UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO PENAL

REFORMAS AL ARTÍCULO 231 FRACCIÓN XIV DEL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL

T E S I S:

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN DERECHO

PRESENTA:

MARTHA FIGUEROA PÉREZ

ASESOR: **MTRO. CARLOS BARRAGÁN SALVATIERRA**

CIUDAD UNIVERSITARIA, 2006

Este esfuerzo lo dedico con gran respeto y cariño:

A mis padres:

> *Por su cariño, comprensión y apoyo incondicional, por ser el estímulo más grande de mi vida, por sus consejos, por inculcar en mí principios y valores que me han llevado a culminar uno de mis máximos anhelos y sabiendo que jamás existirá una forma de agradecer una vida de lucha, sacrificio y esfuerzo constante, sólo deseo que comprendan que mi logro es suyo y que mi esfuerzo es inspirado en ustedes.*

A mi hermana:

> *Por apoyarme en todo momento, por sus consejos y cariño.*

Al Mtro. Alberto Enrique Nava Garcés:

> *Por su gran apoyo para culminar el presente trabajo, por todos sus consejos y conocimientos compartidos.*

Al Mtro. Carlos Barragán Salvatierra:

> *Con gran respeto y admiración, a quien con su apoyo y dedicación dirigió el presente trabajo.*

A mi Universidad Nacional Autónoma de México:

> *Por ser la Máxima Casa de Estudios, que me dio las herramientas necesarias para formarme como profesionista y con quien siempre estaré agradecida.*

A la Lic. Anabel Hernández Sierra:

Por brindarme su valiosa amistad, cariño y apoyo incondicional .

A Juan Alberto Morales Almonte:

Por su gran amistad y cariño incondicional, por su apoyo y consejos.

A Gamaliel Silva Molina:

Por su amistad y cariño.

A Diego O. Carrasco Hinojosa:

Por su amistad, confianza y apoyo para culminar el presente trabajo.

Al Cinvestav:

Institución que me ha permitido convivir con grandes científicos e investigadores. Pero principalmente a la Subdirección de Asuntos Jurídicos: Alberto Enrique Nava Garcés, Diego O. Carrasco Hinojosa, Alejandra Sánchez Baena, Diana Judith Rubí Crespo, Julio Bautista Hernández y Raymundo Álvarez Campillo

ÍNDICE

INTRODUCCIÓN

La informática está hoy presente en casi todos los campos de la vida moderna, por ello las computadoras se han convertido en una herramienta indispensable para el desarrollo de la sociedad, ya que son utilizadas para almacenar una gran cantidad de datos, realizar diversas operaciones contribuyendo al mejoramiento y progreso de las áreas científicas e industriales.

Mucho se habla de los beneficios que los medios de comunicación han aportado a la sociedad actual y sobre todo el uso de las computadoras, pero no todo es así; la aparición de la nueva era informática ofrece un aspecto negativo, ya que ha abierto las puertas a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginarse.

Por ello ha surgido la necesidad de proteger los datos personales contenidos en una computadora, de tal manera que asegure la integridad, confidencialidad y disponibilidad de estos.

Debido a la magnitud e impacto que ha tenido el uso de la computadora en la sociedad, ya sea por la posibilidad de almacenar datos, o la de realizar operaciones por medio de una computadora con otra sin importar la distancia ni su ubicación, el Estado se ha visto obligado a intervenir para salvaguardar los intereses de sus gobernados, considerando a todos estos elementos como un bienes jurídicamente tutelados.

Los avances en la tecnología de los sistemas informáticos, provocan una serie de trasformaciones en la realidad social. Estos cambios, repercuten en todas las personas que utilizan estos medios informáticos ya sea por motivos laborales, de entretenimiento, educativos o científicos.

El derecho también se ve afectado con los avances tecnológicos, debido a que tiene que adaptarse a esos cambios, muestra de ello, es la aparición de nuevas formas de delincuencia, las cuales se manifiestan dentro del campo de la informática, conductas ilícitas que constituyen los llamados “delitos informáticos”,

como lo son: el acceso no autorizado a sistemas informáticos, la intercepción de correo electrónico, la manipulación de programas, la reproducción no autorizada de programas informáticos de protección legal o el mismo robo por medios informáticos.

La aparición de estas conductas ilícitas en el campo de la informática, acarrea la necesidad de crear nuevos tipos penales, o bien, ubicarlos con sus peculiaridades, en los tipos penales ya establecidos en nuestra legislación.

La respuesta de nuestros legisladores no se ha hecho esperar, a lo largo de estos últimos años, hemos visto varios intentos por regular a los llamados delitos informáticos, sin embargo, dicha regulación ha sido ineficaz e insuficiente, la redacción de estos tipos penales, es muy ambigua, lo cual trae como consecuencia que sean poco entendibles y su interpretación se vuelva obscura.

Es por ello, que cada día es más urgente una regulación adecuada de estos delitos, en la cual se considere la importancia que revisten dichos delitos.

En el presente trabajo, analizaremos lo establecido en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, el cual regula el acceso ilícito a los sistemas o programas informáticos del sistema financiero, a fin de realizar operaciones, transferencias o movimientos de dinero o valores, sin embargo, dicho precepto no es suficiente para tratar este problema que se presenta en el mundo informático.

En el primer capítulo, nos ocuparemos del origen y evolución de la informática, partiendo de la evolución que han tenido las computadoras, en virtud de que consideramos importante tener una perspectiva y una visión general de esta evolución. Asimismo, daremos una definición de aquellos conceptos fundamentales en materia informática, para una mejor comprensión del tema.

En el segundo capítulo, abordaremos el tema de delitos informáticos, para lo cual veremos sus orígenes, antecedentes y conceptos; así como las principales

peculiaridades que les caracteriza a este tipo de ilícitos, los diversos medios que se utilizan para llevarlos acabo, la dificultad que existe para su investigación y comprobación, la problemática de la extraterritorialidad en su comisión, la disociación temporal, las complicaciones que presenta el Internet y las autopistas de la información al Derecho Penal, así como la cooperación conjunta de diversos países para combatir el delito informático.

En el tercer capítulo, hablaremos de las legislaciones que algunos países han adoptado para hacer frente a los delitos informáticos. Hablaremos de la regulación que se ha hecho al respeto en nuestro país; misma que presenta una problemática al carecer de una correcta regulación, debido a que los tipos penales que para el efecto fueron creados, considero que no están adecuadamente redactados, ni se encuentra ubicados en los tipos penales que corresponden, lo que en nada facilita su interpretación, trayendo consigo imposibilidad jurídica para poder aplicar las sanciones que se imponen en la legislación.

Finalmente, haremos un análisis dogmático del artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, en el que se examinarán todos y cada uno de los elementos del tipo penal y del que concluimos que no se trata de un delito equiparable a fraude, sino se trata de un delito de robo, como lo veremos a lo largo de este trabajo

Motivo por el cual consideramos apropiado proponer una reforma a este tipo penal, en donde el legislador proporcione una correcta ubicación de la conducta que se pretende tipificar, ya que en este tipo de ilícitos no puede darse un engaño a una computadora, ni mucho menos puede inducírsele a un error, por lo tanto, no puede ser equiparable al delito de fraude, cuando lo correcto es ubicarlo dentro del capítulo de robo por tratarse se un apoderamiento que se realiza por medio electrónico.

CAPÍTULO I
COMPUTADORAS

1.1. Concepto.

El mundo de la alta tecnología, nunca hubiera existido de no ser por el desarrollo de la computadora. La sociedad utiliza estas máquinas en distintos tipos y tamaños, para el almacenamiento y manipulación de datos.

Los equipos informáticos han permitido mejorar los sistemas de comunicación, pues los inevitables avances tecnológicos a nivel mundial, han logrado que las computadoras se conviertan en una de las herramientas más poderosas de la sociedad actual, haciendo posible su uso tanto en organizaciones, como en los hogares, provocando serios cambios en los individuos, algunos de índole positivo y otros de índole negativo como veremos más adelante.

Por ello resulta interesante, averiguar qué son y de dónde surgieron éstas, pues juega un papel central para la tarea humana por ser tan básicas y primordiales ya que su uso y aplicación se ha extendido a todas las ramas del saber humano. De esta forma es necesario, exponer los principales rasgos de las computadoras, ya que en realidad, no hay una definición que pueda manifestar lo que verdaderamente es la computadora, la mayoría de las personas pueden formular una imagen mental de ésta, pero las computadoras hacen muchas cosas y están diseñadas en una variedad tan amplia de formas y tamaños que resulta casi imposible describir sus características comunes en un concepto que abarque todo.

La palabra “*computer*” ha sido parte del idioma inglés desde 1646, sin embargo antes de 1940, a las máquinas que se desarrollaron para realizar cálculos se les consideraba como calculadoras y tabuladores, no como computadoras. La definición moderna y el uso del término “computadora” surgieron en los años cuarenta, cuando se desarrolló el primer dispositivo electrónico de computación.

En esencia, señala June Jamrich Parsons y Dan Oja una computadora es: "un dispositivo que acepta entrada, procesa y almacena datos y produce salida; todo ello de acuerdo con una serie de instrucciones almacenadas. La entrada de una computadora, es cualquier cosa que se ponga en un sistema de cómputo, puede proporcionarla una persona u otra computadora. Las computadoras manipulan los datos de muchas maneras y a esta manipulación se le denomina procesamiento. La mayor parte de las tareas de procesamiento, se realizan en un componente llamado unidad de procesamiento central mejor conocido como CPU que significa *Central Processing Unit*, que suele describirse como el "cerebro" de la computadora. La memoria es un área de la computadora que conserva temporalmente los datos que esperan procesamiento, almacenamiento o salida, que es el resultado producido por una computadora, por ejemplo: documentos, imágenes, etcétera."[1]

La Real Academia de la Lengua Española, define la palabra computadora de la siguiente manera:

"Computador electrónico o computadora electrónica: es aquella máquina, dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, capaz de resolver problemas aritméticos y lógicos gracias a la utilización automática de programas registrados en ella. Existen tres tipos de computadoras:

a) Analógica.- Aparato computador cuyos componentes se ajustan de modo que sus leyes físicas de funcionamiento sean análogas a las leyes matemáticas de proceso que se trata de estudiar.

b) Digital.- Aquel en que todas las magnitudes se traducen en números, con los cuales opera para realizar los cálculos.

