo 1999.

PAÍSES CON EL MAYOR NÚMERO DE USUARIOS DE INTERNET 1998 *2*

Lugar	País	Usuarios de Internet (miles)
1	Estados Unidos	54,675
2	Japón	7,965
3	Reino Unido	5,828
4	Canadá	4,325
5	Alemania	4,060
6	Australia	3,347
7	Países Bajos	1,386
8	Suecia	1,311
9	Finlandia	1,250
10	Francia	1,175
11	Noruega	1,007
12	España	920
13	Brasil	861
14	Italia	841
15	Suiza	767
27	México	312

COMPUTADORAS INSTALADAS EN AMÉRICA LATINA 1994-2000 (millones) *3*

	1994	1995	1996	1997	2000
México	2.05	2.57	3.23	3.96	6.25
Argentina	0.74	0.97	1.22	1.51	2.58
Brasil	1.76	2.42	3.15	4.01	8.54
Chile	0.30	0.40	0.52	0.65	1.34
Colombia	0.52	0.69	0.87	1.08	1.98
Perú	0.35	0.44	0.56	0.69	1.24
Venezuela	0.49	0.61	0.74	0.88	1.45
Mundial	219	259	306	360	579

2 Idem.
3 Idem.

USUARIOS DE INTERNET EN AMÉRICA LATINA 1994-2000 (miles) *4*

	1994	1995	1996	1997	2000
México	23.1	47.9	119	312	2,048.0
Argentina	4.4	18.2	42.6	92.8	946.0
Brasil	2.8	70.4	290.0	861.0	5,198.0
Chile	10.4	30.7	63.7	156.0	824.0
Colombia	3.9	7.7	32.4	87.0	671.0
Perú	0.57	2.77	18.1	47.6	442.0
Venezuela	1.81	3.96	9.38	37.6	534.0
Mundial	17,952.0	345,599.0	59,852.0	99,960.0	327,069.0

POBLACIÓN ESTIMADA 1994-2000 (millones) *5*

	1994	1995	1996	1997	2000
México	92.10	94.00	95.70	97.50	102.90
Argentina	33.87	34.29	34.70	35.10	36.20
Brasil	158.50	160.70	163.00	164.50	169.50
Chile	13.91	14.16	14.40	14.60	15.21
Colombia	35.49	36.20	36.90	37.50	39.17
Perú	23.63	24.09	24.50	24.93	26.26
Venezuela	20.53	21.01	21.40	21.82	23.20
Mundial	5,638.00	5,734.00	5,824.00	5,912.00	6,170.00

4 Idem.
5 Idem.

1.1.2 Informática en México.

Desde hace más de dos décadas se reconoció en México la importancia de la informática en el desarrollo nacional, por lo que se iniciaron acciones de distinta índole para estimular su desarrollo y asimilación.

En los años sesenta se instrumentaron fundamentalmente políticas de protección para los usuarios incipientes del sector público. En los años ochenta las acciones favorecieron el establecimiento de una industria microelectrónica nacional y mantuvieron un adecuado control del gasto gubernamental en bienes informáticos.

Las acciones adoptadas en relación con la política informática fueron consistentes con la política económica prevaleciente y probaron ser razonablemente exitosas en ese contexto. Sin embargo, el vertiginoso avance de la tecnología y la interdependencia mundial, aunado a importantes cambios en el contexto nacional, dio un nuevo marco a la política informática; diversos factores como la globalización de la economía, la apertura de fronteras al mercado de cómputo, la reorientación de la política y el mercado de

telecomunicaciones, la privatización de los bancos, la desincorporación de empresas paraestatales y la redefinición del papel rector del Estado, dieron como resultado el crecimiento de la informática en nuestro país.

Con base en la información proveniente de distintas encuestas y censos, se ofrece un panorama sobre la situación de la informática en México, dicha situación se maneja en cuatro aspectos fundamentales:

A) *Economía Digital:* Un importante indicador de la creciente participación de la informática en la economía es el Producto Interno Bruto Informático (PIB), el cual creció 27.2% en términos reales en el año 2000 respecto a 1999, esto es 4 veces más que la economía en su conjunto. Con ello el sector informático participa con 3.5% del total de la economía. En cuanto a la balanza comercial de equipo informático, las exportaciones totales sumaron 8,141 millones de dólares (MD) el año pasado, cifra que se compara favorablemente con los 6,399MD que se exportaron en 1999; las importaciones ascendieron a 8,258MD.

B) *Infraestructura Informática:* El parque instalado de computadoras personales (PCS) en México muestra un crecimiento constante. Se estima de manera preliminar que existen 65 equipos por cada mil

habitantes, cifra muy superior a la que se tenía hace 5 años de 26, pero resulta notablemente inferior a la que observan nuestros principales socios comerciales como son Estados Unidos y Canadá con 500 y 260 computadoras por cada mil habitantes, en cada uno de ellos.

C) *Gobierno en línea:* Hoy día, prácticamente todas las Secretarías de Estado cuentan con una página en Internet donde proporcionan información sobre su sector y los servicios que ofrecen a la ciudadanía. De las entidades paraestatales del gobierno, 120 cuentan también con un sitio en Internet, donde presentan información correspondiente a sus atribuciones y ámbitos de competencia. Por su parte, en la totalidad de las entidades federativas, los gobiernos estatales brindan información a través de un sitio electrónico sobre las diferentes actividades económicas de su región, su industria, lugares turísticos más importantes, así como sobre la administración estatal. Actualmente la mayor parte de las dependencias y entidades del Gobierno Federal cuentan con una red para la transmisión de voz y datos (redes institucionales).

D) *Sociedad de la Información:* Los bienes duraderos más frecuentes en las viviendas mexicanas son la televisión y la radio, que están presentes en alrededor del 85% de ellas. Un menor porcentaje dispone de teléfono 36.2% y solamente 9.3% cuenta al menos con una computadora. Dato es altamente indicativo de la existencia de la denominada *Brecha*

Digital, que ha surgido como respuesta al acceso desigual que tienen las personas a las tecnologías de la información, dicha brecha se aprecia al notar que mientras en el Distrito Federal 21.6% de las viviendas poseen computadora, y en las de Baja California, Sonora, Chihuahua, Nuevo León y Jalisco alrededor de 15% disponen de esta tecnología, en el extremo opuesto siete entidades presentan porcentajes inferiores a 5 por ciento. 6

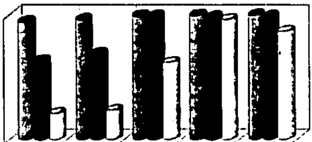
A continuación se mostraran algunos cuadros ilustrativos de los indicadores más importantes a nivel nacional con relación a la informática:

PARQUE INFORMÁTICO DE LA ADMINISTRACIÓN PÚBLICA, 1999 7

Sector	Main Frames	Minis	Workstations	PC's	Total
Central	3	658	1,252	97,471	99,384
Paraestatal	64	2,556	4,771	192,674	200,065
Estatal	9	265	670	64,681	65,625
Total	76	3,479	6,693	354,826	365,074

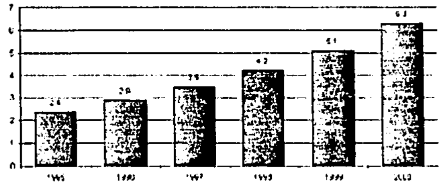
6 "*Situación de la Informática en México*"; INEGI; www.inegi.gob.mx; 2001.
7 "*Encuesta Informática en la Administración Pública Federal y Estatal*"; INEGI; www.inegi.gob.mx; 1999.

ESTABLECIMIENTOS CON EQUIPO INFORMATICO
SEGÚN SECTOR DE ACTIVIDAD ECONOMICA Y TAMAÑO 1998



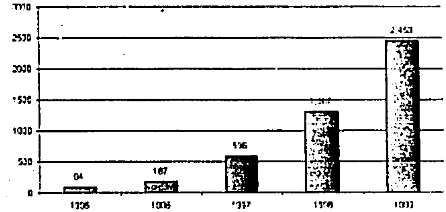
	Servicios	Comercio	Manufacturas	Construcción	Agroindustria
Grandes	[illegible]	[illegible]	[illegible]	[illegible]	100.0%
Medianos	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Pequeños	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

BASE INSTALADA DE PC'S EN MEXICO
millones de unidades



8

USUARIOS DE INTERNET 1995-1999
miles



9

8 *Ídem.*

9 *Ídem.*

1.2 Conceptos fundamentales.

Los conceptos fundamentales, así como los antecedentes, en el presente trabajo son los puntos de referencia esenciales para la adecuada comprensión por parte del lector del presente trabajo de investigación.

En los puntos anteriores se ofreció un breve panorama de la evolución de la informática; la importancia que tiene en México y en el mundo, aportando fechas, eventos trascendentales, datos y cifras relacionadas a ella. En este tema daremos al lector los conceptos necesarios para la comprensión del tema que nos ocupa.

1.2.1 DERECHO.

Etimológicamente la palabra Derecho deriva de la voz latina *directum*, de *diregire*, dirigir, encauzar y que significa lo que esta conforme a la regla, a la norma. Derecho se dice en italiano *Diritto*; en portugués, *Directo*; en romano, *Dreupto*, en francés, *Droit*, en ingles *Right*, en alemán, *Recht*.

La palabra Derecho tiene una multiplicidad de significaciones y sentidos, así podemos decir que al hablar de Derecho se entiende lo que es justo, lo recto, lo que es directo que no es doblado ni corvo, sin desvíos ni vueltas. Es necesario definir al *Derecho*, no como palabra, si no como la ciencia o materia, existen cientos de definiciones, entre las que destacan:

- ***Roma:*** No se estableció una diferencia precisa entre *Derecho* y *Justicia*, así **Celso** definía: "El Derecho es el arte de lo bueno y de lo justo".
- ***Giorgio del Vecchio:*** El *Derecho* es "la coordinación objetiva de las acciones posibles entre varios sujetos, según un principio ético que las determina excluyendo todo impedimento".
- ***Francisco Carnelutti:*** "Un conjunto de leyes que regulan la conducta de los hombres".
- ***Julien Bonnecase:*** "Conjunto de reglas de conducta exterior que, consagradas o no expresamente por la Ley en el sentido genérico del término, aseguran de manera efectiva en un medio dado y en una época dada la armonización de la vida social sobre el fundamento de las aspiraciones colectivas e individuales". *10*

10 Iriarte, Mauricio; El Derecho, definiciones, delimitaciones y aspectos generales: www.chez.com/cmi/definición; 1997.

De esta forma se puede percibir que en las diversas definiciones existen elementos comunes para ellas, por lo que me permito dar una definición propia del Derecho: *Conjunto de normas jurídicas plenamente reconocidas, que regulan las relaciones entre los particulares, entre estos y el Estado, en un momento y lugar determinado, con una fuerza tal, que garantiza la convivencia en un momento y tiempo determinado.*

1.2.2 Derecho Penal

El Derecho penal es el poder punitivo del Estado, constituyendo, desde luego, la expresión más enérgica del poder. Así de esta forma se establecen los delitos y las penas correspondientes, siendo el Estado el regulador de los medios que se requieren para la sana convivencia de la sociedad, imponiendo valores que aseguren la subsistencia y desarrollo del Estado como tal.

Para el presente trabajo de investigación tomaremos en cuenta la definición de **Sáinz Cantero**, que define al *Derecho Penal* como: "el sector del

ordenamiento jurídico que tutela determinados valores fundamentales de la vida comunitaria, regulando la facultad estatal de exigir a los individuos comportarse de acuerdo con las normas y de aplicar penas y medidas de seguridad a quienes contra aquellos valores atenten mediante hechos de una determinada intensidad". *11*

1.2.3 Delito.

Por *Delito* debemos entender: "hecho del hombre que vulnera las condiciones de existencia, de conservación, de desarrollo, de una sociedad en un momento determinado y por el cual se prevé para el sujeto agente como consecuencia, una pena". *12*

Delito: "Delito es el acto u omisión que sancionan las Leyes Penales".

11 González Quintanilla, José Arturo; DERECHO PENAL MEXICANO; México; Editorial Porrúa, 1997, cuarta edición; pp. 17-18.

12 Idem pp. 194.

1.2.4 Derecho Informático.

Existen diversas opiniones en la actualidad en relación a la existencia del *Derecho Informático*, en relación a su existencia o no, pero en una opinión personal es indudable que se encuentra plenamente reconocido, ya que como hemos visto con anterioridad, la informática ha venido a revolucionar todas y cada una de las relaciones humanas; y el *Derecho*, como lo hemos definido, tiene como finalidad regular las relaciones del hombre para su sana convivencia.

Por ello y aunque no existe un concepto claramente difundo, en opinión personal, el *Derecho Informático es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática con la finalidad de regular los problemas jurídicos que se originan por el uso y aplicación de la informática.*

1.3 La problemática de los Delitos Informáticos en la Legislación Penal Mexicana.

Como se ha mostrado en los puntos anteriores, el Derecho tiene la necesidad de regular la conducta del hombre para la convivencia y supervivencia de un Estado; el Derecho Penal es el encargado de tutelar los valores más importantes en una sociedad a través de penas que impidan vulnerar los bienes jurídicos.