[1] June Jamrich Parsons y Dan Oja, ***Conceptos de Computación*****,** 6ª Edición, Editorial Thomson, Traducción Eloy Pineda, México, 2004, Págs. 4, 5.

c) Híbrida.- Está compuesta de una parte analógica y otra digital y que aprovecha óptimamente las características de ambas."[2]

En la actualidad se utilizan dos tipos de computadoras: las analógicas y las digitales. Sin embargo, la mayoría de las computadoras modernas son digitales, éstas funcionan bajo el sistema binario de unos y ceros.

La Enciclopedia Científica, explica más ampliamente los tres tipos de computadoras de la siguiente manera:

"Computadora Analógica.- Es la que trabaja por medio de las funciones continuas, no calcula directamente números sino los representa mediante escalas y medidores, esto es, en la naturaleza, los fenómenos no se limitan a unas cuantas posiciones fijas de sus respectivas escalas de manifestación, sino más bien a una variación continua entre dos límites, el superior y el inferior, esos fenómenos que se comportan así reciben el nombre de analógicos. Son usadas para fines industriales, ya que en lugar de números resuelven los problemas mediante flujos de energía; por ejemplo el velocímetro de un automóvil (aguja que mide la velocidad de un vehículo).

Computadora Digital.- Es aquella que maneja y funciona interna y exclusivamente con números digitales, que es la información de manera discreta en unidades que se llaman bits (dígitos binarios).

Las computadoras digitales son máquinas destinadas a usos generales, adecuadas para tratar una gran variedad de problemas. Para su funcionamiento dependen del hecho de que cualquier número puede representarse en forma binaria y con varias combinaciones de los dígitos 1 y 0.

En general las computadoras digitales constan de cuatro partes:

---

[2] ***Diccionario de la Lengua Española, Real Academia Española***, Vol. III, 22ª edición, España, 2001, Pág. 417.

1.- La unidad de entrada, que es la parte de la computadora encargada de recibir información del exterior y conducirla hacia la sección de procesamiento.

2.- La unida de salida, es la parte que permite que los datos procesados salgan de la computadora.

3.- La unidad de memoria, es un medio de almacenamiento de datos; ahí se alojan tanto los datos procesados como las instrucciones.

4.- La unidad de control, es la sección de la computadora que dirige y coordina los procesos a realizar.

Computadora Híbrida.- Es menos común que las anteriores, usa técnicas continuamente inconstantes y técnicas digitales discretas en su funcionamiento." [3]

Actualmente disponemos de computadoras digitales de uso general de todos los tamaños desde la supercomputadora a la microcomputadora mejor conocida como laptop o portátiles. Una característica muy importante de estas máquinas, es el empleo de programas almacenados que residen en la misma memoria que los datos, han sido clasificadas según sus características de tamaño y velocidad que a continuación se detallan:

"***1.-Supercomputadoras:*** Son máquinas muy grandes y costosas, capaces de realizar millones de operaciones por segundo, una supercomputadora equivaldría a más de cien mil computadoras personales, son utilizadas en simulaciones científicas, meteorológicas, en México las supercomputadoras CRAY Y–MP4/432, CARY-SILICON GRAPHIC ORIGIN 2000, son propiedad de la Universidad Nacional Autónoma de México.

2.- Minicomputadoras: Han sido mejoradas en tamaño y capacidad, en la actualidad tienden a ser sustituidas por las redes de microcomputadoras, son pequeñas y económicas, su capacidad es adecuada para las pequeñas empresas.

[3] Enciclopedia Científica, Vol. I, Editorial Larousse, México, 1997, Págs. 277-279.

3.- Microcomputadora: Ha evolucionado con más rapidez; esta máquina es de menor dimensión, por lo que se le conoce como computadora personal, suele abreviarse "PC", la cual usa un microprocesador único, debido a su tamaño, éstas requieren de un escritorio, es el caso de la *laptop* que agrupa las computadoras de tipo portafolio; se trata de un tipo de máquinas diseñadas para cubrir las necesidades de cómputo de un individuo."[4]

Por su parte, la Enciclopedia de la Biblioteca de Consulta Microsoft Encarta, define a la computadora como "el dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información".[5]

Para el autor Julio Téllez Valdés, la computadora "es un equipo informático de tratamiento automático de datos que contiene los órganos (o elementos) necesarios para su funcionamiento autónomo."[6]

Guillermo Levine Gutiérrez, señala que la computadora: "es un aparato o un conjunto de máquinas interconectadas capaz o capaces de realizar, según un programa establecido, una sucesión de operaciones que le son suministradas y que se recuperarán en las salidas."[7] Advierte que es un sistema, que ejecuta los deseos, caprichos y veleidades de los programadores, así como sus errores y aciertos.

Como hemos visto, la definición de computadora puede ser tan variada como nuestro abundante idioma lo permita, pero la siguiente definición, es aceptada internacionalmente; según el autor George Breekman, establece que la computadora: "es una máquina electrónica, humanamente programada, capaz de

---

[4] ***Cfr.*** Vasconcelos Santillán, Jorge, ***Introducción a la Computación***, 2ª Edición, Editorial, Grupo Patria Cultural, México, 2002, Págs. 52 y 53 y June Jamrich Parsons y Dan Oja, ***Op. cit.,*** Págs. 6-8
[5] ***Biblioteca de Consulta Microsoft Encarta,*** 2002, 1993-2001, Microsoft Corporation.
[6] Téllez Valdés, Julio, ***Derecho Informático*****,** 2ª Ed., Edit. Mc Graw Hill, México, 2001, Pág. 281.
[7] Levine Gutiérrez, Guillermo, ***Introducción a la Computación***, 2ª Edición, Editorial, Mc. Graw Hill, México, 1997, Págs. 2-4.

realizar a gran velocidad cálculos matemáticos y procesos lógicos, capaz de leer, almacenar, procesar y escribir información con mucha rapidez y exactitud."[8]

Dicha definición señala que el término máquina, es una estructura mecánica capaz de desarrollar actividades que podría realizar el hombre. La idea de la computadora como cerebro electrónico es adecuada si se entiende como un mecanismo que debe ser programado para cada tarea que se quiere realizar.

Varios autores establecen que la computadora "es una máquina capaz de aceptar unos datos de entrada, efectuar con ellos operaciones lógicas y aritméticas, y proporcionar la información resultante a través de un medio de salida; todo ello sin intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en la propia computadora."[9]

Nuestra opinión es, que la computadora es la herramienta más versátil que se haya inventado, con igual facilidad nos permite escribir documentos o realizar cualquier otra tarea, como el producir películas o controlar vuelos espaciales, provocando serios cambios en los individuos, algunos de índole positivo y otros de índole negativo.

De acuerdo con lo que se ha dicho anteriormente, llegamos a la conclusión que una computadora es muy parecida a una persona, la primera coincidencia es el manejo de datos, las personas necesitamos conocimiento para desarrollar cualquier labor, de manera similar, la computadora también necesita información, que son instrucciones para convertir los datos en resultados. Como consecuencia, se requiere memoria para mantener la información durante largos períodos; la máquina guarda lo indispensable en la memoria principal, mientras que los datos muchas veces no primordiales son archivados en diskettes, discos duros o los llamados *Cd-Roms* , que es lo que se conoce como memoria externa.

---

[8] Breekman, George, ***Computación e Informática hoy*****,** Una mirada a la tecnología de mañana**,** (Traducción de Ernesto Morales Peake) Editorial Addison-Wesley Iberoamericana S.A., México 1995, Pág. 4.

[9] Consultable en http://www.geocities.com/planetamx/introducción.html/definicion.

Otra similitud muy importante es la recepción de información desde el exterior, las personas colectamos datos por medio de los sentidos: vista, oído, olfato, tacto y gusto. Las computadoras suelen recibirlos mediante un teclado y un ratón *mouse*. Las personas externamos nuestras ideas y sentimientos por medio de la voz o la escritura; las computadoras muestran resultados en una pantalla, obteniendo sus resultados a través de una impresora.

Para coordinar el flujo de información entre estos elementos se encuentra una parte de primordial importancia, en el caso humano esta tarea está a cargo del cerebro, de donde emanan nuestros pensamientos y se controlan nuestras acciones. La computadora también tiene un cerebro pero electrónico, llamado microprocesador o CPU (del inglés *Central Process Unit*), el cual se encarga del traslado de datos, operaciones aritméticas, operaciones lógicas y relacionamiento de datos; para ello basta que reciba las instrucciones apropiadas.

Como hemos visto, en las definiciones anteriores, se utilizan términos como: datos, sistema, programa, memoria, etcétera, de los cuales se hablará más adelante, para una mejor comprensión del tema.

Para concluir respecto de lo que es una computadora y de lo visto en las definiciones anteriores, hemos tomado elementos esenciales de cada una para elaborar un definición personal de lo que es una computadora, definiendo a ésta, como una máquina electrónica, que realiza funciones complejas, recibiendo todo tipo de información, la cual procesa, es decir, la ordena y una vez procesada la emite ya digerida para su interpretación, obteniendo resultados útiles como respuesta a ese procedimiento, satisfaciendo necesidades que al usuario le convengan.

1.2. Antecedentes históricos.

Desde tiempos remotos, el hombre, al verse en la necesidad de cuantificar sus pertenencias: animales, objetos de caza o armamento, pieles, habitantes, vegetales, tuvo que procesar datos, y así llevar un registro de cantidades, pues requería saber de algún modo cuántos animales había cazado o cuántos vegetales recolectaba, de cuantas armas disponía y cuántos miembros había en su clan.

En un principio este procedimiento fue muy rudimentario: utilizaba sus manos y almacenaba toda la información posible en su memoria, esto impedía un flujo fácil de la información, porque al no existir representaciones fijas de los elementos que se tenían en un proceso determinado, las conclusiones a las que llegaba resultaban ser meras especulaciones.

Esto fue superado cuando empezó a utilizar otros medios como cuentas, granos y objetos similares, para satisfacer esta necesidad tuvo que dar un gran salto intelectual y desarrollar un concepto nuevo, que fue el número, posteriormente, cuando aumentó la cantidad de pertenencias y situaciones, estas técnicas se volvieron insuficientes, por ello se vio forzado a inventar aparatos mecánicos, inventando sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez.

Con el tiempo fue mejorando el manejo de los números, pero poco a poco la complejidad de las cuentas fue aumentando, por lo que tuvo que mejorar las técnicas para contar; e incluso tuvo que inventar aparatos o herramientas que le ayudaran a su afán de cuantificar, así hasta llegar a crear una máquina capaz de realizar todo tipo de actividades, como lo es la computadora, la cual ha ido evolucionando día con día.

Entre las primeras creaciones del hombre dirigidas a facilitar las operaciones de cálculo tenemos al ábaco.

1.2.1. El ábaco.

La historia del ábaco se remonta a la época cuando el hombre se hizo agricultor y se dedicó al comercio. De ahí surgió la necesidad de contar, ayudado por sus dedos y por pequeñas piedras por lo que más tarde idearía el ábaco, el cual parece haber sido inventado por diferentes civilizaciones de manera independiente, como la hindú, egipcia, griega, china y azteca, pero se le atribuye tanto a los babilonios como a los chinos.

El ábaco, ha sido conocido y ampliamente usado por más de 2,000 años. La palabra ábaco encuentra su raíz etimológica en la voz fenicia *"abak"* que significa "tabla lista cubierta de arena", con estas tabletas de arcilla se llevaban registros de bancos y empresas de préstamos que funcionaban en aquella época.

Carlos A. Coello Coello, señala que "fue en Babilonia (hoy Irak), en el que se inventó una tabla de arcilla proveniente de Senkereh, alrededor del año 2000 a.C., que usaba para multiplicar. Se cree que quien elaboró esa tabla pudo haber usado la primera computadora digital de la historia: el ábaco, aunque señala que el uso más antiguo claramente documentado fue en China unos 500 años a.C. Los chinos, además, fueron los que le dieron al ábaco su forma moderna en el año 1200 de nuestra era, y luego lo distribuyeron a Corea, en 1400 y a Japón en 1600.

El ábaco no sólo fue un instrumento muy popular en la mayoría de las sociedades antiguas, incluyendo a los griegos, en el año 300 a.C., y los aztecas en el año 1000 de nuestra era, sino que ha sido la única computadora en resistir los embates del tiempo, pues todavía sigue en uso común entre los chinos y los japoneses."[10]

Vemos que la necesidad de contar, llevó al hombre a la creación del primer dispositivo mecánico, el ábaco, este invento aparece de forma

[10] ***Cfr.*** Coello Coello, Carlos A., ***Breve historia de la computación y sus pioneros,*** Editorial, Fondo de Cultura Económica, México, 2003, Pág. 22 y Freedman, Alan, ***Glosario de Computación*****,** 3ª Edición, Editorial, Mc Graw Hill, (Traducción de María de Lourdes Fournier García) México, 1985, Págs. 69-75.

independiente en varias culturas de la antigüedad, toda vez que su origen es incierto, aunque generalmente se ha atribuido el crédito de su realización al pueblo babilónico. El ábaco lo podemos describir como un palo de madera que sostiene alambres paralelos en los que se atan cuentas que el usuario debe memorizar, en base a estas, todas las operaciones de la aritmética ordinaria pueden realizarse.

1.2.2. Tabla de logaritmos (1614).

La dificultad para realizar operaciones de multiplicación y división motivó al matemático John Napier a crear un nuevo método que redujera de manera notable ese trabajo. Así fue como surgieron las tablas de logaritmos, a través de las cuales es posible realizar multiplicaciones en forma sencilla y rápida.

John Napier descubre la relación entre series aritméticas y geométricas, creando tablas que él llama logaritmos. Edmund Gunter se encarga de marcar los logaritmos de Napier en líneas. Bissaker por su parte coloca las líneas de Napier y Gunter sobre un pedazo de madera, creando de esta manera la regla de cálculo, la cual es perfeccionada, convirtiéndose en una calculadora de bolsillo, extremadamente versátil.

"Los logaritmos son números que están relacionados de tal modo con los números cotidianos que convierten las multiplicaciones en sumas y las divisiones en restas. Sin embargo, había que crear las tablas y sus antilogaritmos e imprimirlas, pero esto representaba un enorme trabajo, no obstante las tablas tuvieron errores que fueron detectados tiempo después."[11]

Esta herramienta permitió una notable simplificación de las principales operaciones aritméticas, por lo que consideramos que John Napier hizo dos contribuciones al campo de las matemáticas, inventó logaritmos y un dispositivo para multiplicar y dividir, que es la tabla de logaritmos, la cual estaba conformada

[11] ***Cfr.*** Prieto Espinosa Alberto y otros, ***Introducción a la informática***, 3ª Edición, Editorial Mc. Graw Hill, España, 2002, Pág. 676.

con varillas dividida en diez cuadros, estas varillas se construían con huesos, de modo que se les llamó huesos de Napier.

1.2.3. Regla de cálculo (1630).

Poco tiempo después de que Napier inventó la tabla de logaritmos, surgió otro nuevo inventó, menos exacto pero mucho más fácil de utilizar: la regla de cálculo.

"Ésta funciona con base a la medición de longitudes entre dos reglas que guardan relación, deslizándose una sobre la otra, cada regla tiene marcados varios números; es por esto que los desplazamientos se traducen en multiplicaciones o divisiones, según el sentido del movimiento.

Los resultados de las operaciones que se realizan con ella se aproximan con suficiente exactitud; sin embargo, es hasta estos últimos años que ha sido desplazada por las calculadoras electrónicas de bolsillo."[12]

Esta regla fue fruto directo de los logaritmos, prestó un gran servicio para los cálculos de ingenieros y científicos, esta regla de cálculo ha sido sustituida casi por completo por la calculadora electrónica portátil.

1.2.4. La máquina de Pascal (1642).

Décadas después, el científico francés Blaise Pascal inventó y construyó la primera sumadora mecánica de la historia, llamada *Pascalina*, para ayudar a su padre, un cobrador de impuestos, a calcular las entradas por contribuciones.

La máquina de Pascal, consistía en "un sistema de ruedas engranadas, en cada una de la cuales estaban marcados los dígitos del cero al nueve. Cada vez que una regla completaba una vuelta, la siguiente a la izquierda caminaba un elemento y así sucesivamente, dando como resultado la suma de varias

[12] ***Idem.***

cantidades. A esta sumadora se le considera como la primera máquina de calcular construida por el hombre."[13]

Pascal fue enaltecido por toda Europa debido a sus logros, sin embargo la Pascalina resultó un desconsolador fallo financiero, pues para ese momento, resultaba muy costosa. La máquina de Pascal se trataba de una serie de engranes en una caja, que proporcionaban resultados de operaciones de suma y resta en forma directa mostrando un número a través de una ventanita y por este simple hecho tiene la ventaja de que evita tener que contar, como en el ábaco, además presenta los resultados en forma más accesible y directa; consideramos que éste dispositivo era considerablemente más complejo, sólo era capaz de sumar, ya que para restar se dice que requería de una técnica especial que limitaba su uso de manera considerable.

1.2.5. La tarjeta perforada (1804).

Durante el siglo XVIII la industria textil británica creció mucho, en buena medida gracias a los telares mecánicos automáticos. "Hacia 1804, con una industria en pleno desarrollo, el tejedor francés Joseph Jacquard construyó una máquina para tejer complicados diseños de telas, esta máquina funcionaba con tarjetas perforadas que contenían información del camino que debía seguir los hilos de la tela para lograr un diseño determinado.

En estas tarjetas se podía representar la respuesta sí, a una pregunta mediante una perforación en un lugar determinado de la tarjeta y la respuesta no, con la ausencia de dicha perforación. La gran ventaja del tratamiento de la información mediante estas tarjetas consiste en que, una vez registrados los datos

[13] Arechiga Gallegos Jorge, y otros, ***Fundamentos de la Computación***, 2ª Edición, Editorial Limusa, México, 1978, Pág. 7.

en las mismas, es posible manejarlas por medios mecánicos todas las veces que hagan falta y a una gran velocidad."[14]

Este invento no estuvo relacionado con las máquinas de calcular, sin embargo, la idea de usar tarjetas perforadas para representar información sería aprovechada años más tarde por Charles Babbage y Hermann Hollerith.

Es importante resaltar que la tarjeta perforada tuvo grandes repercusiones; introdujo la automatización y con ella Joseph Jacquard se convirtió en el padre de las tarjetas perforadas, que habían dado nacimiento a la industria de los telares mecánicos durante la Revolución Industrial pues de esta forma consideramos que favoreció a la industria textil, pues la elaboración de telas ya no requirió del trabajo manual, sino de los telares mecánicos automáticos.

1.2.6. La máquina de Babbage (1834).

"Hasta el siglo XIX las calculadoras sólo servían para una aplicación única, pero en 1834 el matemático e inventor inglés Charles Babbage introdujo un nuevo concepto: resolver diferentes problemas con la misma máquina. Fue uno de los notables contribuyentes de las máquinas de cálculo, obtuvo el apoyo de su gobierno para realizar una máquina que fuera capaz de efectuar cálculos complejos y de esta forma eliminar los errores en que frecuentemente se incurría en las tablas de logaritmos."[15]

La máquina analítica estaba dividida funcionalmente en dos grandes partes: "una que ordenaba y otra que ejecutaba las órdenes. La que ejecutaba las órdenes era una versión muy amplia de la máquina de Pascal, mientras que la otra era la parte clave."[16]

La innovación consistía en que el usuario podía, cambiando las especificaciones del control, lograr que la misma máquina ejecutara operaciones

[14] ***Cfr*.** Vasconcelos Santillán, Jorge, y otros, ***Estampas de la Ciencia***, Editorial Fondo de Cultura Económica, México, 1999, Págs. 180-184, y Téllez Valdés, Julio, ***Op. cit.,*** Págs. 6-7.
[15] Téllez Valdés, Julio, ***Op. cit.,*** Págs. 8.
[16] Prieto Espinosa Alberto y otros, ***Op. cit.,*** Pág. 654.

complejas, diferentes de las que había hecho antes, ésta contaba también con una sección en la que se recibían los datos con los que se iba a trabajar. La máquina seguía instrucciones dadas por la unidad de control, las cuales indicaban qué hacer con los datos de entrada, para obtener luego los resultados deseados.