En la Legislación Penal Mexicana, no se puede hablar de Delitos Informáticos en estricto sentido, ya que como se manejo anteriormente, delito es el acto u omisión que sancionan las leyes penales; y como se vera a través del presente trabajo, nuestra Legislación no tipifica en estricto sentido algunas de las figuras de los Delitos Informáticos; si no que los relaciona con tipos legales preestablecidos, manejando a estos delitos solo como un medio de comisión de dichas figuras.

Pero este tema va más allá de la Legislación Mexicana; la doctrina internacional establece una gran controversia en relación a la existencia de los

Delitos Informáticos; existen diversas posturas, desde la que afirman que los Delitos Informáticos no existen y que solo son un medio más para cometer ilícitos, y que ya se encuentran todos los bienes jurídicos tutelados, por lo que no es necesario crear un nuevo bien jurídico a tutelar en la Legislación vigente.

Así tenemos dentro de esta teoría a diversos doctrinarios que niegan la autonomía de los Delitos Informáticos, alegando que la computadora solo se utiliza como una nueva forma de perpetrar viejos ilícitos; en esta postura destacan los doctrinarios **Francés Gutiérrez, Taber J. K., Jorge Boumpadre, Alicia Lili y Ricardo Guibourg**.

Otra teoría totalmente opuesta establece la autonomía de los Delitos Informáticos, esta teoría establece una nueva categoría delictual conformada por conductas ilícitas que constituyen una acción antijurídica que encuentra vinculación de determinada manera con un sistema informático; esta postura considera a los delitos por su medio comisivo y no por los bienes jurídicos tutelados, diametralmente opuesta a la teoría anterior, establece una infinidad de conductas que vulneran diversos bienes jurídicos. En esta corriente destaca el jurista **Gustavo Arocena**.

Actualmente ha surgido una tercer teoría que pretende dejar fuera de los Delitos Informáticos a todas aquellas conductas que no estén directamente dirigidas a los datos almacenados y que no constituyan el objeto material del crimen; limitando su concepción a la vulneración de la integridad de los datos o programas informáticos, partiendo del bien jurídico como delimitador de la naturaleza jurídica de este género de delitos. Esta teoría es postulada por **Otto Banhao Links** y **Joao Marcello de Araujo**.

A través de la presente investigación se podrán dar los elementos necesarios para apoyar la postura que comulga con nuestro trabajo, ya que como hemos mencionado con anterioridad, el presente trabajo es partidario de la existencia de los Delitos Informáticos como una categoría autónoma, siendo su contenido limitado, es decir, aceptamos la teoría expuesta en el párrafo anterior, ya que va en función del bien jurídico protegido.

CAPÍTULO II

EL DELITO INFORMÁTICO

CAPÍTULO II

2.1 Definición de Delito Informático.

El *delito informático* implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robo, fraude, falsificación, perjuicio, estafa, sabotaje, etc. A nivel internacional se considera que no existe una definición propia del *delito informático*, por lo que se han formulado conceptos funcionales.

Así tenemos al maestro **Julio Téllez Valdés**, que señala la problemática de definir al Delito Informático ya que su situación es muy especial, ya que no se puede hablar de delitos, en México y en otros países la expresión *"Delitos Informáticos"*, no ha sido objeto de tipificación. Por lo que conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". *13*

13 Téllez Valdés, Julio; Derecho Informático; México, Editorial. Mc Graw Hill, 2ª. Edición, 1996; pp. 103-104.

María de la Luz Lima cita: *Delito Electrónico:* en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. *14*

Para **Carlos Sarzana**, *crimen por computadora* es "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo". *15*

Para el presente trabajo se debe adoptar un concepto propio de delito informático, por que es necesario señalar que en la mayoría de los conceptos señalados en la doctrina (y las teorías señaladas con anterioridad), se presentan grandes diferencias, pero también, elementos en común. A través del desarrollo de la presente investigación encontraremos los elementos que fundamenten el concepto propio de "*delito informático*", por lo que citaremos nuestro concepto en el apartado de conclusiones.

14 Lima de la luz, María; "Delitos Electrónicos" en Criminalia; México, Academia Mexicana de Ciencias Penales; Editorial. Porrúa. No. 1-6. Año L, Enero-Junio 1984; pp.100.
15 Sarzana, Carlo; "Criminalità e tecnologia" en Computers Crime; Rassagna Penitenziaria e Criminologia; Nos. 1-2 Año 1; Roma, Italia; pp.53.

2.2 Figuras comprendidas dentro de los Delitos Informáticos.

Tipos de delitos dados a conocer por las Naciones Unidas: *16*

Fraudes cometidos mediante manipulación de computadoras	Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede accesar a los tipos de registros y programas.
La manipulación de programas	Mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.
Manipulación de los datos de salida	Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de computo.
Fraude efectuado por manipulación informática	Accesando a los programas establecidos en un sistema de información, y manipulándolos para obtener una ganancia monetaria.
Falsificaciones Informáticas	Manipulando información arrojada por una operación de consulta en una base de datos.
Sabotaje informático	Cuando se establece una operación tanto de programas de cómputo, como un suministro de electricidad o cortar líneas telefónicas intencionalmente.
Virus	Programas contenidos en programas que afectan directamente a la máquina que se infecta y causa daños muy graves.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.
Bomba lógica o cronológica	Su funcionamiento es muy simple, es una especie de virus que se programa para que explote en un día determinado causando daños al equipo de cómputo afectado.
Piratas Informáticos	Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de computo y pueden causar graves daños a las empresas.
Acceso no autorizado a Sistemas o Servicios	Penetrar indiscriminadamente en todo lugar sin tener acceso a ese sitio.
Reproducción no autorizada de programas informáticos de protección Legal	Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.

16 "Sobre los Delitos Informáticos"; Organización de las Naciones Unidas; www.delitosinformaticos.com; 2001.

2.3 Características y clasificación de los Delitos Informáticos.

En cuanto a las características de los Delitos Informáticos destacan:

- Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

En cuanto a la clasificación existen diversos criterios entre los que destacan:

Julio Téllez Valdés clasifica a los Delitos Informáticos en base a dos criterios:

- *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.
- *Como medio y objetivo:* en esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. *16*

María de la Luz Lima, presenta la siguiente clasificación:

- *Como método:* conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
- *Como medio:* son conductas criminógenas en donde 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. *17*

16 Ibidem; Téllez Valdés, Julio; pp. 104.

17 Ibidem; Lima de la Luz, María; pp. 102.

2.4 Naturaleza jurídica de los Delitos Informáticos.

Es indudable la existencia de los Delitos Informáticos en la actualidad. Existen diversos criterios dentro de la doctrina para otorgar la naturaleza jurídica de los Delitos Informáticos, en nuestro caso, solo a través de la realización del presente trabajo podremos estar en posibilidad de dar o tomar una posición en relación a ello, lo cual, se dará dentro de las conclusiones del presente trabajo de investigación. Entre las posturas adoptadas con relación a la naturaleza jurídica de los Delitos Informáticos destacan:

A) *Negación de una nueva categoría autónoma:* Esta primera postura rechaza la existencia de la categoría autónoma con entidad propia, de acuerdo a ella: "la ilicitud que involucra a un sistema informático no constituye una nueva categoría delictiva, sino más bien se trata del nacimiento de nuevas formas de perpetrar viejos ilícitos"; es decir se trata de la actualización de los tipos penales tradicionales por medio de conductas nuevas, teniendo como medio las computadoras.

B) *Una nueva categoría autónoma de los Delitos Informáticos:* Esta postura sostiene el nacimiento de una nueva categoría delictual integrada por conductas ilícitas y que constituyen una acción antijurídica que encuentra vinculación de determinada manera con un sistema informático. Se pugna por la elaboración de una nueva teoría del delito informático; "que enmarque a la delictuosidad informática como una realidad delictiva autónoma, de imposible solución en las figuras tradicionales típicas".

C) *Limitación de los Delitos Informáticos:* Esta teoría pretende limitar a los Delitos Informáticos, en un marco que deje fuera de él a todas aquellas conductas que no estén directamente ligadas a los datos almacenados y en las que éstos no constituyan el objeto material del crimen; no podrán considerarse como Delitos Informáticos las conductas que solo utilicen a las computadoras como medio comisivo si no atacan directamente a los datos o programas almacenados en ellas.

2.5 Problemática internacional y organizaciones

En la actualidad el uso de la computadora ha llegado a ser indispensable, las empresas utilizan con más frecuencia las computadoras para manejar y almacenar su información, esto les trae muchos beneficios, pero también las hace un blanco perfecto para los Delitos Informáticos.

El informe del Pentágono, *"White paper on information infraestructure assurance" ("Documento blanco sobre la seguridad de la infraestructura de información")*, lo confirma: "el sistema telefónico, los bancos, la Reserva Federal, la distribución de electricidad y combustible, el control del tráfico aéreo y otros sistemas inteligentes de transporte, la sanidad pública, las fuerzas de la ley e incluso el sistema de las elecciones dependen totalmente de las redes". Sólo en Estados Unidos, los daños por ataque vía Internet a las empresas, que casi nunca se denuncian, ascendieron en 1995 a 5,000 millones de dólares. **John McConnell**, director del NSA (Agencia Nacional de Seguridad), dijo: "Somos la nación más vulnerable de la Tierra". *18*

18 Zambrano L, Rene; Crimen y Castigo en el ciberespacio; www.skyscraper.fortunicity.com/472; 2001.

Según estimaciones del servicio *Compuserve* el 60% de las comunicaciones entre proveedores y distribuidores de estupefacientes se realizan a través de *la red.* Pero el delito por computadora de mayor incidencia es la piratería de software.

Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Hay un número no despreciable de personas poco honestas en las redes: fisgones que quieren curiosear, morbosos que buscan violentar los sistemas; espías industriales y ladrones digitales. A todos estos se los ha englobado bajo la denominación de *hackers*, pero existen matizaciones. El término (que en castellano significa *cortador*) se suele aplicar a las intrusiones no dañinas, provocadas normalmente por simples fisgones que quieren probar que se puede violar un sistema de seguridad. Para las acciones nocivas existe la más contundente expresión *Cracker* (*rompedor*). Las acciones de los *crackers* pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender, denominado "robo económico".

Las familias de piratas navegan en barcos distintos. Incluso utilizan en los mensajes entre ellos "jergas" diferentes. Para referirse a la piratería, los

norteamericanos distinguen entre "*chicos buenos*" y "*chicos malos*". Los chicos buenos buscan los agujeros de seguridad en los sistemas (una línea mal escrita entre las miles que forman los programas) y avisan del fallo a las empresas.

Las medidas de seguridad se han creado para proteger nuestra intimidad y otros derechos individuales. Sin embargo, en ocasiones estos procedimientos de seguridad amenazan dichos derechos. Los estándares de seguridad y libertad de las computadoras generan importantes problemas de carácter jurídico, legal y ético.

2.5.1 Organización para la Cooperación Económica y el Desarrollo (OCDE).

El primer esfuerzo internacional para tratar la problemática de los Delitos Informáticos se da en la **OCDE**; en 1983 encargó a un grupo de expertos el estudio de la posibilidad de una armonización internacional para que las leyes

penales pudieran hacer frente a los Delitos Informáticos. En 1985 se dio la recomendación a los Estados miembros extender sus leyes penales para penalizar a quien dolosamente cometa actos de abuso en el campo de las computadoras.

En 1986, la **OCDE** publicó un estudio llamado *"Delitos Relacionados con las Computadoras: Análisis de la Política Legal"*. Del análisis de las leyes existentes, se recomendó a los Estados miembros tipificar una lista mínima de conductas, relacionadas con el abuso de las computadoras; estas conductas mínimas son:

- El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos con la intención de transferir ilegalmente fondos u otras cosas de valor.
- El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos con la intención de falsificar documentos.
- El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos, o cualquier otra interferencia con equipos informáticos con la intención de impedir el funcionamiento de equipos informáticos o de telecomunicaciones.

- La infracción a los derechos exclusivos del propietario de programas informáticos protegidos, con la intención de explotar comercialmente el programa y ponerlo en el mercado.
- El acceso o intercepción a equipos de computo o de telecomunicaciones a sabiendas y sin autorización de la persona responsable del sistema, ya sea por la infracción de medidas de seguridad o por cualquier otra intención deshonesta o dañosa. *19*

El 24 de noviembre de 1992, los Estados miembros de la **OCDE** adoptaron los *"Lineamientos Guía para la Seguridad en los Sistemas Informáticos"*; sobre las sanciones que deben adoptarse los lineamientos establecen:

> Las sanciones por abuso sobre sistemas de informática son un medio importante en la protección de los intereses de aquéllos que tienen confianza en los mismos, respecto de los daños que puedan resultar de los ataques a la disponibilidad, confidencialidad e integridad de los sistemas de información y de sus componentes. Ejemplos de esos ataques incluyen daños o interrupciones a los sistemas informáticos por la introducción de virus, alteraciones a los datos computarizados, acceso ilegal, fraude o falsificación por computadora y reproducción ilegal de programas informáticos. En el combate a tales peligros, los Estados han escogido responder a estos actos en diversas formas. *Existe un creciente consenso internacional de que estos abusos a las computadoras deberían ser cubiertos por las leyes penales internacionales.* *20*

19 ONU; Manual de prevención y control relacionada con el crimen informático; Nos. 43 y 44, s. F.; pp. 25.

20 OCDE; "Lineamientos para la Seguridad de los Sistemas de Información"; 1992; pp.20.

2.5.2 Organización de las Naciones Unidas (ONU).

En el Octavo Congreso de las **Naciones Unidas** sobre la *Prevención del Crimen y Tratamiento de los Delincuentes* se publicó un documento titulado "*Revisión Internacional de la Política Criminal, Manual de las Naciones Unidas sobre la Prevención y Control del Crimen relacionado con Computadoras*". En dicho manual están reconocidas las siguientes conductas:

- *Fraude por manipulación*: debido a que en la actualidad los negocios están remplazando las operaciones en efectivo por depósitos en sistemas informáticos.
- *Falsificación informática*: es la alteración de datos de documentos almacenados en la computadora, así como el uso de la computadora como instrumento para cometer el delito de falsificación.
- *Daños o modificaciones a datos computarizados o a programas informáticos*: incluye el acceso de virus o de bombas lógicas; también conocido como sabotaje informático.
- *Acceso no autorizado a sistemas informáticos y servicios*: a través de él se da la oportunidad de causar daños adicionales o impedir el uso a los legítimos propietarios.