"Fue así, que Babbage ideó una "máquina analítica" que sería capaz de ejecutar procesos más complicados como la multiplicación y la división, almacenando resultados en un dispositivo interno, contaba con las tablas de logaritmos, efectuaba decisiones simples y finalmente entregaba un resultado impreso de manera automática."[17]

La máquina analítica, habría sido una auténtica computadora programable si el proyecto hubiera contado con la financiación adecuada, no obstante, a pesar de esa utilidad que representaría este proyecto, el trabajo no pudo concluirse, pues desafortunadamente el invento de Babbage fue superior a la capacidad técnica de su época y por lo tanto no pudo realizarse.

Sin embargo, debemos mencionar que la máquina de Babbage fue determinante en el desarrollo de las computadoras actuales, los historiadores computacionales creen que el diseño de ésta encarnó muchos de los conceptos que definen la computadora moderna, al introducir conceptos como memoria, impresora, tarjetas perforadas y el control de programas secuénciales.

1.2.7. El código de Herman Hollerith (1880).

El año de 1880 fue el principio de la época moderna de la tarjeta perforada. "En ese año Herman Hollerith, trabajaba en la oficina de Censos de los Estados Unidos como agente especial para acelerar el procedimiento de los datos en los padrones. Se usaron métodos manuales da tabulación para el recuento de una población de cincuenta millones de habitantes y fueron completamente

[17] Long Larry, ***Introducción a las computadoras y al procesamiento de información***, 2ª Edición, Editorial Hispanoamericana, México, 1990, Pág. 31.

inadecuados. Fue así, que Herman Hollerith se propuso mecanizar la operación de los censos. Para 1887 había completado un sistema que empleaba el principio de la tarjeta perforada; aunque la primera máquina utilizaba tiras de papel con agujeros perforados de acuerdo con una clave, las tiras de papel resultaron pocas prácticas, así que desarrolló una tarjeta de tamaño normal, en la que se registrarían los datos de cada persona, haciendo perforaciones en lugares específicos y después otra máquina leería las tarjetas y sumaría los datos."[18]

Su invento resultó tan exitoso que en 1896 Hollerith fundó su propia empresa: la Compañía de Máquinas Tabuladoras (T abulating Machine Company), para desarrollar sus máquinas y venderlas al público. En 1901 presentó la forma básica de un teclado perforador numérico y se hicieron otras mejoras al sistema, con esto, además se desarrollo máquinas capaces de ordenar automáticamente sus tarjetas.

Algunos años después esta compañía se transformaría en la *International Business Machines*, mejor conocida como IBM. Con su máquina tabuladora, Hollerith introdujo un nuevo concepto: el procesamiento de datos, esto es, movilizar, almacenar y contabilizar grandes cantidades de datos, además de hacer cálculos. Este nuevo concepto constituyó la introducción de tarjetas perforadas como elemento de tabulación lo que llevaría a lo que es hoy la moderna computadora.

1.3. Evolución de las computadoras.

Durante las primeras décadas del siglo XX se construyeron grandes calculadoras automáticas, las últimas antes del surgimiento de las computadoras electrónicas.

[18] Levine Gutiérrez, Guillermo, ***Op. cit.,*** Págs. 3-5.

a) La MARK I (1937-1944).

"El profesor Howard Aike, de la Universidad de Harvard, desarrolló la computadora Mark I, cuya denominación oficial fue: Automatic Sequence Controlled (Calculador Automático de Secuencia Controlada), que fue la primera máquina que llevó a la realidad el sueño de Babbage, con el apoyo de la IBM a finales de la década de los treinta y principios de los cuarenta.

Fue la primera computadora electromecánica automática, era capaz de realizar largas secuencias de operaciones codificadas, registrándolas en una cinta de papel perforada y calculando los resultados con la ayuda de las unidades de almacenamiento (memoria), imprimiendo resultados en un teletipo. No obstante, esta máquina era relativamente lenta, ya que su velocidad de operación dependía de la rapidez de sus numerosos componentes. Siendo utilizada durante quince años."[19]

La MARK I marca la fecha del la primera computadora que se pone en funcionamiento, es la primera máquina procesadora de información. Funcionaba eléctricamente, las instrucciones e información se introducen en ella por medio de tarjetas perforadas, realizaba sumas, multiplicaciones y operaciones logarítmicas en poco más de un minuto.

A pesar de su peso y su lentitud comparada con los equipos actuales, fue la primera máquina en poseer todas las características de una verdadera computadora, pero los historiadores han establecido que la Mark I se aparta de manera considerable de la ruta del desarrollo que llevó a las computadoras modernas, era digital pero usaba representación decimal, en lugar de la binaria que se aplica en las computadoras actuales.

[19] Long Larry, ***Op. cit,*** Pág. 37.

b) La ENIAC (1937-1945).

El ejército y la Universidad de Pennsylvania, trabajaron en el diseño y construcción de una calculadora que fuera electrónica y automática conocida como la ENIAC (Electronic Numerical Integrator and Calculator), era capaz de realizar cinco mil operaciones por segundos y fue utilizada principalmente para resolver problemas de balística y aeronáutica.

La ENIAC, fue reconocida como la primera computadora digital completamente electrónica de propósitos generales, señaló el comienzo de la primera generación de computadoras, sus inventores fueron, J. Presper Eckert y el Dr. John W. Mauchly. El proyectó culminó dos años después, cuando se integró a ese equipo el ingeniero y matemático, John von Neumann.

Su mayor mérito fue el de tener gran cantidad de componentes y trabajar con ellos; sin embargo, era demasiado grande, ocupaba todo un sótano, consumía mucha energía eléctrica, requería todo un sistema de aire acondicionado industrial y se calentaba con mucha rapidez, pero con ésta se inauguró una nueva etapa en las capacidades de procesamiento de datos.

La ENIAC fue mil veces más veloz que sus predecesoras, se presentó como un importante descubrimiento en la tecnología de la computación, ingresar un nuevo programa era un proceso muy tedioso que requería días o incluso semanas, pero era capaz de efectuar alrededor de cinco mil operaciones aritméticas en un segundo, dejando atrás las limitaciones humanas de velocidad y precisión e inaugurando una nueva etapa en las capacidades de procesamiento de datos.

c) La EDVAC (1945-1952).

“En 1945, el matemático John von Neumann, estudió cuidadosamente el diseño de la ENIAC y elaboró un informe con el cual sentó las bases de las modernas computadoras digitales. La primera computadora que se construyó bajo el modelo de von Neumann fue la llamada EDVAC (Electronic Discrete Variable

Computer o computadora electrónica de variable discreta), que era capaz de realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente."[20]

John von Neumann, estableció que la computadora debería funcionar conforme el sistema de numeración binario, es decir, almacenar y procesar datos en formas de unos y ceros. La propuesta de von Neumann abarcó aún más: la computadora debería tener un módulo para hacer las operaciones aritméticas, otro para controlar el funcionamiento siguiendo instrucciones, uno más que sería la memoria y varios dispositivos de entrada de datos, así como para salida de resultados.

Consideramos que la propuesta de von Neumann, permitió que en la memoria de la máquina coexistieran datos con instrucciones, para que entonces la computadora pudiera ser programada de tal manera que fuera manejable y no por medio de alambres que eléctricamente interconectaban varias secciones del control. Alrededor de este concepto gira toda la evolución posterior de la industria y la ciencia de la computación.

El desarrollo de las computadoras suele dividirse en ***generaciones***. El criterio para determinar cuándo se da el cambio de una generación a otra no está claramente definido, pero resulta aparente que deben cumplirse al menos dos requisitos estructurales:

1) Forma en que están construidas: que haya tenido cambios sustanciales, (como es la arquitectura global del sistema, tecnología electrónica).

2) Forma en la que el ser humano se comunica con ellas: que haya experimentado progresos importantes, (programas básicos, sistema operativo, lenguajes, es decir, cómo se entabla la comunicación con ella).

[20] ***Cfr.*** Long Larry, ***Op. cit,*** Pág. 35-36.

En lo que respecta al primer requisito, los cambios han sido drásticos en el corto lapso que tienen de existencia las computadoras, mientras que el avance en relación con el segundo requisito, ha sido más cauteloso, sin embargo, cabe mencionar que entre las actuales computadoras y las de hace diez años no hay diferencia sustancial alguna, la comunicación entre el usuario y la máquina sólo se ha vuelto más cómoda y conveniente.

1.3.1. Primera Generación.

Los comienzos de la industria de la computación se caracterizan por un gran desconocimiento de las capacidades y alcances de las computadoras. Esta primera etapa abarcó la década de 1950 y se conoce como la primera generación de las computadoras. Las máquinas de esta generación se caracterizan por los siguientes requisitos:

A) Por el uso de circuitos de tubos de vacío, para procesar la información.
B) Uso de las tarjetas perforadas para la entrada de datos y programas.
C) Empleo de cilindros magnéticos para almacenar información e instrucciones internas.
D) Se lleva a cabo mediante la programación en lenguaje de máquina (que era el lenguaje binario).

En esta etapa, Eckert y Mauchly junto con una compañía privada la Remington Rand Corporation, contribuyeron al desarrolló de la UNIVAC I (Universal Automtatic Computer), que fue la primer computadora de uso comercial y que apareció en 1951, ésta máquina marcó el inicio de la era informática, se caracterizó por procesar letras, símbolos y números, por el uso de un programa especial capaz de traducir programas en el lenguaje particular a un lenguaje de máquina.

Como consecuencia eran demasiado voluminosas, consumían mucha energía y producían calor; no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno pero

limitado. A la UNIVAC I, le continuaron otros modelos de máquinas desarrolladas por la compañía IBM, (International Business Machines), con esto IBM se consolidaba como líder en la fabricación de computadoras.