- Reproducción no autorizada de programas protegidos legalmente: esta conducta esta plenamente reconocida a nivel mundial. 21

2.5.3 Asociación Internacional de Derecho Penal.

En octubre de 1992, después de la reunión en *Würzbur*, se elaboro un proyecto de recomendaciones con base a los Delitos Informáticos, destacan:

- Para evitarse la excesiva criminalización debe considerase el alcance y ampliación de los tipos penales en esta área, la cual requiere un cuidadoso examen y justificación, primordialmente a la intencionalidad.
- Se recomienda que los Estados, de acuerdo a su tradición y leyes, tipifiquen como delito a las conductas descritas en la lista opcional (**ONU**).

21 Ibidem; ONU; pp. 14.

En septiembre de 1994, se celebra el *XV Congreso Internacional de Derecho Penal* en Río de Janeiro, él cual recoge los avances de las distintas organizaciones; dentro de las recomendaciones emitidas, tenemos:

- El abuso de la tecnología informática afecta tanto a los intereses de carácter económico así como los orientados hacia la intimidad.
- El desarrollo de la tecnología informática exterioriza la emergencia de nuevos tipos de intereses que requieren protección legal.
- En la medida que el Derecho Penal es insuficiente, debe respaldarse la modificación de la Legislación existente o la definición de nuevos delitos.
- Es importante proteger los intereses de la intimidad contra los cambios que provoca la tecnología informática.

Es de gran importancia este Congreso por que por ves primera se trata el problema del crimen informático con criterios jurídicos basados en el bien jurídico que se vulnera; tanto lo económico como la intimidad y nuevos tipos de intereses, como la integridad y disponibilidad exclusiva de ciertos datos.

2.6 Derecho Comparado.

A nivel internacional, Latinoamérica tiene un atraso legislativo en materia de Delitos Informáticos, las respectivas legislaciones penales no han introducido en ellas el concepto y la tutela necesaria para la prevención y erradicación de este problema. Chile, Argentina y tal vez México son los países que han tenido una mayor actividad legislativa en este respecto, pero muy lejos de países como Estados Unidos, Alemania y Francia.

Estados Unidos

Uno de los mayores avances legislativos en Estados Unidos, se da en 1994, con el *Acta Federal de Abuso Computacional* (*18 U.S.C. Sec.1030*) que modificó al *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, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa,

información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 distingue el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles:

a) Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus, sino describiendo el acto para dar cabida en un futuro a la nueva era de los ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen, subrayando el carácter que se lo otorga a los mismos en su aspecto doloso o no.

Asimismo, 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.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente.

Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de Delitos Informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas y que utilizan legalmente esas computadoras, sistemas y bases de datos.

Asimismo, 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.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente.

Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de Delitos Informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas y que utilizan legalmente esas computadoras, sistemas y bases de datos.

Francia

Este país contiene una legislación en materia penal informática que data de tiempo atrás, ya que, la *Ley número 88-19* es del 5 de enero de 1988, de la cual, se resalta:

El fraude informático: acceso fraudulento a un sistema de elaboración de datos (462-2): en este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje informático (462-3): en este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4): en este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o

modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5): en este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6): en este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la Legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (*sabotaje*).

ESPAÑA

En España el problema de los Delitos Informáticos a tenido gran tarea legislativa, la solución fue dada con la expedición del Nuevo Código Penal Español de 1995, ya que en este, se agrego al delito tradicional de estafa (Art. 248 num.1) un párrafo donde se incluye el fraude informático (Art. 248 num. 2), el cual viene a superar los inconvenientes señalados por la doctrina en cuanto a la imposibilidad de aplicar la estafa tradicional, ya que en el caso, no concurre el engaño sobre una persona sino sobre una máquina. Este es uno de los casos en que el legislador ha optado por la introducción de un tipo específico, que, en cumplimiento del principio de legalidad del Derecho Penal, viene a regir esta nueva forma de delincuencia.

En el Nuevo Código Penal de España, el art. 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2 establece que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

CAPÍTULO III

LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL MEXICANA

CAPÍTULO III

3.1 Aclaración previa.

En el presente Capítulo se analizaran las figuras afines en la Legislación Penal Mexicana, ya que como se señalo en el capítulo primero, si bien es cierto que no se puede hablar propiamente de Delitos Informáticos, existen figuras jurídicas descritas como tales.

Se analizaran las figuras comprendidas por el Manual de las Naciones Unidas sobre la Prevención y Control del Crimen Relacionado con Computadoras:

- Fraude informático.
- Falsificación informática.
- Daños o modificaciones a datos computarizados o a programas informáticos.
- Acceso no autorizado a sistemas informáticos y servicios.
- Reproducción no autorizada de programas protegidos legalmente.

3.2 Fraude Informático.

Por fraude informático debemos entender "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero". 22

Se trata de una conducta directamente relacionada con la manipulación de datos almacenados en una computadora, provocando la transferencia de datos o valores en perjuicio de un tercero y a favor de otro. La problemática de este delito es saber a quien se realiza el engaño, numerosos analistas sostienen que la estafa se realiza a la máquina; nuestro código, solo establece los conceptos de estafa y engaño de hombre a hombre, debido a que los legisladores no se han planteado los retos de la revolución.

22 Acuario Del Pino, Santiago; El fraude y los daños informáticos; www.delitosinformáticos.com/trabajos; 2001.

Algunos autores norteamericanos consideran que la introducción de datos falsos en una computadora equivale al engaño sobre un humano. Ya que el uso actual de los sistemas computarizados, encargados de ejecutar transacciones directamente, la equiparación de engaño a un ser humano y a una máquina es necesaria y conceptualmente justificada para asegurar la represión penal del fraude moderno. No hay diferencia ni de facto ni legal, entre engaño utilizado para apoderarse de propiedad ajena a través de una máquina y aquél dirigido a la persona con idéntica intención.

Conforme a lo anterior la figura del fraude informático encuadraría en el fraude; pero en la realidad jurídica de nuestro país no es así, toda vez que nuestra legislación requiere que el sujeto pasivo se engañado o se encuentre bajo error, de conformidad con el artículo 386 del **CPDF**:

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

Es erróneo pensar en el engaño a la máquina, en virtud de lo siguiente:

- *"Engañar"*, uno de los verbos rectores del fraude, de acuerdo al Diccionario de la Real Academia Española significa: dar a la mentira apariencia de verdad o inducir a otro a tener pór cierto lo que no lo es, valiéndose de palabras o de obras aparentes y fingidas. Por lo quien sufre el engaño es necesariamente una persona, pues sólo ésta puede apreciar los hechos, sean verdaderos o no.
- La sola manipulación de datos en un sistema informático no implica la variación patrimonial de quien con ello se vea perjudicado. Se requerirá además que se realice la transacción de los fondos transferidos, para que con ello quien lo haga, sufra un beneficio en su patrimonio.
- La máquina solo es el instrumento por medio del cual se logra engañar a una persona.

Por lo que se puede considerar que la transacción de una suma de dinero, producto de una transferencia ilícita de fondos por medio de equipos computacionales, encuadra en el tipo penal del fraude genérico pues esta conducta implicaría un engaño al titular del sistema, que es el titular del bien jurídico protegido. Es decir, el pago se efectuaría en virtud del engaño que se ha hecho al titular del sistema, pues de conocer éste la naturaleza ilícita de la transferencia, no habría realizado el pago.

Elementos objetivos:

- *Sujeto activo:* el que modifica los datos integrados en la computadora y obtiene un lucro indebido o se hace ilícitamente de una cosa.
- *Sujeto pasivo:* el titular del sistema que inducido al error por la manipulación de los datos, sufre una lesión en su patrimonio.
- *Bien jurídico tutelado*: patrimonio.
- *Acción*: Provocación del engaño mediante la manipulación de información.
- *Resultado*: Se hace ilícitamente de una cosa u obtiene un lucro indebido, por lo que la sola manipulación de datos constituiría tentativa de fraude, hasta en tanto no se dé este resultado.
- *Nexo causal*: El engaño causado mediante la manipulación informática conduce al pago indebido de dinero o de valores.

Elemento subjetivo:

- *Dolo*: La manipulación de los datos contenidos en la computadora se hace con el objeto de inducir al error al titular de la misma, y con ello obtener un lucro indebido o hacerse ilícitamente de una cosa.

Aparentemente el único elemento distintivo entre el fraude genérico y el fraude informático, es el medio comisivo. Ya que las máquinas no pueden incurrir en un error, las personas son las que han dado instrucciones para realizar una acción ilícita, con la finalidad de obtener un lucro.

Así, después del análisis presentado, tenemos que el fraude informático, aparentemente se encuentra tutelado por el artículo 386 del **CPDF**; pero cabe señalar que esta tutela esta totalmente dependiente a esta figura (fraude genérico), ya que como tal, no contempla al fraude informático y deja grandes lagunas para su tipificación, y por ende su penalidad.

Por todo lo anterior, se concluirá que el delito de fraude informático, si bien es cierto se encuentra tutelado en nuestra Legislación, no esta contemplado como un delito informático, y por ende no puede tutelar y proteger de una forma tal, que contemple la "evolución", que ha sufrido el fraude, al contemplar en él, nuevas conductas y mayores problemáticas para su adecuada prevención y tutela.

3.3 Falsificación Informática.

Por este Delito Informático, debemos de entender el ingreso, alteración o supresión de datos computarizados o de programas informáticos, o cualquier otra interferencia durante el procesamiento de datos realizada de tal forma o bajo condiciones tales que constituyen un delito de falsificación, cuando sea cometido respecto de un objeto tradicional de tal delito.

La modificación o alteración de los datos almacenados en una computadora, es la parte medular del análisis que se hará en este apartado, analizando si efectivamente esta conducta puede considerarse como falsificación en nuestra legislación.

El análisis se referirá únicamente a la falsificación material, que consiste en la alteración de un documento que ya existe, sin analizar a la falsificación ideológica, que no requiere de un documento previo que haya de modificarse,

sino que se configura por conductas tendientes a falsear la veracidad de los hechos, por ejemplo atribuyéndose un nombre o investidura que no se tenga (art. 244, fracción V del **CPDF**), o redactando un documento en términos distintos a los convenidos (art. 244, fracción VI del **CPDF**).

En la doctrina existe gran controversia en si debe o no considerarse a esta conducta como falsificación, o si es uno de los actos que conforman la realización de otro delito, por ejemplo el fraude.

El **CPDF** señala en su art. 244:

El delito de falsificación de documentos se comete por alguno de los medios siguientes:

I.- Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera;
II.- Aprovechando indebidamente una firma o rúbrica en blanco ajena, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, o causar un perjuicio a la sociedad, al Estado o a un tercero;
III.- Alterando el contexto de un documento verdadero, después de concluido y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto substancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación;
IV.- Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento;
VII.- Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, si el documento en que se asientan, se extendiere para hacerlos constar y como prueba de ellos;
VIII.- Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una variación substancia, y
IX.- Alterando un perito traductor o paleógrafo el contenido de un documento, al traducirlo o descifrarlo.

X.- Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente.

La cuestión principal consiste en dilucidar si puede considerarse como documento a los datos almacenados en un sistema informático, y si la alteración de este documento encuadraría en alguna de las figuras previstas por el artículo antes señalado.

Arteaga Sánchez señala: "¿puede decirse que en los casos reseñados los datos en informaciones que procesa la computadora son documentos, a los efectos del delito de falsedad? La respuesta parece negativa, un documento exige, entre otras cosas, su carácter escrito y la posibilidad de apreciación o captación de su sentido por el hombre. Pero ¿puede decirse que un dato en una cinta o disco magnético o en pantalla es un documento y es apreciable como tal para el ser humano?... por lo menos a nivel del *input* y del tratamiento pareciera que no se puede hablar de un documento, lo que sí podría admitirse cuando el *output* se materializa en la forma de un impreso legible". *23*

23 Arteaga Sánchez, Alberto; "El Delito Informático, algunas consideraciones jurídico-penales: Venezuela; Revista de la Facultad de Ciencias Jurídico Penales; año XXXIII; No. 68, pp. 130.

En su acepción literal se considera documento, según el Diccionario de la Real Academia al escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo. En un sentido jurídico, en la doctrina se ha considerado que por documentos solo deben entenderse aquéllos que son escritos.