Esta primera generación, se caracterizó por tener máquinas grandes y pesadas, así como por el alto consumo de energía, además de no tener sistemas operativos como los conocemos hoy en día, siendo la UNIVAC, la computadora representativa de ésta generación, con esto se inició la fabricación de computadoras en serie.

1.3.2. Segunda Generación.

Las computadoras seguían en constante evolución, reduciendo de tamaño y aumentando sus capacidades de procesamiento. Al mismo tiempo se iba definiendo con mayor claridad toda una nueva ciencia: la de comunicarse con las computadoras, que recibiera el nombre de programación de sistemas.

En esta etapa se habla de la segunda generación de computadoras, que se caracterizan por los siguientes aspectos:

A) Usaban circuitos transistores para almacenar información.

B) Se programan en nuevos lenguajes llamados lenguajes de alto nivel o lenguajes de programación.

C) Empleo de anillos magnéticos para almacenar información.

En general, las computadoras de la segunda generación no sólo fueron de tamaño más reducido, sino también su precio; esto permitió mayores ventas y el surgimiento de nuevas empresas, pues el invento del transistor hizo posible una nueva generación de computadoras, más rápidas, más pequeñas, con menos necesidades de ventilación, menos costosas y producían menos calor. Esto hizo, que hubiera más competencia y que la tecnología de las máquinas fuera cada vez más avanzada, ésta generación duró poco tiempo, porque pronto hubo nuevos avances, el hecho fundamental que marcó esta etapa fue la incorporación del transistor a las computadoras sustituyendo los bulbos, sin embargo consideramos

que debe ser considerada como una transición entre las máquinas electrónicas, que nadie sabía con precisión para qué podrían ser útiles y el actual concepto de computadora.

Esta generación se caracterizó por la disponibilidad de lenguajes de programación computacional de lato nivel que permitió el desarrollo del software y esa capacidad consideramos que fue fundamental para el nacimiento de la industria del software.

1.3.3. Tercera generación.

Con la aparición de nuevas y mejores maneras de comunicarse con las computadoras, junto con los progresos en la electrónica, surge la que se conoce como la tercera generación de computadoras, a mediados de la década de 1960.

A mediados de la década de 1970 (en plena tercera generación), surge un gran mercado para las computadoras de tamaño mediano, o las llamadas ***"minicomputadoras"*** que no son tan costosas como las grandes máquinas, pero que ya disponen de una gran capacidad de proceso.

Las computadoras de esta generación manejaron técnicas, por lo que alcanzaron un éxito enorme a tal grado que la gente en general, pronto llegó a identificar el concepto de computadora con el nombre de IBM, por ser esta compañía quien utilizara este tipo de técnicas.

Las características estructurales de la tercera generación son:

A) Su fabricación electrónica está basada en circuitos integrados y son conocidos también por su nombre popular en inglés como *"chips"*, para almacenar y procesar la información.

B) Su manejo es por medio de los lenguajes de control de los sistemas operativos.

Las computadoras se tornaban más pequeñas, más ligeras y más eficientes, consumían menos electricidad, por lo tanto generaban menos calor, trabajaban a tal velocidad que proporcionaban la capacidad de correr más de un programa de manera simultánea.

Esta fue una época de pleno desarrollo acelerado y de competencia por los mercados internacionales, ya que la industria de la computación había tenido grandes avances. A partir de la tercera generación, los avances en la industria de la computación han sido tan numerosos y frecuentes que de alguna manera han hecho que el hombre de nuestro tiempo pierda su capacidad de asombro. Las computadoras han invadido la industria, el comercio, la administración, la educación y han llegado hasta nuestros hogares, constituyéndose esta industria de gran importancia en el mundo.

1.3.4. Cuarta Generación.

El adelanto de la microelectrónica prosigue a una velocidad impresionante, y ya por el año 1972 surge en le mercado una nueva familia de microprocesadores que permitió la fabricación de las llamadas ***"microcomputadoras"***, es decir, computadoras personales o PC, son extremadamente pequeñas y baratas, por lo que dieron un tremendo impulso a la industria de la computación, pues la obligaron a mejorar los equipos y sus accesorios.

Hoy en día hay microprocesadores en muchos aparatos de uso común, como relojes, televisores, hornos, juguetes, etc., y naturalmente, en toda una nueva generación de máquinas.

La popularidad de estas máquinas se debió a que el usuario no requería ser un especialista en cómputo; el equipo era de fácil manejo, bastaba conectarlo a un televisor y a una grabadora de cassettes y se programaba con un sencillo lenguaje.

La compañía IBM logró convencer a las personas de que la computadora personal tenía grandes ventajas en la industria, en la administración y en el hogar.

La PC se convirtió en el modelo a seguir en sólo 18 meses y ha influido poderosamente sobre la percepción que la sociedad en general tiene sobre la llamada "revolución informática", porque los sistemas que en las computadoras se manejan han tenido un considerable avance, haciendo más interactiva la comunicación con el usuario.

Es necesario mencionar que desde hace tiempo algunos especialistas en computación ya hablaban de la idea de desarrollar programas que le permitan a la computadora realizar funciones relacionadas con la inteligencia humana, como aprender a solucionar problemas o entender el habla, los cuales actualmente ya existen.

1.3.5. Quinta Generación.

La sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo de sistemas con los que se manejan las computadoras. Ha surgido un interesante fenómeno de competencia internacional por el dominio del gigantesco mercado de la computación, sin embargo, no se ha podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora mediante el lenguaje natural y no a través de códigos o lenguajes de control especializados.

Con esta idea, Japón se propuso desarrollar el "programa de la quinta generación de computadoras", el que construiría computadoras con inteligencia artificial para 1990. Pero el plazo venció y los resultados obtenidos por los japoneses distaron mucho de las expectativas que generaron.

El futuro previsible de la computación es muy interesante, y se pude esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.

1.4. Nuestra opinión.

La historia de las computadoras tiene un significado especial para nosotros, porque muchos de los sucesos más importantes han ocurrido a lo largo de nuestra vida. Las últimas décadas han sido la parte más interesante de la computadora, si se toma en cuenta la manera en que la gente vive y trabaja, el invento de la computadora puede considerarse como uno de los sucesos más significativos de la historia.

El panorama general que dimos de la historia de la computadora, proporciona una perspectiva histórica y una idea de lo que son las raíces de la computadora moderna. Pues al igual que otros inventos, la historia de la computadora evolucionó a medida que los inventores creaban diversos dispositivos, los seres humanos empleaban auxiliares para contar, como piedras palos para llevar registro de ciertas cantidades por ejemplo, el número de animales cazados, los vegetales recolectados y muchas otras necesidades que aparecieron al evolucionar la humanidad, sin embargo muchas transacciones requerían cálculos.

Así pues el primer concepto que desarrolló el hombre fue el número, como respuesta a la necesidad de controlar sus pertenencias. Tiempo después sistematizó el manejo de los números y con posterioridad, se apoyó en objetos materiales para facilitar el proceso de contar. Cuando aumentó la cantidad de pertenencias y situaciones, estas técnicas se volvieron insuficientes, por ello el hombre se vio forzado a inventar aparatos mecánicos y a mejorar las técnicas para facilitar el cálculo numérico.

El desarrollo de lo que hoy conocemos como computadora se fue formando desde aquellas primera herramientas que el hombre inventó con el objetivo de poder realizar cálculos de una manera más sencilla y rápida y que hoy en día han abierto una nueva era permitiendo mejorar los sistemas de comunicación, convirtiéndose en una de las herramientas más poderosas de las sociedad actual.

1.5. Conceptos fundamentales.

Lo anterior hace necesario que hablemos de algunos conceptos que son fundamentales para entender como funciona la computadora.

1.5.1. Internet.

Hacia los años sesenta, cuando el número de computadoras ya era considerable, surgió el interés en conectarlas entre sí y de ese modo formar una red para compartir la información que obtuviesen.

Esta idea fue desarrollada especialmente por el gobierno de los Estados Unidos, preocupado por mantener las comunicaciones militares en caso de un ataque nuclear; a principios de 1970 ya tenía funcionando las primeras redes que enlazaban diferentes partes del país.

“Por dos décadas el acceso a las redes estuvo prácticamente limitado a las grandes computadoras institucionales. Sin embargo, poco después de su aparición, las computadoras personales fueron incorporadas a las grandes redes, lo que provocó su crecimiento desmedido. Al unirse esas redes surgió la "red de redes", conocida como *Internet*, que conecta a millones de usuarios del mundo.

La tecnología actual permitió que Internet se convirtiera en una supercarretera de la información, pues abrió la puerta para que muchas personas tuvieran acceso a los más variados documentos, sonidos, imágenes. Además, ofreció toda una gama de servicios: comunicaciones, ventas, intercambio de ideas, y mucho más.”[21]

June Jamrich Parsons y Dan Oja, definen al Internet, “como la interconexión de redes informáticas que permite a las computadoras comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de

[21] Leal Güemez Regina y otros, ***Fundamentos de computación,*** Edit. Trillas, México, 2000, Pág.18.

organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados *intranet,* por lo general es para servicios de comunicación interna de un negocio o de una organización y su uso está limitado a los empleados del negocio.

Los recursos que proporciona Internet, son los llamados sitios Web (abreviatura de World Wide Web, telaraña mundial), es un conjunto de archivos organizados como hipertexto gigante, muchos de estos archivos producen documentos denominados páginas Web que son lugares del ciberespacio que corresponden a las oficinas, las tiendas, la revista, etcétera, proporciona información o acceso a otros recursos, como correo electrónico mejor conocido como e-mail, que permite a una persona enviar un mensaje electrónico a otra persona o a un grupo de personas, estos archivos contienen fotografías, videos, animaciones y sonidos."[22]

Se consideran que Internet, es una red de líneas de comunicación interconectadas que crean una especie de sistema de supracarretera para el transporte de datos, construidas y mantenidas por las principales compañías de telecomunicaciones, que son las que mueven enormes cantidades de datos a velocidades increíbles, además de que abarca un conjunto de líneas de comunicación regionales y locales, entre éstas se incluyen sistemas de telefonía local, líneas de televisión por cable, sistemas de telefonía celular y antenas parabólicas personales.

El sistema de comunicaciones de Internet, transporta datos entre millones de computadoras y otros dispositivos electrónicos, casi todo el material accesible está almacenado en servidores, que son propiedad y reciben mantenimiento de oficinas gubernamentales, corporaciones, pequeñas empresas, escuelas, organizaciones e incluso individuos. Estos servidores usan software, especiales para servidores, que permiten localizar y distribuir datos solicitados por los usuarios.

[22] ***Cfr.*** June Jamrich Parsons y Dan Oja, ***Op. cit.,*** Pág. 15.

La tecnología de Internet es precursora de la llamada superautopista de la información, un objetivo teórico de las comunicaciones informáticas que permitiría proporcionar a colegios, bibliotecas, empresas y hogares acceso universal a una información de calidad que eduque, informe y entretenga. A finales de 1998 estaban conectados a Internet unos 148 millones de ordenadores, y la cifra sigue en aumento.

"Los sistemas de redes como Internet permiten intercambiar información entre computadoras, y ya se han creado numerosos servicios que aprovechan esta función. Entre ellos figuran los siguientes: conectarse a un ordenador desde otro lugar (*telnet*); transferir ficheros entre una computadora local y una computadora remota, leer e interpretar ficheros de ordenadores remotos (*gopher*).

El servicio de Internet más reciente e importante es el protocolo de transferencia de hipertexto (http), un descendiente del servicio de gopher. El http puede leer e interpretar ficheros de una máquina remota: no sólo texto sino imágenes, sonidos o secuencias de vídeo. El http es el protocolo de transferencia de información que forma la base de la colección de información distribuida denominada *World Wide Web*,(también conocida como Web o WWW) es una colección de archivos, que incluyen información en forma de textos, gráficos, sonidos y vídeos, además de vínculos con otros archivos."[23]

"Las principales aplicaciones del Internet, son la comunicación personal, la distribución y recuperación de documentos, así como las transacciones comerciales, que se realizan a través del *World Wide Web*, (www) un servicio de búsqueda y recuperación de datos. Estos componentes en realidad son archivos localizados en los servidores Web que contienen un tipo de información específico, en texto, imagen, sonido, voz o video, y es transportado hasta la

[23] Biblioteca de Consulta Microsoft Encarta, ***Op. Cit.***

computadora del usuario donde un navegador de Internet interpreta los datos y los convierte nuevamente en texto, imagen o sonido."[24]

De lo anterior, concluimos que el servicio de Internet, nos permite enlazar diferentes redes, de modo que los datos localizados en una pueden ser aprovechados por otra sin importar la distancia que las separa o los componentes que las conforman. En la actualidad, Internet integra muchas redes independientes, universitarias, empresariales, gubernamentales, y particulares, lo que produce una gran diversidad y riqueza de información disponible en prácticamente cualquier lugar del mundo.

Es importante destacar, que Internet tiene una ventaja respecto otros medios de comunicación, el usuario selecciona la información que desea ver, además brinda acceso a una amplísima gama de datos que van desde los avances científicos, hasta las últimas noticias del momento.

Sin embargo, junto con sus múltiples beneficios, Internet también ha resultado un eficiente vehículo para conductas delictivas como lo veremos más adelante, o simplemente para la propagación de virus informáticos muchos de ellos antes de atacar la computadora en que se hospedan, se duplican a sí mismos y se diseminan, logrando así afectar a una gran cantidad de usuarios.

1.5.2. Base de datos.

"El término base de datos puede usarse como sinónimo de banco de datos o banco de información, y se refiere a un conjunto de archivos organizados de tal forma que permitan guardar y extraer información útil por medio de la ejecución de programas especiales.

Un dato es todo aquello susceptible de ser captado por la mente, como los datos no son objetos sólidos, para que se puedan almacenar y propagar deben adaptarse a las características del medio adecuado para su captación, además,

[24] Consultable en: http://www.geocities.com/definicion/internet.html.

representarse de una manera adecuada para que la información no vaya a perderse, en la actualidad el proceso de datos se hace en su mayoría con señales digitales, que es cuando el medio físico donde se produce cambia en forma discreta."[25]

De acuerdo con Vasconcelos Santillán, también podemos referirnos de forma más técnica a un sistema de uso general que sirve para crear y mantener bancos de datos sin necesidad de escribir programas específicos para manejarlos, sino usando las facilidades integradas a un sistema complejo que se encarga de interrelacionar los diversos archivos de un banco de información, para que éste se comporte como si estuviera dotado de cierta inteligencia que le permite responder preguntas acerca de sus contenidos.

Para comprender la razón de las bases de datos, es necesario antes hacer una distinción básica entre datos e información.

Por **datos** se entiende la representación de números y letras o palabras, mientras que por **información** se entiende esos mismos datos más las relaciones estructurales entre ellos, o sea puede haber datos sin información (simples números), pero no puede haber información sin datos, pues la información se extrae de los datos mediante relaciones explícitas que se proponen.

Jorge Vasconcelos Santillán define a la base de datos como "el grupo de archivos relacionados, que se caracteriza por un manejo eficiente de los datos de tal forma que evite la repetición de datos y facilita un manejo eficiente de los mismos."[26]

Consideramos que una base de datos, es un programa precisamente de datos que tiene como función virtualizar el manejo de archivos para permitir el acceso a la información, mediante esta base es posible procesar archivos guiados por el significado de sus contenidos, está diseñado para facilitar el acceso a la

[25] ***Cfr.*** Vasconcelos Santillán, ***Introducción a la Computación, Op. cit.***, Págs. 12, 16.
[26] Vasconcelos Santillán, Jorge, ***Introducción a la Computación, Parte II***, Editorial, Grupo Patria Cultural, México, 1999, Pág. 321.

información almacenada en la computadora; los datos suelen aparecer en forma de texto, números o gráficos.

1.5.3. Hacker.

Un hacker (del inglés *hack*, recortar) es el neologismo utilizado para referirse a un experto en programación que puede conseguir de un sistema informático cosas que sus creadores no imaginan; así, es capaz de pensar y hacer cosas que parecen "magia" con los ordenadores. Se suele llamar *hackeo* y *hackear* a las obras propias de un hacker.

"El término también se utiliza para referirse a diversas personas que utilizan programas de cómputo, como son:

- Aficionados a la informática que buscan defectos, puertas traseras y mejorar la seguridad del software, así como prevenir posibles errores en el futuro.
- Delincuentes informáticos, o crackers, que es su uso más extendido, y que sería incorrecto, según los propios hackers."[27]

Se dice que el término de hacker, nació a finales de la década de 1970, las computadoras de Stanford y Massachusetts Institute of Technology (MIT), atrajeron comunidades informales de fanáticos de las computadoras quienes se autodenominaron *hackers*, en esos días un hacker era una persona que disfrutaba aprendiendo los detalles de los sistemas de computación y escribiendo programas ingeniosos, llamados *hacks*, en su mayor parte, los hackers eran curiosos, entusiastas, inteligentes, idealistas, excéntricos e inofensivos, de hecho se dice que muchos de esos primeros hackers fueron los arquitectos de la revolución de las microcomputadoras, el estereotipo del hacker actual, es aquella persona que ingresa ilegalmente a las computadoras.

Por su puesto, no todas las personas ingresan ilegalmente a sistemas de computación, ni todas las personas que acceden sin autorización a otros sistemas

[27] Consultable en http://www.iespana.es/canalhanoi/articuloshackers.htm.

se ajustan al mencionado estereotipo, los que ingresan ilegalmente usan contraseñas robadas o deficiencias de seguridad en el software del sistema operativo, en ocasiones se enlazan directamente con módems por vía telefónica con las computadoras objetivo, entre otros casos viajan a través de Internet y otras redes, algunos se valen de caballos de Troya, bombas lógicas y otros trucos para hacer estropicios en sistemas corporativos y gubernamentales, una vez que han logrado ingresar en un sistema , curiosean y se van sin dejar huellas digitales electrónicas.

En la década de 1980, con la llegada de las computadoras personales, y posteriormente con la posibilidad de conexión a los grandes sistemas de ordenadores a través de Internet, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar o alterar los programas o los datos almacenados en las mismas.

Por lo que definimos al *hacker*, como aquel usuario que por su elevado nivel de conocimientos técnicos, son capaces de superar determinadas medidas de protección, es decir, son aficionados a los ordenadores o computadoras, totalmente cautivados por la programación y la tecnología informática, cometiendo un acto ilícito, ya que utiliza el acceso indebido a un sistema de información.

Existen distintas manifestaciones tales como son los crackers, phreaker, piratas informáticos, script kiddie, lamer, que a continuación se da una breve explicación de las actividades que éstos realizan, para una mejor comprensión del tema.

1.5.3.1. Crackers.

Del inglés *crack*, romper. Es un término creado alrededor de 1985 por hackers como defensa por el uso incorrecto del término hacker.

Se considera que la actividad del cracker es ilegal, también se considera como cracker a aquella persona que diseña y programa cracks informáticos.

Un crack es un parche informático, creado sin conocer el código fuente del programa, cuya finalidad es la de modificar el comportamiento del software original. Generalmente, el crack elimina limitaciones que fueron impuestas por el autor para evitar su copia ilegal.

Por lo tanto un cracker es alguien que viola la seguridad de un sistema informático con fines de beneficio personal o mera diversión, de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal.

1.5.3.2. Phreaker.

Un phreaker es una persona que interfiere en los sistemas telefónicos, de forma ilegal, mediante el uso de tecnología para poder obtener algún tipo de beneficio. El término proviene de las palabras *phone+phreak+hacker* (telefono+loco+hacker) y surgió en los Estados Unidos en los años 60.

"El primer phreaker, conocido como *Capitán Crunch*, empleaba un silbato para poder lograr sus objetivos. De ahí que los primeros phreakers usaban silbatos que emitían una frecuencia de 2600 HZ, para poder engañar a la compañía telefónica Bell. Durante muchos años los phreakers usaron las llamadas *boxes*, artefactos que provocaban diversas anomalías en la línea telefónica, estos dispositivos se conocen por un color identificativo *blue boxes* (artefactos azules), *black boxes* (artefactos negros), *beige boxes* (artefactos beige)."[28]

En la actualidad, los phreakers tienen también como blanco a la telefonía móvil y a las tecnologías inalámbricas.