En este sentido **Becerra Bautista** señala que "los documentos a que nos referimos deben ser escritos, para distinguirlos de aquellas cosas que sirven también para reproducir acontecimientos por otros procedimientos como los son la fotografía, la cinematografía, la fonografía, etc." [24]

Para **Carrancá y Trujillo y Carrancá y Rivas**, documento es todo género escrito; éste es el sentido de nuestro texto legal... sin escrito no hay documento. [25]

24 Becerra Bautista, José; El Proceso Civil en México; México; Editorial Porrúa, Ed. 14ª; pp. 144.

25 Carrancá y Trujillo Raúl, y Carrancá y Rivas, Raúl; Código Penal Anotado; México; Editorial. Porrúa; Ed. 18ª; pp. 643.

Si bien es cierto que muchos de los datos almacenados en una computadora son datos escritos, esto no les otorga el carácter de documento, piénsese por ejemplo en un escrito almacenado en un disco, el disco no podría considerarse como documento sino como un medio de almacenamiento de datos para ser reproducido en un sistema informático, que puede darle, una vez impreso, la calidad de documento. Sin embargo, este es aun un campo poco aclarado para la doctrina.

Además existe un elemento adicional que difícilmente podría probarse respecto de los datos almacenados en una computadora: *la autenticidad.* Como se desprende del art. 244 del **CPDF**, los documentos que sean objeto de falsificación tienen elementos que permiten denotar su autenticidad, por ejemplo firmas o rúbricas.

En este sentido la Primera Sala de la Suprema Corte de Justicia de la Nación ha considerado que:

Falsificación de documentos: La tutela penal por lo que hace al tipo de falsificación de documentos, radica en la necesidad de ***proteger eficazmente***

***la veracidad de los documentos públicos y privados, a los que la generalidad reconoce valor probatorio más o menos firme**, por no dudarse de su autenticidad literal.* 26

Por todo lo anterior concluimos que no puede hablarse en estricto sentido de documentos, para los efectos de la tutela penal, sino hasta que éstos adquieren forma impresa. El ingreso o alteración de datos almacenados en una computadora que den como resultado la impresión de un documento falso pueden considerarse como parte de los actos tendientes a la comisión del delito de falsificación, el cual se agotará una vez impreso el documento y que concurran los requisitos previstos por el artículo 245 del **CPDF**.

Como puede apreciarse, en nuestra Legislación la modificación de datos computarizados, por lo que hace a la falsificación, no es punible *per se*, si como tentativa del delito de falsificación. Solo será sancionado si forma parte de los actos que den como resultado la falsificación de un documento escrito, no de la alteración como tal.

26 Amparo directo 1430/52. Pelefrin J. Castro. 21 de abril de 1958. Unanimidad de 4 votos. Ponente: Luis Chico.

3.4 Daños o modificaciones a datos computarizados o a programas informáticos.

Será materia de este apartado sólo aquellas conductas que ataquen directamente al *software*, que constituye la estructura lógica que permite a la computadora la ejecución del trabajo que se ha de realizar, es decir, el equipo lógico informático.

Siguiendo el Manual de las Naciones Unidas, caben dos tipos de conductas:

- *Daños a datos computarizados o a programas informáticos.* El daño, deterioro o supresión de datos computarizados o programas informáticos sin derecho a hacerlo.
- *Sabotaje informático.* El ingreso, alteración o supresión de datos computarizados o programas informáticos, o cualquier otra interferencia en los sistemas informáticos con la intención de impedir el funcionamiento del sistema informático o de telecomunicaciones.

En el primer supuesto se encuentran todas aquellas conductas dirigidas a la modificación, alteración o daño de los datos almacenados o de los programas, entre ellos los virus, que consisten en pequeños programas que introducidos súbitamente en una computadora, poseen la capacidad de auto reproducirse sobre cualquier soporte apropiado que tenga acceso al ordenador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar; además de reproducirse, llevan en su código ciertas instrucciones para actuar en un momento predeterminado, ya sea sólo mostrando mensajes en la pantalla o deliberadamente destruyendo información contenida en los soportes físicos, aun a ellos mismos, en algunos casos.

Dependiendo de la forma en que se presenten estas conductas, lo cierto es que están orientadas a variar el estado en que se encuentra el soporte lógico, lo que podría considerarse como daño.

Por ello, tanto las modificaciones a los datos como el sabotaje quedan comprendidos dentro del tipo de daño en propiedad ajena, previsto por el art. 399 del **CPDF**, si estas conductas traen por consecuencia una lesión al patrimonio:

"Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple".

Del artículo citado se desprende que el daño se realice a una *cosa*. A este respecto se señala que solo los bienes tangibles deben considerarse como *cosa*. **Vincenzo Manzini** opina que por cosa se entiende un "objeto corporal susceptible de tener un valor, el cual no debe ser necesariamente económico, pudiendo ser documental o meramente moral o afectivo". *27*

Algunos autores sostienen que este tipo de conductas pueden encuadrarse dentro del tipo de daños (**Gustavo Arocena** o **Alberto Arteaga Sánchez**), sin embargo otros autores consideran un error el querer dar a este tipo de conductas el mismo tratamiento de aquellas que van dirigidas a los bienes tangibles. **Otto Banho Licks** señala: "el inconveniente de muchas Legislaciones que han aparecido consiste en el hecho de tratar a estas nuevas conductas pertenecientes al medio tecnológico de procesamiento digital de datos a la computarización de la sociedad con los mismos principios legales aplicables a los delitos de bienes tangibles o corporales la cuestión principal de las leyes

27 Ibidem; Carrancá y Trujillo Raúl, y Carrancá y Rivas, Raúl; pp. 1180.

penales informáticas respecto de los sistemas informáticos es la necesidad de proteger sus componentes inmateriales, es decir, el software y los datos, que aun carecen de la misma protección que tiene el hardware".

Debe señalarse que haciendo un análisis del objeto que se tutela este consiste finalmente en un bien tangible. En la alteración a los datos almacenados en una computadora, el bien tangible (un disco magnético o chip), es distinto al que existía antes de la modificación, ya que varió su contenido, y en relación con los programas informáticos ya que se ha alterado el chip, disco magnético o a todo el equipo informático, de tal forma que el mismo ya no tiene la capacidad de realizar ciertas funciones que tenía antes de la alteración.

Por lo que hace a la alteración o supresión de datos computarizados o a programas informáticos que no necesariamente son efectuados con el propósito de impedir el funcionamiento del sistema, se aplicaría de igual forma el tipo de daño en propiedad ajena, si esta conducta trae por consecuencia un daño, pues el tipo no requiere el elemento subjetivo del dolo.

Por ultimo, es discutible si cualquier modificación o alteración a la información almacenada en una computadora puede considerarse como daño, es preciso para agotar el tipo descrito, que se afecte al bien jurídico protegido, es decir, que el titular sufra una lesión en su patrimonio, pero ¿la modificación de un texto o archivo almacenado en una computadora puede considerarse como lesión patrimonial?.

A este respecto la Primera Sala de la Suprema Corte de Justicia de la Nación ha considerado que "el daño puede ser cuantitativo y cualitativo, puede recaer por tanto, quitando algo material al objeto o aminorando su valor, sus fines, su esencia, cambiándola, y por último daño es la destrucción, pues afecta totalmente el patrimonio del sujeto pasivo, tenga un valor de cambio o puramente estimativo.....". [28] Siguiendo esta descripción, el solo cambio del bien puede entenderse como daño.

28 Amparo penal en revisión 4391/50. Pérez Ruiz Pablo. 28 de septiembre de 1950. Mayoría de cuatro votos. Seminario Judicial de la Federación, Quinta Época, parte CV, pp. 2577.

Sabotaje Informático, en este segundo supuesto, nos referiremos solo al que va dirigido a impedir el funcionamiento de sistemas de telecomunicaciones, respecto del cual puede decirse que nuestra Legislación otorga la protección, independientemente de que el medio comisivo de las conductas descritas sea un medio informático o cualquier otro.

Así tenemos al art. 167 del **CPDF**, que señala en su párrafo sexto:

Se impondrá de uno a cinco años de prisión y multa de quinientos a cincuenta mil pesos:

VI.- Al que interrumpiere la comunicación telegráfica o telefónica, alámbrica o inalámbrica, o el servicio de producción o transmisión de alumbrado, gas o energía eléctrica, destruyendo o deteriorando uno o más postes o aisladores, el alambre, una máquina o aparato de un telégrafo, de un teléfono, de una instalación de producción, o de una línea de transmisión de energía eléctrica;

El art. 533 de la **LVGC**, señala:

Los que dañen, perjudiquen o destruyan las vías generales de comunicación, o los medios de transporte, o interrumpan la construcción de dichas vías, o total o parcialmente interrumpan o deterioren los servicios que operen en las vías generales de comunicación o los medios de transporte, serán castigados con tres meses a siete años de prisión y multa de 100 a 500 veces el salario mínimo general, vigente en el área geográfica del Distrito Federal.

Para el debido entendimiento de los anteriores artículos es necesario precisar el concepto legal de *vías de comunicación*, él cual, para la **LVGC** son tan solo las rutas del servicio postal; por lo cual debemos remitirnos a la **LFT**, la cual, en su artículo cuarto, con relación al tercero, nos da el concepto jurídico buscado, así tenemos:

Art. 4 Para los efectos de esta ley, son vías generales de comunicación el espectro radioeléctrico, las redes de telecomunicaciones y los sistemas de comunicación vía satélite.

Art. 3. Para los efectos de esta ley se entenderá por:

II. Espectro radioeléctrico: el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz;

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

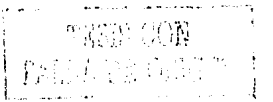
XIII. Sistema de comunicación vía satélite: el que permite el envió de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envía de regreso a la tierra para ser captadas por estación receptora, y

XIV. Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

A través de los artículos antes mencionados, notamos que no se exige un medio comisivo determinado, por lo que la realización de tales conductas, por medios informáticos, (por supuesto a través de cualquier medio), será punible de conformidad con los mismos.

Por lo que podemos concluir en este apartado que el daño, deterioro o supresión de datos computarizados o programas informáticos sin derecho de hacerlo, así como el ingreso, alteración o supresión de datos computarizados o programas informáticos, o cualquier otra interferencia en los sistemas informáticos con la intención de impedir el funcionamiento del sistema informático o de telecomunicaciones, son conductas que ya se encuentran cubiertas por los tipos penales de nuestro sistema jurídico.

Es necesario precisar que para muchos autores la cuestión principal en este tipo de delitos, es la acción causante de los daños, la cual indudablemente reside en el acceso no autorizado; el punto central de su peligrosidad no es su carácter, definición o constitución; sino el acceder o ingresar sin autorización a un sistema que no se encuentra preparado para ello.



3.5 Acceso no autorizado a sistemas informáticos y servicios.

La introducción sin autorización a un sistema informático, puede tener un sinnúmero de objetivos y ser realizado a través de diversas conductas, desde la curiosidad, hasta la realización de diversas conductas delictivas.

La criminalidad informática se ha manifestado de forma alarmante en nuestros días, la aparición de los denominados hackers, esa persona que intercepta en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, conocer, difundir o hacer uso de la información que se encuentre almacenada en los sistemas de cómputos perteneciente a organizaciones con o sin fines de lucro y de diversa índole.

La presencia de la informática en las telecomunicaciones, es innegable, y la importancia de ellas en la vida diaria es vital. Por ello en el presente apartado debemos distinguir tres conductas:

- Acceso no autorizado al sistema informático
- Acceso no autorizado a un servicio (llamado robo de tiempo)
- Sustracción de información.

3.5.1 Acceso no autorizado al sistema informático.

Aquí debemos distinguir dos situaciones distintas, el acceso no autorizado al sistema informático, y el acceso no autorizado a determinada información.

En cuanto al acceso no autorizado al sistema informático, éste podría encuadrar dentro del tipo previsto por el art. 380 del CPDF:

Art. 380: Al que se le imputare el hecho de haber tomado una cosa ajena sin consentimiento del dueño o legítimo poseedor y acredite haberla tomado con carácter temporal y no para apropiársela o venderla, se le aplicarán de uno a seis meses de prisión o de 30 a 90 días multa, siempre que justifique no haberse negado a devolverla, si se le requirió a ello. Además, pagará al ofendido, como reparación del daño, el doble del alquiler, arrendamiento o intereses de la cosa usada.

Esta equiparación es conocida en la doctrina como robo de uso o apropiación indebida con carácter temporal y no requiere para su agotamiento el ánimo de apropiación de la cosa. La conducta, desde este punto de vista atentaría en contra del bien jurídico del patrimonio.

El acceso no autorizado a determinada información podría encuadrarse al artículo 380 del **CPDF**, si el equipo informático no es propio del que accesa, si no esta autorizado para usarlo, o habiendo sido autorizado para ello, su uso vaya más allá del autorizado, pues independientemente de la información a la que se accede, no es lícito el uso del equipo informático.

Sin embargo, cuando el equipo informático es propio del que accesa a la información o éste está autorizado para usarlo, el tratamiento jurídico será distinto. No se vulnera ya, en términos de nuestra legislación, al patrimonio, sino a la información, que como tal no esta protegida salvo pocas excepciones.

En materia de propiedad intelectual la **LFDA**, en su Capítulo IV "De los Programas de Computación y las Bases de Datos", establece algunas de las disposiciones respecto de los datos o informaciones contenidas en bancos de datos.

Art. 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el articulo anterior, así como la publicación, reproducción, divulgación, comunicación publica y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Este artículo protege el acceso a la información pero tan solo aquella que posee el carácter de *privado*, siendo un concepto limitado y ambiguo por lo indeterminado del concepto "de carácter privado de las personas", y con la imposición de una multa.

El **CPDF** tutela y tipifica este tipo de conductas, si bien no a la información en general, si aquella contenida en comunicaciones:

Art. 173: Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad:

I.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y
II.- Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.
Los delitos previstos en este artículo se perseguirán por querella.

Art. 177: A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

De manera preventiva al acceso, pero no como protección del acceso en sí mismo, el artículo 424 bis del **CPF** fracción II, sanciona de tres a diez años de prisión y de dos a mil a veinte mil días de multa: "a quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación", dentro de los que pueden incluirse a aquellos dispositivos tendientes a evitar intromisiones no autorizadas.

Las disposiciones mencionadas, como ya se ha visto solo protegen la información de carácter privado relativa a las personas o a la información contenida en las comunicaciones, no encontramos disposición alguna que brinde la adecuada protección respecto del acceso no autorizado a información almacenada en equipos informáticos, por lo que concluimos que esta conducta, en nuestro derecho es muy limitada.

3.5.2 Acceso no autorizado a servicios

Independientemente de que el equipo informático sea usado con o sin autorización, nos encontramos en el supuesto de que a través del equipo informático se logra la obtención de un servicio informático sin el correspondiente pago. Nos referimos a las relaciones contractuales que pueden tener lugar a través de los medios informáticos, aquellas situaciones en las que se logra la prestación de un servicio informático a través de manipulaciones informáticas, por ejemplo los servidores de red, servicios de consulta o noticias, o paginas de Internet que requieren de un pago.

Esta conducta podía encuadrar en el tipo previsto por el art. 386, fracción II del **CPDF**:

Art. 368. Se equiparan al robo y se castigarán como tal:

II.- El aprovechamiento de energía eléctrica o de cualquier otro fluido, ejecutado sin derecho y sin consentimiento de la persona que legalmente pueda disponer de él.

A este respecto señala **Carrancá y Trujillo y Carrancá y Rivas**: "por no constituir el fluido eléctrico una cosa *strico sensu*, ya que carece de corporeidad y sólo existe como propiedad de la materia o estado transmisible

de la misma, no puede, en rigor, ser objeto material del delito de robo. Pero su aprovechamiento o consumo al igual que de cualquier otro fluido aprovechable como satisfactor de necesidades, y cuya producción representa la incorporación de un costo económico, está equiparado al robo por la ley penal, a los efectos de la tutela patrimonial correspondiente". 29

Efectivamente, si bien no podemos hablar en estricto sentido de robo, el Legislador a otorgado la protección al patrimonio de quien provee este fluido y que no puede ser sujeto pasivo del robo, por lo que esta figura de delito informático encuentra eficaz protección en nuestras leyes penales, a través del llamado "*robo de fluido*".

El artículo 426 fracción II del **CPF**, protege las señales de satélite:

Art. 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

29 Idem; pp. 910-911.

Si bien es cierto que el anterior se ubica dentro de los delitos en materia de derechos de autor, el bien jurídico tutelado es el patrimonio del titular de la señal. A diferencia del *robo de fluido*, además de la especificidad del objeto material de protección (señal de satélite), la protección es mucho más amplia, ya que este tipo sanciona cualquier acto con la finalidad de descifrar.

Como protección accesoria, no de la conducta en sí, sino como medio preventivo a su comisión la fracción I establece: "a quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal".

3.5.3 Sustracción de información

No será tema de este apartado la sustracción de los medios de almacenamiento o reproducción de la información, como discos o documentos escritos, en cuyo caso se configuraría el robo. El tema a tratar, se limita a tratar de determinar si nuestro derecho protege la sustracción de la información en sí misma, que puede lograrse con el solo acceso a una base de datos.

Es preciso analizar si esta conducta esta prevista por el delito de robo previsto por el artículo 367 del **CPDF**:

Art. 367. Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.

Las interrogantes son ¿puede considerarse como *cosa* mueble la información almacenada en los sistemas informáticos?, ¿Y si puede ser susceptible de apropiación?.

La doctrina señala el término cosa como "un objeto corporal susceptible de tener un valor, el cual no debe ser necesariamente económico, pudiendo ser documental o meramente moral o afectivo".

El término mueble es un elemento normativo, que exige para la debida integración del tipo penal de robo acudir a las normas que prevean tal concepto, esto nos remite al **CCDF**:

Artículo 752.- Los bienes son muebles por su naturaleza o por disposición de la ley.
Artículo 753.- Son muebles por su naturaleza, los cuerpos que pueden trasladarse de un lugar a otro, ya se muevan por sí mismos, ya por efecto de una fuerza exterior.
Artículo 754.- Son bienes muebles por determinación de la ley, las obligaciones y los derechos o acciones que tienen por objeto cosas muebles o cantidades exigibles en virtud de acción personal.

Aun cuando ha habido tesis encontradas, respecto de lo que debe entenderse por bienes muebles para los efectos penales, el criterio de la Corte ha sido que debe entenderse a la Legislación para encontrar su contenido, aunque ésta no sea penal.

En virtud que la información almacenada en una computadora no es por razones expuestas una cosa muble, no puede configurarse el delito de robo tal como lo prevé nuestra Legislación. Así **Arteaga Sánchez** señala: "la doctrina penal parece estar de acuerdo en considerar que no puede hablarse de hurto cuando se obtienen datos almacenados de una computadora por no tener éstos el carácter de bien mueble corporal exigido por el delito en cuestión, salvo por lo que respecta a la materialización del dato mismo en un documento o instrumento escrito". *30*

30 Ibidem; Arteaga Sánchez, Alberto; pp. 132.

Por lo que podemos señalar que la información almacenada en un sistema informático carece del requisito de *corporeidad*, ahora bien, puede entonces ser objeto de apoderamiento. El apoderamiento es la aprehensión de la cosa, por lo que se entra en su posesión o sea que se ejerce sobre de ella un poder de hecho. "El apoderamiento se consuma cuando, además de la simple remoción de la cosa del lugar en que se encontraba, el agente la tiene en su posesión material". *31*

Nuestros tribunales han reconocido:

> El delito de robo no queda en grado de tentativa, sino que llega a la consumación, si se realiza la conducta típica de apoderamiento, la cual implica en cuanto al sujeto pasivo, desapoderamiento, vulnerándose así el bien jurídico del patrimonio, al sustraer el inculpado el objeto materia del ilícito y colocarlo bajo su poder de hecho; sin que sea relevante la circunstancia de que el sujeto activo no logre sacar el bien material del robo del local del ofendido, dado que ello, en ultima instancia, tendría significado en cuanto al agotamiento del delito, por el logro de la finalidad del acusado, pero es intrascendente en orden a la consumación, misma que ocurre desde el momento en que el sujeto activo toma el objeto, pues desde ese instante se ataca el bien jurídico tutelado, en razón de que el ofendido, en la hipótesis de querer disponer del bien, no puede hacerlo, por haber salido de su esfera de disposición. *32*

31 Ibidem; Carrancá y Trujillo Raúl, y Carrancá y Rivas, Raúl; pp. 905.

32 García, Manuel Víctor; Amparo en Revisión 209/95; 26 de abril de 1995. Unanimidad de votos; Novena Época; Primera Sala de la Suprema Corte Justicia de la Nación.

A este respecto **Gutiérrez Francés** señala: "en la sustracción de la información, el apoderamiento puede realizarse con una simple lectura o memorización de datos, de cuya utilización por lo demás no queda excluido el titular. Es por ello que **Nimmer** considera que en este delito lo que se lesiona es el derecho al secreto de los datos almacenados, el derecho a su exclusivo control, o un hipotético derecho a negar el acceso a terceros fuera de los que él decida". *33*

Como podemos ver, el legislador ha interpretado el término de propiedad dentro de la ley penal, de tal forma que no incluye a los impulsos electrónicos de un sistema. Siendo su razonamiento principal el de que la información permanece intacta dentro del sistema, es decir, nunca existe un abandono de la estructura de la computadora. Por lo que podemos concluir que no se puede hablar en estricto sentido, de robo de información.

En materia de propiedad industrial la **LPI** contiene disposiciones que podrían adecuarse a los supuestos de sustracción e información. Los preceptos son:

33 Gutiérrez Francés, Ma. Luz; Fraude Informático y Estafa; Ministerio de Justicia, Madrid, España; pp. 134.

Artículo 82. Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

No se considerara secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerara que entra al dominio publico o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad.

Artículo 83. La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

Artículo 223. Son delitos:

IV. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado.

De acuerdo con los artículos antes señalados, esta Ley protege la sustracción de información pero sólo aquélla que en términos de la misma constituya un secreto industrial; además de que se requiere el elemento subjetivo de lesionar un interés patrimonial. Aunque esta Ley presenta el avance de tutelar a la información, ya que al exigir un apoderamiento, este puede recaer en ella, a través de medios electrónicos, magnéticos o de un sistema informático. Por lo que concluiremos que en nuestra Legislación no existe una protección eficaz en la regulación de la conducta denominada como sustracción de información.

3.6 Reproducción no autorizada de programas protegidos legalmente.

Por mucho tiempo no fue reconocido dentro de la doctrina la tutela jurídica de los programas de cómputo, ya que como invenciones, eran susceptibles de ser protegidas como patentes, la **LPI**, los excluye de esta protección

Art. 19.- No Se Consideraran Invenciones Para Los Efectos De Esta Ley:

IV.- Los programas de computación;

V.- Las formas de presentación de información.

Para **Tello Valdez** "sin lugar a dudas, el derecho de la propiedad literaria y artística y, más específicamente, los derechos de autor, se prestan como la figura más aplicable frente al problema de la protección de los programas". *34*

Esta protección se prevé en la **LFDA**, en su artículo 13, que señala:

Art. 13. Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

III. Programas de Computo.

IV. De compilación, integrada por las colecciones de obras, tales como las enciclopedias, las antologías, y de obras u otros elementos como las bases de datos; siempre que dichas colecciones, por su selección o la disposición de su contenido o materias, constituyan una creación intelectual.

34 Ibídem; Téllez Valdés, Julio; pp. 90.

Art. 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

A su ves, estos derechos se encuentran tutelados por el **CPF**, el cual señala:

Art. 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

II. Al editor, productor o grabador que a sabiendas produzca mas números de ejemplares de una obra protegida por la ley federal del derecho de autor, que los autorizados por el titular de los derechos.

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la ley federal del derecho de autor.

Art. 424 bis. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la ley federal del derecho de autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior.

Por lo antes expuesto, puede señalarse que esta forma de conducta reconocida como Delito Informático, encuentra protección en nuestro sistema jurídico. Es claro que el bien jurídico tutelado por estas normas es el derecho del autor, por lo que es necesario cuestionarse si esta conducta es un Delito Informático o no.

CAPÍTULO IV

HACIA UNA NUEVA REGULACIÓN JURÍDICA PENAL DE LOS DELITOS INFORMÁTICOS

CAPÍTULO IV

4.1 La realidad jurídica de los Delitos Informáticos en la actualidad.

Del análisis jurídico del Capítulo anterior, se desprende que los Delitos Informáticos no se encuentran debidamente tutelados, tanto por el atraso Legislativo de la Legislación Penal mexicana, al no actuar conforme a los avances tecnológicos; como por la gran variedad de bienes jurídicos que pueden vulnerar dichos delitos, y que van desde el patrimonio hasta la vida o la seguridad nacional, pasando por la autenticidad de documentos, derechos de autor, etc.

Precisamente la amplitud del concepto de Delitos Informáticos (por el sinnúmero de bienes jurídicos que pueden dañar), y la naturaleza de género autónomo, ya que para muchos autores, no es distinto lo que se puede hacer con una computadora para dañar bienes jurídicos ya protegidos, que lo que se puede hacer por otros medios, por lo que no puede hablarse en estricto sentido, de una nueva categoría de delitos.

Se puede entender la critica de los autores, ya que como se ha visto, por regla general los bienes jurídicos que se vulneran con las conductas definidas comúnmente como Delitos Informáticos, encuentran protección eficaz en los tipos penales tradicionales, ya que en muchos casos el sistema informático sólo funge como medio comisivo.

CONDUCTA	BIEN JURÍDICO TUTELADO	PRECEPTO LEGAL
Fraude Informático	Patrimonio	**Art. 386 CPDF**
Falsificación por Computadora	Veracidad o autenticidad de los documentos	**Art. 243 CPDF**
Daños o modificaciones de datos computarizados o programas informáticos	Patrimonio	**Art. 399 CPDF**
Sabotaje a equipos de telecomunicaciones	Vías generales de comunicación	**Art. 167 CPDF** **Art. 533 LVGC**
Acceso no autorizado a sistemas informáticos	Patrimonio	**Art. 380 CPDF**
Acceso no autorizado a información	Protección limitada a comunicaciones. Inviolabilidad de correspondencia o de comunicaciones privadas.	**Art. 173 y 177 CPDF**
Acceso no autorizado a un servicio	Patrimonio	**Art. 368 CPDF frac. II** **Art. 426 CPF frac. II**
Sustracción de Información	Protección limitada a la propiedad industrial Confidencialidad del sector industrial	**Art. 233 LPI frac. IV**
Reproducción no autorizada de programas protegidos legalmente	Derechos de autor	**Art. 424 CPF frac. II y III**

Por lo anterior, la sola característica de que estas conductas tengan como instrumento u objeto a sistemas informáticos, no justifica *per se* la creación de un nuevo género de delitos, cuyo único elemento distintivo sería su vinculación con el sistema informático. Desde esta perspectiva, el principal error en que incurren los que pugnan por una noción amplia de delitos informáticos, considerándola como un nuevo género de delitos con autonomía propia, consiste en que no atienden al bien jurídico como criterio delimitador.