[28] Consultable en: http://es.wikipedia.org/wiki/Phreaker.

1.5.3.3. Piratas informáticos.

"Aquél que hace uso de los recursos libres y o de pago que pueden ser movidos a través de las vías de la información que conforman Internet, telnet, (entre otras) para beneficio propio y lucrativo."[29]

No hay que confundirlo con el apelativo hacker, ya que este es aquél que comparte información y conocimiento por mera afición, y no precisamente buscando un fin monetario. Los habitantes del submundo, como son los crackers, hackers y los phreakers suelen ser catalogados dentro de la categoría de *piratas informáticos*, cuando en realidad ésta es otra catalogación que supuestamente debe de estar por debajo de los decretos de la ley.

1.5.3.4. Script kiddie.

Aquella persona que presume de ser un hacker o cracker cuando en realidad no posee un grado de conocimientos suficientes. Normalmente usa cracks, exploits y programas similares construidos por personas con grandes conocimientos pero cuyo uso está al alcance de cualquiera.

1.5.3.5. Lamer.

Persona que dice ser un hacker o un cracker cuando en realidad no es considerada como tal por las personas que le conocen, hacen uso indebido de programas peligrosos para la seguridad en Internet sin conocer su fundamentación ni el riesgo que pueden provocar. Se dice que es un hacker irresponsable.

En los párrafos anteriores, se destacan las acciones que realiza cada uno de las personas que se introducen a las computadoras, sin embargo, es importante que señalemos que un hacker no es un cracker, ni tampoco un phreaker.

Entre las variantes de crackers maliciosos están los que realizan el llamado Carding (Tarjeteo o uso ilegal de tarjetas de crédito), Trashing (Basureo,

[29] Consultable en: http://www.comsto.org/Menu/piratas01.htm.

obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos) y *Phreaking* o *Foning* (uso ilegal de las redes telefónicas).

El hacker nunca está conforme, no puede pensar en un mundo con limitaciones, le apasiona investigar, no soporta la limitación de la información, de la tecnología, etcétera, el hacker lucha por una red libre, que no tenga dueños, que todos tengan acceso a la información, pero que la información clasificada esté bien protegida. En este sentido el hacker, le hace un favor a la sociedad violando sistemas informáticos porque si lo hiciese un espía o enemigo podría causar graves perjuicios.

El cracker tiene como intención destruir, el hacker todo lo contrario. El cracker comete fraudes con tarjetas de crédito, el hacker no. A lo mucho el hacker puede violar algún servidor, o una página web, lo que hace es dejar constancia de que ese sitio es vulnerable, para que el dueño modifique la seguridad del mismo.

Habitualmente, se entiende por hacker aquella persona capaz de introducirse en sistemas informáticos ajenos, a través de cualquier medio, sin autorización y de forma secreta, habitualmente tras la obtención de nombres de usuario y claves de acceso (*login* y *password*), empleando programas que por medio de la fuerza prueban miles de posibles *passwords* hasta encontrar alguna válida, o el acceso a través de agujeros en la seguridad del ordenador. Para ser más exacto, se trata de obtener privilegios que no se poseen en un sistema informático ajeno, en especial los privilegios del administrador del sistema.

De esta forma no sólo se logra entrar en el sistema sino que se obtiene un control total sobre dicho sistema informático, que es lo realmente peligroso. La obtención de dichos privilegios se hace generalmente mediante el uso de exploits que aprovechan algún error del sistema operativo para conseguir los privilegios del administrador.

Los hackers son personas con importantes conocimientos de sistemas operativos (en especial de *unix*), redes, protocolos, seguridad informática y programación entre otras cosas. El problema es que esta afición, es potencialmente muy peligrosa si las motivaciones de quien las realiza son malintencionadas, de ahí la mala fama de los hackers.

Sin embargo, el mundo *hacker* también tiene su lado oscuro, las técnicas de *hacking* son potencialmente muy peligrosas y si caen en manos inmaduras, malintencionadas o delictivas el daño que se puede realizar es considerable.

1.5.4. Cibernética.

La etimología de la palabra cibernética "proviene del griego *kibemetes*", que significa arte del piloto o timonel, el arte del gobierno de guiar, de ella proviene nuestro vocablo gobierno y es una palabra que alude a la función del cerebro con respecto a las máquinas.

La Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes.

"El nacimiento de la cibernética se estableció en el año 1942, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto. La cibernética puede ser considerada como una adquisición sumamente aprovechable para la evolución científica."[30]

Jorge Vasconcelos Santillán, escribe "que cibernética nos remite a una de las áreas más avanzadas en donde interviene la computación, sin embargo se trata de un proceso de retroalimentación, ya sea mecánico, biológico o electrónico.

[30] Couffgal, Louis, ***La Cibernética,*** 4ª.Edición, Industrias Gráficas, Barcelona, 1989, Pág.149.

A través de la cibernética se busca el control de un proceso, enlaza a la teoría general de sistemas con el derecho, cuando éste es visto como un sistema del que se desprenden."[31]

Hans W. Baade, establece que "la cibernética es una ciencia general, capaz de hacer aportaciones a las disciplinas tradicionales como por citar algunos ejemplos la sociología, política, biología, entre otros, incluyendo el derecho, éste como técnica de control social."[32]

El concepto de cibernética, fue utilizado por primera vez en 1848 por el francés Ampere en una clasificación de las ciencias políticas, ya que había creado un sistema para coordinar todo el conocimiento humano y había introducido el término cibernética para indicar el arte de gobierno entendido en sentido político.

"En 1943 el mexicano Arturo Rosenblueth publicó un artículo donde analizaba las líneas futuras del desarrollo de la cibernética: por un lado, las máquinas destinadas a reproducir funciones humanas; por otro lado, el mismo sistema nervioso se presenta como un sistema complejo, con ello no sólo se innovaba la neurofisiología, sino que se establecía una estrecha unión entre un cierto tipo de máquina y las funciones nerviosas del hombre. El problema de la comunicación y el control es único en las máquinas como en el ser vivo. Nace así el estudio paralelo de las máquinas y el hombre."[33]

El concepto cibernética es utilizado para identificar a "la ciencia que estudia los mecanismos automáticos de comunicación y de control de los seres vivos y de las máquinas. Por lo que es necesario explicar su originalidad derivada de dos aspectos:

---

[31] Vasconcelos Santillán, Jorge, ***Informática II, Sistemas de información,*** 1ª.Edición, Publicaciones Cultural, México, 2002, Pág.106.
[32] Fix Fierro, Héctor, ***Informática y Documentación Jurídica,*** 2ª.Edición, Instituto de Investigaciones Jurídicas. UNAM, México, 1996, Pág.116.
[33] Couffgal, Louis, ***Op. cit.,*** Pág.12.

A) Muestra que la estructura de un órgano de un ser viviente es semejante a la se una máquina y por consiguiente sus deducciones son aplicables tanto a las máquinas como al animal y,

B) Muestra que lo esencial de una máquina o sistema automático y en un organismo vivo, es la transmisión de información."[34]

Para conseguir un fin, lo mismo el ser vivo que el órgano de la máquina capta información del mundo exterior, y antes de resolver el problema que se les presenta lo relacionan con la información que permanece almacenada en su memoria.

De lo que se ha visto anteriormente, podemos decir que la cibernética estudia la creación de instrumentos informáticos que simulen actividades del hombre, por ejemplo los robots, desarrollo de la inteligencia artificial, utilización de métodos que le dan a una máquina facultades de decisión a través de programas computacionales, para la búsqueda de soluciones en concreto.

Así concluimos, que la cibernética hace extensivos sus conceptos a otras disciplinas, por ello ha podido ser considerada como puente entre las ciencias, el punto de conexión entre los mundos tecnológico y humano, sin embargo, la cibernética busca el control de los fenómenos, más que su explicación causal, ya que trata del empleo de métodos científicos para explicar fenómenos en la naturaleza o en la sociedad y la forma de representación del comportamiento humano de forma matemática en una máquina, buscando precisamente el control de los fenómenos.

1.5.5. Hardware.

Equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento. Los componentes de esas categorías están conectados a través

[34] Diccionario Enciclopédico Salvat, Tomo 7, 4ª. Edición, Salvat Editores, España, 1995, Pág. 877.

de un conjunto de cables con la unidad central de proceso (CPU) del ordenador, el microprocesador que controla la computadora y le proporciona capacidad de cálculo.

"El hardware de entrada consta de dispositivos externos, esto es, componentes situados fuera de la CPU de la computadora que proporcionan información e instrucciones, el hardware de salida consta de dispositivos externos que transfieren información de la CPU de la computadora al usuario informático y el hardware de almacenamiento sirve para almacenar permanentemente información y programas que el ordenador deba recuperar en algún momento. Los dos tipos principales de dispositivos de almacenamiento son las unidades de disco y la memoria."[35]

Para Guillermo Levine Gutiérrez "es el conjunto de elementos y sistemas electrónicos que forman un sistema de cómputo. Al inicio de la corta historia de la computación digital era fácil distinguir el hardware del software, aunque a medida que avanzan los desarrollos tecnológicos se vuelve más sutil la barrera que separa uno del otro, porque ahora buena parte de la programación de sistema de muchas computadoras reside en un nivel intermedio."[36]

1.5.6. Informática.

La palabra informática es de origen francés, *informatique* neologismo formado por la conjunción de las palabras *Information* y *Automatique*, de información y automatización, sugerido por Phillipe Dreyfus en el año 1962.

En sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones. Su campo cubre los sistemas de información, la forma en que ésta se elabora, transmite y utiliza.

---

[35] ***Cfr.*** Téllez Valdés, Julio, ***Op. cit.,*** Págs. 11, 282.
[36] Levine Gutiérrez, Guillermo, ***Op. cit.,*** Pág. 398.