Este es el elemento más importante a tomarse en cuenta al considerar la creación de una nueva figura jurídica, como señala el **Dr. Moisés Moreno**, "...de la consideración del bien jurídico, que realmente es la razón de ser de los tipos penales, la razón de ser del Derecho Penal y, en definitiva, la razón de ser de todo el sistema penal, se derivan límites precisos de la intervención que corresponde al Derecho penal...la consideración de los bienes jurídicos tiene como función importante, precisar los contenidos de los tipos penales; determinando las formas de su afectación que son materia de regulación penal, así como otros requisitos que servirán para la sanción penal". *35*

35 Moreno Hernández, Moisés; Penalización y Despenalización en la Reforma Penal: Importancia del Principio del Bien Jurídico en la Creación de los Tipos Penales; Criminalia; Editorial Porrúa, año LIX, No. 2, México, 1993, pp. 68.

Esta ha sido además la sistemática adoptada por nuestro Código Penal, por lo que compartimos la opinión de **Bustos Ramírez**, que al referirse a la configuración de tipos penales considera que el bien jurídico "constituye el punto de partida y la idea que preside su formación...cualquier tipificación resulta imposible o bien arbitraria si no se hace desde el bien jurídico". *36*

Si se vulneran bienes jurídicos ya existentes y protegidos por las leyes penales, no se justifica la creación de nuevos delitos que busquen proteger lo que ya está protegido, por lo que estamos en contra de la teoría que sostiene una noción tan amplia de los Delitos Informáticos. Ya que también niega radicalmente la existencia de los Delitos Informáticos, negando *a priori* la existencia de bienes jurídicos nuevos que requieran protección.

Es éste nuestro principal planteamiento, ¿solo se vulneran bienes jurídicos existentes o existen conductas que vulneran otro bienes jurídicos hasta ahora desconocidos por nuestro Derecho?. La respuesta la encontraremos en el presente apartado.

36 Ibidem; Gutiérrez Francés, Ma. Luz; pp. 200.

Es claro que las conductas ya tipificadas cuyo único elemento distintivo es su vinculación con un sistema informático, no vulneran bienes jurídicos distintos, por lo que no ameritan protección penal distinta de la ya existente; por ejemplo, el robo o destrucción de una computadora.

Por otro lado, en muchos de los supuestos de los Delitos Informáticos, incluyendo a aquellas conductas que utilizan a los sistemas informáticos como un medio para la comisión del delito (fraude, ataques a las vías de comunicación) y en las que la propia información almacenada en los sistemas informáticos es el objeto de la comisión de la conducta (acceso no autorizado a información, alteración de datos, programas y sustracción de información), existe un elemento común: la afectación, antes que el patrimonio, las vías generales de comunicación o los derechos de autor, a la información almacenada en una computadora; es decir, a la información como tal, como objeto de ataque, más aún el derecho del titular de disponer de ella.

El ejemplo más claro es el acceso no autorizado a datos computarizados que es, por lo general, el primer paso en la comisión de los demás delitos informáticos (en su concepción más amplia), y que actualmente encuentra una protección muy limitada en nuestro sistema legal.

Con motivo de la revolución informática, el tratamiento y procesamiento de información forma parte del quehacer cotidiano y un elemento importante en el desarrollo de nuestra sociedad. Pero este progreso trae aparejado riesgos, y es que este mismo desarrollo tecnológico pone al descubierto la vulnerabilidad de los sistemas informáticos y de su contenido, o sea la información almacenada o procesada.

En las últimas décadas se han visto cambios muy importantes, el desarrollo de la sociedad industrial hacia una nueva era post-industrial y el incremento del valor de la información en materia económica, cultural política y hasta en la esfera privada de las personas. Estos avances tecnológicos exigen al Derecho nuevas respuestas frente a estas nuevas situaciones.

Nos encontramos frente a un bien que aunque no nuevo, ha adquirido un gran valor hasta ahora desprotegido por nuestro derecho, o protegido muy limitadamente. En este sentido **Núñez Ponce** resalta la importancia de la información, al señalar que la información "es un bien inmaterial e incorporal desde el punto de vista jurídico, pero también es un bien en el sentido económico del termino, que sirve para la satisfacción de alguna necesidad,

que puede ser elemento de producción y consumo, así como puede cotizarse en el mercado conforme a la ley de la oferta y la demanda". 37

Por todo lo anterior, se considera errónea la teoría que niega la existencia de los Delitos Informáticos, pues como se desprende del análisis hecho, existe un bien jurídico distinto de los protegidos por los tipos penales tradicionales, mismo que será objeto de estudio en el siguiente apartado, pero que por ahora puede decirse de manera general que consiste en el derecho del titular de la información de disponer de ella exclusivamente.

Nos pronunciamos por la existencia de los Delitos Informáticos, incluso como un nuevo género del delito, pero no en una acepción tan amplia como la manejada por la doctrina que incluye en este género a muchas conductas, sino en una concepción limitada en atención a la vulneración de un bien jurídico que hasta ahora carece de protección.

37 Núñez Ponce, Julio; "La Acción Habeas Data: su aplicación en un contexto jurídico informático", Revista Aequitas, segunda época, No. 22, México, diciembre de 1994; pp. 27.

Y serán Delitos Informáticos las conductas típicas, antijurídicas y culpables que tengan como objeto la información almacenada en los equipos o sistemas informáticos.

Lo que amerita la creación de una nueva figura jurídica es la desprotección actual de un bien jurídico que ha cobrado un creciente valor a propósito de la revolución tecnológica, de tal suerte que no pueda pensarse en la comisión de estas conductas sin la presencia de equipos informáticos.

Con el objeto de distinguir estas conductas de aquellas en las que se puede lograr el mismo resultado mediante el ataque físico al *hardware* (robo, daños, etc.), es preciso señalar que las primeras sólo tendrán lugar cuando además de ser la información el objeto material del delito, los medios informáticos darán los medios para la comisión del mismo.

Cuando los bienes jurídicos son otros: propiedad, patrimonio, vías generales de comunicación, autenticidad de los documentos, nuestro ordenamiento jurídico ofrece una protección efectiva, pero tratándose del bien "*información*"

no puede decirse lo mismo. En esto reside la esencia de los Delitos Informáticos.

Es necesario que nuestro derecho se actualice respecto de esta nueva conducta delictiva, para que cuente con los elementos necesarios para, por un lado prevenirlo, y por otro sancionarlo, ya que como señala **Carlo Amanzana**, "el control de la criminalidad será siempre un problema social además que criminológico y legal. Más los sistemas del mundo occidental, proyectados hacia la represión de la criminalidad, no parecen estar en grado de enfrentar este tipo de desafío tecnológico". *38*

Así tenemos, que si bien es cierto que existe una protección jurídica a los Delitos Informáticos en nuestra Legislación, también es cierto que se necesita incluir dentro de ella un nuevo bien jurídico a tutelar, el cual, analizaremos a continuación.

38 Ibidem; Lima Ma. De la Luz; pp. 109.

4.2 La autonomía de los delitos informáticos.

En este apartado analizaremos la naturaleza del bien jurídico que debe protegerse para dar una autonomía y crear así en estricto sentido a los Delitos Informáticos; se debe aclarar como se analizo en el Capítulo Segundo, que no existe un consenso en la doctrina en relación a la naturaleza jurídica, más aún se han adoptado posiciones bajo muy distintos criterios.

Podemos agrupar las posturas existentes en tres categorías:

- Protección de la intimidad.
- Protección de un interés macrosocial.
- Protección de la información.

El tema se ha abordado principalmente desde la perspectiva del derecho a la intimidad. Se ha desarrollado contemporáneamente toda una teoría relacionada con la intimidad, misma que se ha pretendido aplicar a la informática.

Con el objeto de comprender esta postura, haremos un breve análisis de la concepción de la intimidad, que nos permitirá verificar posteriormente si efectivamente éste es el bien jurídico que requiere de protección.

En su origen etimológico, "*intimidad*" proviene del termino *intus* (dentro), superlativo del interior. El Diccionario de la Real Academia de la Lengua define a la intimidad como "zona espiritual íntima reservada de una persona o un grupo, especialmente de una familia".

En la definición del concepto, han surgido diversas doctrinas que pretenden explicar el concepto de intimidad; por un lado la teoría de las "*esferas*", según la cual "el ser humano es un centro de actividades alrededor del cual se desarrollan varios círculos concéntricos. Los más cercanos al individuo son los más íntimos y los más externos son los menos cercanos". [39] Así, las esferas de lo que concierne al ser humano irían de la más cercana, esfera secreta o íntima, a la más externa, esfera social, relacionadas por otras intermedias como esfera de confianza, individual o propia.

39 Meján, Luis M.; El Derecho a la Intimidad y la Informática; Edit. Porrúa, segunda ed. México, 1996; pp. 73.

Por otro lado, la teoría del "*mosaico*", cuyo contenido se centra más en los roles que sociológicamente desempeña el individuo cuya privacía se afecta, sosteniendo que un individuo no es sólo una información, sino un complejo entre ellas, y relacionadas con otras el resultado puede variar. Es decir, un ilícito puede o no ser agresivo al derecho de la intimidad, reunido con otros si puede serlo,

Las teorías expuestas adolecen de auténticos criterios objetivos para la determinación del concepto, lo que por su misma naturaleza resulta difícil, ya que en nuestra opinión su contenido puede variar de persona a persona.

Esto ha llevado a algunos autores a señalar las áreas específicas que deben considerarse como integrantes de la intimidad, por ejemplo: imagen, correspondencia, papeles y archivos particulares, conversaciones privadas, información médica o financiera, relaciones sexuales, posturas ideológicas relaciones relacionadas con el honor. Áreas que podríamos llamarlas de cuestiones personales.

El desarrollo de la teoría de la protección de este importante derecho, que ha sido reconocido por la Declaración Universal de los Derechos del Hombre ha dado a lugar a instituciones legales incluso constitucionales en varios países, que protegen el derecho "para conocer y decidir respecto de la información propia de carácter personal", entre estas distintas instituciones ha surgido un importante recurso denominado "*Habeas Data*".

Núñez Ponce señala que "en el contexto latinoamericano la Constitución Brasileña ha incluido la acción *Habeas Data* que trata tanto el aspecto preventivo como el correctivo con el objeto de defender derechos de la persona, como el de la intimidad, frente a la utilización de la informática principalmente por el poder público. En la Constitución Colombiana si bien no se hace mención expresamente el *Habeas Data* se señala en su artículo 15 que la persona tiene derecho a "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas..."; en la Constitución Paraguaya, sí se incluye expresamente la acción de *Habeas Data*. [40]

40 Ibidem; Núñez Ponce; Julio; pp. 41.

El Derecho a la Intimidad es un bien jurídico que debe protegerse ante los avances tecnológicos en materia informática. **Luis Meján** señala, "con las facilidades que hoy en día proporcionan los avances en electrónica como en las comunicaciones, las informaciones que dichas entidades acumulan en el ejercicio de sus acciones, son fácilmente recuperables, usables, relacionables entre sí, transmisibles y accesibles. Esta enorme ventaja que, sin duda alguna, facilita enormemente la labor de los dueños de los bancos de datos, supone una terrible amenaza al básico derecho de la intimidad...Por ello puede hablarse que existe un derecho a la intimidad Informática que regule precisamente la salvaguarda del derecho a la privacía en la materia de acumulación de información". *41*

Este derecho, lo podríamos entender desde dos puntos de vista; el primero, desde el punto de vista de aquél a quien se refiere la información y, segundo, desde el punto de vista del titular de la información almacenada. Es este segundo aspecto el que es relevante para efectos de nuestra investigación.

41 Banho Licks, Otto; pp. 65.

No cabe duda que debe protegerse a las personas a quienes se refiere la información almacenada en una base de datos, y menos que ese derecho encuadre dentro del Derecho a la intimidad, pero ¿puede decirse que ese derecho se le vulnera al titular de la información, ya por que la haya sustraído o por que la haya adquirido legítimamente, cuando una persona no autorizada accesa a ella o la modifica, independientemente de su contenido?.

Como se ha visto, el derecho a la intimidad es un derecho que se encuentra sustentado en cuanto a su contenido, es decir, información de carácter personal, incluso las acciones que han surgido en torno a él no pueden ir más allá de la información relacionada con la intimidad, ya que la función esencial del *Habeas Data* es asegurar el conocimiento de las informaciones relativas al solicitante.

Por lo anterior, si la información que un sujeto mantiene almacenada dentro de sus sistemas informáticos no le es personal, no podría en estricto sentido decirse que se afectó su intimidad con el acceso a la misma o con su alteración, aunque si puede con esas mismas conductas afectarse la intimidad de otros.

Morales Prats señala, "...esta criminalidad informática no sólo constituye una amenaza tecnológica para la privacidad individual, otros bienes jurídicos se han visto puestos en peligro o destruidos con el evento del uso generalizado de ordenadores y redes telemáticas". 42

Gutiérrez Francés opina que existe un interés de carácter macrosocial susceptible de ser calificado como la confianza en el funcionamiento de los sistemas informáticos, pues el auge de estos sistemas y su irrupción en la mayoría de las facetas de nuestro actuar cotidiano, han desembocado en una dependencia a estos sistemas. "Se trata de una condición indispensable para el normal desarrollo del sistema de relaciones en nuestros días, por que en la misma se apoyan de modo esencial las actividades del mundo bancario, bursátil, de seguros, transportes, seguridad social, etc." 43

42 Morales Prats, Fermín; La Tutela Penal de la Intimidad: Privacidad e Informática; Ed. Destino, España, 1984; pp. 325.

43 Ibidem; Gutiérrez Francés, Ma. Luz; pp. 266.

Desde esta percepción se trata de un interés colectivo, porque afecta a la comunidad en cada uno de sus miembros. Este interés consiste en la confianza o en la buena fe colectiva del correcto funcionamiento de estos sistemas, lejos de agresiones.

Compartimos la opinión de **Gutiérrez Francés**, ya que existe un interés social que puede vulnerarse con estas conductas, sobre todo porque como ya se demostró, suelen ser pluriofensivas, por lo que en última instancia, la lesión es a la sociedad. Sin embargo, esta postura no da luz respecto del bien jurídico inmediato que pueda afectarse con la comisión de estas conductas.

Por otro lado, con motivo de una sentencia del Tribunal Constitucional Alemán, de 15 de diciembre de 1983, habla de un nuevo derecho: "**el derecho a la autodeterminación informativa**", que consiste, según el propio Tribunal, en "la facultad de un individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo, cuando y dentro de qué límites puede revelar situaciones referentes a la propia vida". *44*

44 Ibidem; Banho Licks, Otto; pp. 70.

El ámbito de esta protección debe ser más amplio que el derecho a la intimidad, en orden a proteger los datos personales frente a la informática conviene abandonar la referencia de la intimidad y enunciar un nuevo derecho, el derecho a la autodeterminación informativa, que tendría como objeto preservar la información individual (íntima y no íntima) frente a la utilización incontrolada.

Se ha reconocido la estrecha relación de este nuevo derecho con el derecho a la intimidad; por un lado, el derecho a la intimidad consiste en la libertad frente a toda intromisión sobre uno mismo, su casa, familia, comunicaciones (derecho de defensa), y por el otro, el derecho a la autodeterminación informativa que consiste en el derecho a determinar cómo y en qué , medida se puede comunicar a otros sobre uno mismo (derecho de actuación).

Aun cuando a primera vista pudiera parecer que se trata de las dos caras de una moneda, consideramos que nos encontramos frente a un nuevo derecho de contenido más amplio que el derecho a la intimidad, toda vez que se evitan

problemas que se presentan al hablar del derecho a la intimidad, por ejemplo lo subjetivo de su contenido, o las dificultades ante las que nos encontramos respecto de la información que es propia de las personas morales, pues en estricto sentido es cuestionable que las mismas tengan intimidad.

No obstante a lo anterior, tanto el nuevo derecho a la autodeterminación informativa como el derecho a la intimidad están limitados en su contenido, pues dejan fuera a la información que no es propia de la persona que tiene el derecho; por ejemplo, la información que tiene almacenada una sociedad de información crediticia en su base de datos que no se refiere a la misma, sino a la situación crediticia de los sujetos respecto de los que se posee información.

En este supuesto, el acceso o modificación a la base de datos, en teoría vulneraría el derecho a la intimidad de los sujetos respecto de los cuales se posee información, no así tratándose de la sociedad, pues los datos a los que se accesó no son personales de la misma (autodeterminación informativa) y mucho menos le son íntimos (derecho a la intimidad).

Consideramos necesaria una protección más general que no esté limitada en cuanto a su contenido, sino que proteja a la información almacenada en una base de datos independientemente de que esta sea de carácter personal, íntima o incluso ajena. Es decir, una concepción más amplia de la que ahora tiene el derecho a la autodeterminación informativa.

El experto francés **Pierre Catala** ha sostenido que "la información ha tenido que ser considerada no sólo desde el punto de vista de la comunicación, en otras palabras, como una relación entre la gente, como un servicio; pero en su contenido también ha tenido que ser considerada como un producto, como un bien en sí mismo con un valor social y económico. Ya que la información es pensada como el objeto de un verdadero derecho de propiedad, propiedad intangible. Se ha sugerido que la evolución de las máquinas automáticas han creado un nuevo producto "*el bien jurídico informático*", un nuevo tipo de bien inmaterial que debe ser protegido por la Ley". [45]

45 Frosini, Vitorio; El Derecho y la Información en la Actualidad; Informática e Diritto; vol XXI; Número 2; Italia; 1995.

En este sentido, **Ríos Estabillo** sostiene que "el bien jurídico tutelado en los ilícitos informáticos es la información, debiendo comprender en ésta la que se deriva tanto del lenguaje natural como informático...ya que, por las características de las posibles conductas ilícitas en los supuestos mencionados... lo que se protege es la información contenida en bancos de datos, redes de computadoras, o simples computadoras personales". *46*

Añadiremos que más que la información en sí misma, es el derecho del titular de la información de disponer de ella exclusivamente (lo que comprende su acceso y modificaciones), ya sea por que lo ha generado o porque lo ha adquirido lícitamente.

Lo anterior en virtud de que siguiendo a **Zaffaroni**, el bien jurídico tutelado es la relación de disponibilidad de un individuo con un objeto, protegida por el Estado "...los bienes jurídicos suele decirse que son, por ejemplo, la vida, el honor, la propiedad, etc. En realidad, si bien no es incorrecto decir que el honor es un bien jurídico, eso no pasa de ser una abreviatura, porque el bien

46 Ríos Estabillo, Juan J.; Derecho e Informática en México; UNAM, México, 1997; pp. 128 y 129.

jurídico no es propiamente el honor, sino el derecho a disponer del propio honor, como el bien jurídico no es la propiedad, sino el derecho a disponer de los propios derechos patrimoniales...el ente que el orden jurídico tutela contra ciertas conductas que le afectan no es la cosa en si misma, sino la relación de disponibilidad del titular de la cosa." 47

Esta ha sido, en nuestra opinión, la postura adoptada por varios Estados, desde el momento en que han tipificado el sólo acceso sin autorización a sistemas informáticos, tal es el caso de Alemania, Australia, Dinamarca, Estados Unidos de América, Finlandia, Francia, Grecia, Irlanda, Israel, Italia, Países Bajos, Noruega, Suecia y Suiza.

Luego entonces, el bien jurídico a tutelarse, será en nuestra opinión, la autodeterminación informativa en un sentido más amplio al aceptado por la jurisprudencia extranjera y la doctrina, consistente en la disponibilidad de la información que comprende dos aspectos:

47 Zaffaroni Eugenio, R.; Manual de Derecho Penal; Ed. Cárdenas editor y distribuidor, segunda ed., México, 1994; pp. 410.

- Facultad del titular de la información de decidir sobre quien tenga acceso a ella; aquí, estamos hablando de la confidencialidad o privacidad de la información; y
- Facultad del titular de la información de disponer de ella; aquí, estamos hablando de la integridad de la información.

Con el análisis hecho en el presente punto, debemos concluir que para hablar de una autonomía, y por ende, un pleno reconocimiento de los Delitos Informáticos en la Legislación Penal Mexicana, es necesario tutelar un nuevo bien jurídico, que en este caso es la información.

Información que debe verse desde los dos aspectos señalados con anterioridad, así, las conductas que no se encuentran debidamente tuteladas en la actualidad, por estar sujetas tan solo a la tutela de bienes jurídicos reconocidos, podrán ser tuteladas, para así tener una prevención y posible sanción de dichas conductas.

4.3 El trabajo legislativo nacional con relación a los delitos informáticos.

Si bien es cierto que por los grandes avances tecnológicos, y la falta de trabajo Legislativo a nivel Federal y Local, no existen grandes avances en materia de Delitos Informáticos, en los últimos tres años se ha dado un esfuerzo por realizar un trabajo legislativo que tutele estas conductas que cada vez más afectan las relaciones cotidianas de toda la nación.

4.3.1 Legislaciones locales.

De los Estados de la República que tienen adelantos en materia de Delitos Informáticos debemos señalar a Sinaloa, cuyo Código Penal establece:

Art.º 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, use, altere, dañe a destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa.

En relación con este artículo caben las siguientes observaciones:

- El artículo se ubica dentro del Título correspondiente a los delitos patrimoniales, por lo que atendiendo al bien jurídico tutelado en relación con la sistemática del propio Código, es claro que se pretende proteger el patrimonio del titular, por lo que tal vez se consideró la información como un bien, aunque intangible, integrante del patrimonio.
- Es plausible, que el delito solo admita comisión, lo que es acorde con las recomendaciones del XV Congreso Internacional de Derecho Penal, en el cual coincidimos, pues la comisión culposa de las conductas descritas por el tipo no requiere de punición en atención al carácter del Derecho Penal.
- Además del dolo, el uso o ingreso a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, requiere el elemento subjetivo específico de que dichas conductas se hagan con el fin de defraudar, obtener dinero, bienes o información, lo que deja al descubierto el tan común acceso por simple entretenimiento (hacker), que puede dar lugar a conductas ilícitas posteriores, pero que por lo pronto no agotaría el tipo penal del artículo en cuestión.

Otras legislaciones locales solo otorgan protección a la intimidad, que podrían cubrir ciertas conductas de los Delitos Informáticos, por ejemplo los Estados de Morelos y Tabasco:

Titulo Sexto Delitos contra la Intimidad Personal o Familiar
Capítulo I Violación de la intimidad personal
Artículo 150. Se impondrán de seis meses a cuatro años de prisión, a quién sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer asuntos relacionados con la intimidad de aquél:
I. Se apodere de documentos u objetos de cualquier clase;
II. Reproduzca dichos documentos u objetos; o
III. Utilice medios técnicos para escuchar, observar, transmitir, grabar o reproducir la imagen o sonido.

El Código Penal de Tabasco, tipifica exactamente la misma conducta en su artículo 163, con la única diferencia de que en éste las sanciones son de seis meses a cinco años de prisión.

Como hemos visto en el presente apartado, existen legislaciones donde se ha otorgado protección con fundamento en el derecho a la intimidad, sin embargo, y como se desprende de los artículos en cuestión, la protección es muy limitada, ya que carece de tutela cualquier información que no sea relacionada con la intimidad, así como la alteración de la información en general, incluso la relacionada con la intimidad, que podrían comprender conductas como el fraude informático.

4.3.2 Legislación Federal.

Con fecha 22 y 23 de abril de 1999 y publicada en el **DOF** el 17 de mayo de 1999 fueron aprobadas una serie de reformas al **CPF**, cuyo origen se remonta a la denominada "Cruzada Nacional contra el Crimen y la Delincuencia", la cual presentaba una serie de iniciativas en diversas materias con el objetivo de actualizar nuestra legislación para hacer frente a la inseguridad por la que atraviesa el país.

La reforma consiste en la modificación del Título Noveno del **CPF** y en la adición de un Capítulo II dentro del mismo Título.

TÍTULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPÍTULO II

Acceso ilícito a sistemas y equipos de informática

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

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

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

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

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

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

Art. 211 bis 4.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Art. 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este **art.** se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Art. 211 bis 6.- Para los efectos de los **arts** 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el **art.** 400 bis de este código.

Art. 211 bis 7.- Las penas previstas en este Capítulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno

Consideramos correcta la ubicación dentro del **CPF**, ya que el Título Noveno, antes solo se integraba por el delito de revelación de secretos, el cual protege la confidencialidad de la información. Con la reforma el legislador considera que no solo se atenta con estas conductas en contra de los bienes patrimoniales, sino que pueden dar cabida a la vulneración de otros bienes, como la intimidad o la información en general.

Partiendo del supuesto de que el bien jurídico protegido por el tipo en la revelación de secretos es la confidencialidad de la información, es apropiado extender el Título Noveno a la protección de la privacidad e integridad de la información, pues al compartir el elemento objeto de protección jurídica, comparten su naturaleza.

Podríamos considerar al término "informática" como un elemento normativo del tipo, toda vez que el mismo está definido por el artículo 3 de la **LIEG**, como la tecnología para el tratamiento sistemático y racional de información, mediante el procesamiento electrónico de datos.

Se protege la integridad de la información independientemente de que el acceso haya sido autorizado o no, y a cualquier titular de la misma.

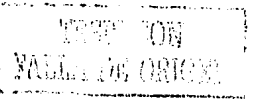
A diferencia del **CPES**, las reformas en materia federal contemplan:

- Se elimina el elemento subjetivo específico consistente en que el uso o acceso a la base de datos se haga con el fin de defraudar, obtener dinero, bienes o información, y
- Se eliminan las conductas de "recibir" "usar" "dañar" que no configuran ataques a la información, por lo que no pueden catalogarse como Delitos Informáticos. Estas conductas están protegidas por otros tipos penales como el robo de uso o el daño en propiedad ajena.

No obstante de los avances logrados en la materia, es necesario precisar:

- Subsiste, como elemento del tipo, la necesidad de que los sistemas o equipos de informática estén protegidos por algún mecanismo de seguridad. Esto no se considera correcto, ya que solo beneficia a las personas con recursos económicos elevados.
- Por lo que hace a la información contenida en los sistemas o equipos de informática de las instituciones que integran el sistema financiero, no se explica la existencia de dos tipos penales distintos que sancionen por un lado al que sin alteración modifique, destruya, provoque pérdida, conozca o copie información (art. 211 bis 4), y por el otro, al que estando autorizado para acceder a sistemas y equipos, indebidamente modifique, destruya, provoque pérdida o copie información.

Esta misma distinción la encontramos respecto de la información contenida en equipos o sistemas informáticos del Estado, en este caso la distinción es relevante ya que en el segundo supuesto la pena es mayor, lo que no sucede con los equipos o sistemas de instituciones que integran el sistema financiero.



En este orden de ideas, del mismo modo es punible la realización de estas conductas independientemente de si el autor está autorizado para acceder o no. La diferencia estriba en que en el primer supuesto la conducta se comete "sin autorización", en tanto que en el segundo, "indebidamente", concepto más amplio que el anterior y que puede ser muy subjetivo.

Realmente el acceso, con autorización o sin ella, no es factor en la realización de las conductas si éstas se realizan sin autorización o indebidamente, salvo en el caso en que se aumenta la pena en atención a la vulneración de la confianza que se ha depositado en quién esta autorizado para acceder. Esto sería congruente con los artículos procedentes que aumentan la pena en la misma situación, respecto de equipos o sistemas del Estado, por lo que se propone aumentar la pena en los mismos términos.

Consideramos conveniente que los delitos previstos sólo sean perseguibles por querella del ofendido, pues en mucha ocasiones son más los perjuicios que pueden causarse en el proceso penal que los causados por la vulneración al bien jurídico, por ejemplo, la fama de inseguridad en los sistemas informáticos de un banco, o la publicidad de vulnerabilidad de secretos comerciales.

4.4 Perspectivas para el futuro de los Delitos Informáticos.

Es indudable que a través del presente trabajo no existe duda alguna de la necesidad de un mayor trabajo jurídico con relación a los Delitos Informáticos, su existencia no tiene ni siquiera punto de discusión; la trascendencia y evolución constante de los mismos requiere un estudio arduo llevado a cabo no solo por los estudiosos del derecho, si no por peritos en materia Informática, para así poder llegar a una posible solución.

En el Derecho Penal Mexicano el paso principal es reconocer a los Delitos Informáticos como tal, para dar un adecuado tratamiento a los mismos; en el futuro existe una iniciativa muy importante para el adecuado tratamiento de los sistemas informáticos, el cual puede ser la punta de lanza para una mejor tutela de los mismos.

La iniciativa de ***"Ley de Protección de datos Personales"***, presentada en el Senado de la República el 14 de febrero de 2001, es un avance en el reconocimiento de la tutelación del derecho a disponer de una información privada y el reconocimiento jurídico de los sistemas informáticos.

En su exposición de motivos, se maneja un objeto jurídico de la misma:

Se propone que la garantía procesal tenga por objeto:

1. Que el interesado pueda acceder a los datos personales que le conciernen.

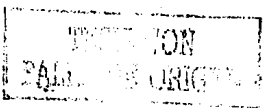
2. Que toda persona pueda acceder a los registros, archivos y bancos de datos públicos o privados de carácter público, y conocer su uso o fin para el que están destinados.

3. Que el interesado pueda pedir la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los datos relativos a su persona.

Con los cuales nos encontramos totalmente de acuerdo, y creemos que esta Ley puede ser la punta de lanza que impulse al poder Legislativo a tener avances en materia de sistemas informáticos.

Y al hablar de sistemas informáticos, no solo nos referimos a los Delitos Informáticos, si no al conjunto de actividades relacionadas con los mismos, ya que solo teniendo una visión amplia de la los mismo se podrán tomar medidas adecuadas para la regulación de los mismos.

Ya que no solo la materia penal se encuentra afectada por el atraso legislativo en materia informática, la materia civil, administrativa, fiscal, etc., se encuentran atrasadas y por ende no tutelan las nuevas figuras jurídicas que se presentan en la realidad y que crean lagunas jurídicas.



Se propone que la garantía procesal tenga por objeto:

1. Que el interesado pueda acceder a los datos personales que le conciernen.

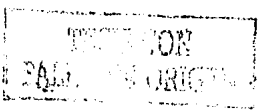
2. Que toda persona pueda acceder a los registros, archivos y bancos de datos públicos o privados de carácter público, y conocer su uso o fin para el que están destinados.

3. Que el interesado pueda pedir la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los datos relativos a su persona.

Con los cuales nos encontramos totalmente de acuerdo, y creemos que esta Ley puede ser la punta de lanza que impulse al poder Legislativo a tener avances en materia de sistemas informáticos.

Y al hablar de sistemas informáticos, no solo nos referimos a los Delitos Informáticos, si no al conjunto de actividades relacionadas con los mismos, ya que solo teniendo una visión amplia de la los mismo se podrán tomar medidas adecuadas para la regulación de los mismos.

Ya que no solo la materia penal se encuentra afectada por el atraso legislativo en materia informática, la materia civil, administrativa, fiscal, etc., se encuentran atrasadas y por ende no tutelan las nuevas figuras jurídicas que se presentan en la realidad y que crean lagunas jurídicas.



CONCLUSIONES

1. El uso del término "Delito Informático", es inadecuado en la Legislación Penal Mexicana, ya que como tal, no se encuentran tipificado por la misma; por lo que hasta que no se tipifique en Ley alguna, es incorrecto el término jurídico de Delito Informático, por lo que únicamente podemos hablar de su tutela a través de otras figuras jurídicas.
2. A nivel internacional, se encuentran plenamente definidas las conductas que comprenden los denominados Delitos Informáticos; dichas conductas han sido reconocidas a través de foros internacionales y plasmadas dentro de las Legislaciones de diversos países, dejando en claro la problemática de tal fenómeno y la necesidad de pronta tutela en la Legislación Penal Mexicana.
3. En la Legislación Penal mexicana, el Delito Informático esta contemplado como un *accesorio*, es decir, las conductas penales tradicionalmente reconocidas (protección de patrimonio, vías generales de comunicación, derechos de autor, etc.), pretenden proteger y en su caso castigar este tipo de conductas, aunque en la realidad ya se encuentra rebasadas dada la evolución de este tipo de conductas.

4. Debido al gran avance tecnológico de nuestros días, es necesario reconocer la autonomía de los Delitos Informáticos; precisando que dicha autonomía debe ser limitada, ya que debe referirse únicamente a los datos o información almacenada en un equipo o sistema informático; sin tratar de negar o de ampliar a la misma.
5. Es indudable la existencia de los Delitos Informáticos, aunque estos se encuentren o no dentro de la legislación de determinado país. Por Delito Informático debemos entender *a las conductas típicas, antijurídicas y culpables que tengan como objeto la información almacenada en los equipos o sistemas informáticos*.
6. Consideramos que el bien jurídico que debe protegerse es la *autodeterminación informativa*, en un sentido más amplio que el reconocido por la jurisprudencia y la doctrina, consistente *en la disponibilidad de la información*. Esta relación de disponibilidad comprende dos aspectos: *la facultad del titular de la información de decidir sobre quien tenga acceso a ella (confidencialidad o privacidad de la información), y la facultad del titular de disponer de la información)*.
7. El trabajo legislativo para el adecuado tratamiento a estas conductas a sido escaso, resaltando el caso de Sinaloa; a nivel Federal y Estatal, no se ha logrado un avance legislativo sustantivo, que se encuentre plasmado en Ley alguna y que permita proteger y castigar este tipo de conductas.

8. Es necesario que las leyes en México *evolucionen* a la par de los acontecimientos de la vida diaria, por ello, nos parece apropiado la propuesta de iniciativa de Ley para la creación de la *Ley de Protección de Datos*, la cual por fin contempla el reconocimiento del problema, y las posibles soluciones; ya que es el primer esfuerzo por incorporar a la Legislación la protección de datos, y por ende de los sistemas informáticos.

FUENTES CONSULTADAS

BIBLIOHEMEROGRAFÍA

- Arocena A., Gustavo; *Delitos Informáticos*; Revista de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Córdova; Vol. 5, No. 1; República de Argentina; 1997.
- Arteaga Sánchez, Alberto; *El Delito Informático, Algunas Consideraciones Jurídico-Penales;* Revista de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela; año XXXIII, No. 68; Caracas; 1987.
- Banho Licks, Otto y De Araujo, Joao M.; *Criminal Laws Aspects of Computer Crime*; Informatica e Diritto, Vol. XXI, No. 2, Italia 1995.
- Barrios Garrido, Gabriela, Muñoz de Alba, Marcia y Pérez Bustillo, Camilo; *Internet y derecho en México*; Editorial Mac Graw-Hill; México; 1998.
- Becerra Bautista, José; *El Proceso Civil en México*; Editorial Porrúa; decimocuarta edición, México, 1992.
- Callegari, Nidia; *Delitos Informáticos y legislación*; Revista de la Facultad de Derecho Y Ciencias Jurídicas de la Universidad Pontificia y Bolivariana, No. 70, Medellín , Colombia, julio-septiembre de 1995.
- Carrancá y Trujillo, Raúl y Carrancá y Rivas, Raúl; *Código Penal Anotado*; Editorial Porrúa, decimoctava edición, México, 1995.
- Clark, Jhon O. E.; *Computadoras en Acción*; Traducción de Corominas Sergio; Editorial Brugera, Italia, 1970.
- Corripio Gil Delgado, María Reyes; *Los Contratos Informáticos: el Deber de Información Precontractual*; Editado por la Universidad Pontificia de Comillas, Madrid, España, 1999.
- De Pina Vara, Rafael; *Diccionario de Derecho*; Editorial Porrúa, Novena Edición, México, 1980.
- González Quintanilla, José Arturo; *DERECHO PENAL MEXICANO*; México, Editorial Porrúa, 1997, cuarta edición.
- Gutiérrez Francés, María de la Luz; *Fraude Informático y Estafa*; Ministerio de Justicia, Madrid, 1991.

- Iriarte, Mauricio; *El Derecho, definiciones, delimitaciones y aspectos generales*; Universidad Católica de Chile; www.chez.com/cmi/definición; 1997.
- *Juliussen, Egil;* Internet Industry Almanac; *Editorial del Fondo de las Naciones Unidas, marzo 1999.*
- Lascano, Edisón; *Historia de la Informática*; Revista Jurídica de la Universidad Católica de Chile; www.sis.epa.edu.ec; 2000
- Lima, María de la Luz; *Delitos Electrónicos*; Criminalia; Editorial Porrúa; año L, números 1-6, México, enero-junio, 1984.
- Meján Luis, M; *El Derecho a la Intimidad y la Informática;* Editorial Porrúa, segunda edición, México, 1996.
- *México Frente a la Era de la Información*; Editado por la Academia Mexicana de Ciencias; México, 1999.
- Morales Prats, Fermín; *La Tutela Penal de la Intimidad Privacy e Informática*; Editorial Destino; España, 1994.
- Moreno Hernández, Moisés; *Penalización y Despenalización en la Reforma Penal: Importancia del Principio del Bien Jurídico en la Creación de los Tipos Penales*; Criminalia, Editorial Porrúa, ano LIX, No. 2, México, mayo-agosto de 1993.
- Núñez Ponce, Julio; *La acción Habeas Data: su aplicación en un contexto jurídico informático*; Revista Aequitas, segunda Época, No. 22, Sinaloa, México, 1994.
- Ríos Estabillo, Juan J.; *Derecho e Informática en México*; UNAM; México, 1997.
- Ruiz Miguel, Carlos; *En torno a la Protección de Datos Personales Automatizados*; Revista de Estudios Políticos; Nueva Época, No. 84, Madrid España, abril-junio, 1994.
- Sarzana, Carlo; *"Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia*; Nos. 1-2 Año 1. Roma, Italia.
- Serrano, A. E.; *Computadoras y Derecho, una Introducción a la Informática Jurídica*; Impreso en la Universidad de Zulia, Maracaibo, Venezuela, 1975.
- Téllez Valdez, Julio; *Derecho Informático*; Editorial Mac. Graw-Hill, segunda edición, México, 1996.

- Velásquez Bautista, Rafael; *Protección Jurídica de Datos Personales Automatizados*; Editorial Colex, Madrid, 1993.
- Wasik, Martin; *Crime and Computer*; Editorial Claredon Press, Gran Bretaña, 1991.
- Zaffaroni, Eugenio R.; *Manual de Derecho Penal*; Editorial Cárdenas, segunda edición, México, 1994.

LEGISLACIÓN

- Código Fiscal de la Federación
- Código Penal para el Distrito Federal en materia Fuero común y para toda la República en materia de Fuero Federal
- Código Penal para el Estado de Morelos
- Código Penal para el Estado de Sinaloa
- Código Penal para el estado de Tabasco
- Código Civil para el Distrito Federal
- Ley Aduanera
- Ley de Comercio Exterior
- Ley de Información Estadística y Geográfica
- Ley de Vías Generales de Comunicación
- Ley de la Propiedad Industrial
- Ley del Impuesto sobre la Renta
- Ley del Mercado de Valores
- Ley Federal de Telecomunicaciones
- Ley Federal del Derecho de Autor

JURISPRUDENCIA

Seminario Judicial de la Federación.

SISTEMA INFORMÁTICO DE COMUNICACIONES

Internet.