“Es en principio, una palabra compuesta por lo términos información del latín *in formare* (poner en forma) y “automática”, lo que significa que es la ciencia del tratamiento automático o automatizado de la información, primordialmente utilizando computadoras.”[37]

Informática es la “ciencia del tratamiento automático de la información mediante una computadora. Entre las tareas más populares que ha facilitado esta tecnología se encuentran: elaborar documentos, enviar y recibir correo electrónico, dibujar, crear efectos visuales y sonoros, elaboración de folletos y libros, manejar la información contable en una empresa, tocar música, controlar procesos industriales y jugar. La informática es un amplio campo que incluye los fundamentos teóricos, el diseño, la programación y el uso de las computadoras.”[38]

Por lo tanto, definimos a la informática, como el conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. Esta disciplina tiene en nuestros días un enorme desarrollo gracias a las computadoras, por la gran capacidad de memoria y el acceso a los datos y a la información que se realiza de manera sencilla y rápida.

1.5.7. Ciberespacio.

El prefijo "*ciber*" de la palabra ciberespacio, está tomado de otra palabra más antigua, aunque reciente, cibernética. El ciberespacio, se describe atendiendo a su estructura como la geografía virtual creada por computadoras y redes. En este mismo sentido ha sido equiparado a las autopistas de la información, entendidas éstas como el espacio común creado en las redes telemáticas.

Uno de los más importantes escritores y pensadores del *ciberpunk*, Bruce Sterling, habla del ciberespacio y al efecto señala:

---

[37] Ríos Estavillo, Juan José, ***Derecho e Informática en México”***, 1° Edición, Instituto de Investigaciones Jurídicas UNAM, México, 1997, Pág. 37.
[38] Consultable en: http://es.wikipedia.org.

"El ciberespacio no es algo de nuestros días y tiene ya un cierto tiempo; habría nacido concretamente cuando se inventó el teléfono. El ciberespacio vendría a ser el lugar donde se produce una conversación telefónica, no los teléfonos, sino el lugar entre los teléfonos. El concepto quizás es difícil de captar, sobre todo porque no se trata de un lugar real, no es algo físico sino más bien conceptual. El caso es que en la actualidad las comunicaciones, el flujo de información, ya no se circunscriben sólo a las conversaciones telefónicas, sino a algo extraordinariamente más sofisticado y complejo. Vivimos en el mundo de las telecomunicaciones, la información, las redes de ordenadores, Internet, etcétera y ahora el ciberespacio, ese espacio o universo eléctrico, es algo con más entidad de la que tenía en una simple conversación telefónica."[39]

El ciberespacio que se describe, es más bien una representación gráfica de los diferentes elementos que interactúan en el espacio electrónico, algo entre la realidad virtual y la representación simbólica de interfaces, y que es percibido por los usuarios gracias a visores. Con el tiempo el concepto original de ciberespacio se ha ido dejando un poco de lado en la ciencia ficción para verse sustituido por la realidad virtual. Cada vez son más comunes los escenarios virtuales y similares

En el Informe del Secretario General de las Naciones Unidas en el año 2000, se establece que en los últimos diez años Internet ha tenido un incremento de desigualdad en todo el mundo y subraya la importancia vital de resolver la discrepancia digital. Las razones que explican ese grave fenómeno son entre otras las siguientes:

"La gran diferencia de penetración del ciberespacio en el mundo. Afecta sólo a una parte muy restringida del planeta, a una tercera parte del mismo: el espacio que corresponde a los países desarrollados. La preocupación, es que por el hecho de que la mayor parte de los países de la región no estaban conectados

[39] Consultable en: http://www.ciencia-ficcion.com/glosario/c/ciberesp.htm.

a Internet. El hecho del retraso en la incorporación a la red supone para los países subdesarrollados un factor de empobrecimiento y desigualdad.

Además, el impacto de la informática sobre las libertades en las sociedades avanzadas ha sido también negativo, en cuanto que ha potenciado y abierto la puerta a nuevas formas de violaciones de los bienes de la personalidad o bienes jurídicos fundamentales que constituyen el objeto de los derechos.

Se ha señalado en este sentido, que su potencialidad en la difusión ilimitada de imágenes e informaciones ha convertido a la red en un vehículo especialmente poderoso para perpetrar atentados criminales contra cuatro tipos de bienes jurídicos básicos:

1.- La intimidad, la imagen, la dignidad y el honor de las personas

2.- La libertad sexual al permitir la propagación de imágenes o informaciones que entrañen formas de exhibicionismo, provocación sexual o fomenten la pornografía entre menores de edad.

3.- La propiedad intelectual e industrial, el mercado y los consumidores.

4.- La seguridad nacional y el orden público.”[40]

El Instituto Politécnico Nacional, también hace referencia a lo que es el ciberespacio y la importancia de éste, señalando lo siguiente:

“El ciberespacio es una visualización completamente especializada de toda la información en los sistemas de procesamiento de información globales, a lo largo de senderos proporcionados por las redes presentes y futuras de comunicación, que posibilita la plena copresencia e interacción de múltiples usuarios y la entrada y salida del y al sensorio humano completo, que permite simulaciones de realidades reales y virtuales, la colección y control de información

[40] Consultable en: http://webworld.unesco.org/infoethics2000/forum.html.

remota a través de la telepresencia y la integración e intercomunicación total con una gama plena de productos y entornos inteligentes del espacio real.

El ciberespacio supone una inversión del modo actual de interacción con la información computarizada. En el presente dicha información es externa a nosotros. Asimismo, ofrece la oportunidad de maximizar los beneficios de separar datos, información, separación hecha posible gracias a la tecnología digital.

Por lo que el ciberespacio es un hábitat para la imaginación. Nuestra interacción con las computadoras ha sido hasta el momento principalmente de un pensamiento claro lineal; es el lugar en donde el sueño consciente se encuentra con el sueño inconsciente, un paisaje de magia racional, de razón mística, el lugar y el triunfo de la poesía sobre la pobreza, del "puede ser así" sobre el "debería ser así". El ciberespacio depende de una mezcla de tecnologías, algunas disponibles, otras aún imaginarias."[41]

Sin embargo, aunque el ciberespacio siga sin tener entidad física su influencia es cada vez más notoria, y términos como ciberdelitos o cibernautas pertenecen ya al lenguaje común. El concepto ahora es más claro de entender y surge al no poder decir dónde suceden las cosas físicamente. Por ejemplo, si un hacker comete un delito ¿dónde lo cometió? ¿En su computadora? ¿En que computadora entró? ¿Por las computadoras por los que pasó? Para responder adecuadamente hay que describir todo el conjunto de acciones realizadas: desde el ordenador X entró clandestinamente en el sistema y, robó ciertos documentos que envió al ordenador Z. Pero ni siquiera la mayoría de las acciones realizadas tienen entidad física, por decirlo de alguna manera. La respuesta más sencilla es: en el ciberespacio.

Por lo tanto concluimos que el ciberespacio, no es un sólo lugar, son muchos lugares distintos, es una metáfora para describir el terreno no físico creado por sistemas de computadoras, es simplemente una realidad virtual.

[41] Consultable enhttp://www.hemerodigital.ipn/arte_ciencia/sep-oct97/arquitec/sec_1.html

1.5.8. Seguridad Informática.

"Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas."[42]

La seguridad informática, generalmente consiste en asegurar que los recursos del sistema de información (Material informático o programas) de una organización sean utilizados de la manera que se decidió.

Se dice que, diversas técnicas sencillas pueden dificultar la delincuencia informática, por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla de la computadora, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos

La seguridad informática debe garantizar:

- La disponibilidad de los sistemas de información.
- El recupero rápido y completo de los sistemas de información
- La integridad de la información.
- La confidencialidad de la información.

La seguridad informática busca la protección contra los riesgos ligados a la informática. Los riesgos son en función de varios elementos:

- Las amenazas que pesan sobre los activos (datos) a proteger.
- Las vulnerabilidades de los datos.
- Su sensibilidad, la cual es la conjunción de diferentes factores:
- La confidencialidad.
- La integridad.

[42] Ríos Estavillo, Juan José, ***Op. cit.,*** Pág. 37.

1.5.9. Sistema Informático.

"Es aquel conjunto de material y de programas comprendiendo en una computadora, destinado a recibir, tratar y restituir datos.

Un sistema informático suele estar compuesto por una unidad central de proceso (CPU), dispositivos de entrada, dispositivos de almacenamiento y dispositivos de salida. La CPU incluye registros, los cuales, almacenan los datos y los resultados de las operaciones. En la mayoría de las computadoras, el principal dispositivo de entrada es el teclado. Dispositivos de almacenamiento son los discos duros, flexibles (disquetes) y compactos (CD). Dispositivos de salida que permiten ver los datos son los monitores e impresoras.

1.5.10. Software.

Es el nombre genérico que se da a los programas de una computadora, pero que implica una responsabilidad adicional: asegurar que el programa o sistema cumple por completo con sus objetivos, opera con eficacia, está adecuadamente documentado y es sencillo de operar.

Software. "Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de software son los sistemas operativos (software del sistema), que controlan los trabajos de la computadora, y el software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras."[43]

Por lo tanto, el software del sistema procesa tareas tan esenciales, aunque a menudo invisibles, como el mantenimiento de los archivos del disco y la administración de la pantalla, mientras que el software de aplicación lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares. Constituyen dos categorías separadas el software de red, que permite

[43] Levine Gutiérrez, Guillermo, ***Op. cit.,*** Pág. 406.

comunicarse a grupos de usuarios, y el software de lenguaje utilizado para escribir programas.

1.5.11. Virus Informáticos.

Existe cierta controversia sobre la definición de virus informático. Quizás la más aceptada pertenece a Fred B. Cohen, quien en 1994 escribió su tesis doctoral acerca de los virus, definiéndolos como un programa de una computadora que puede infectar a otros programas modificándolos para incluir una copia de sí mismo.

"Los virus informáticos tienen básicamente la función de propagarse, replicándose desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando graves perjuicios."[44]

Son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de "inmunizar" o eliminar el virus del ordenador.

"Se definen como los programas de cómputo que se reproducen así mismo e interfiere con el hardware de una computadora o con su sistema operativo (el software básico que controla la computadora). Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione, es decir, la computadora debe cargar el virus desde su memoria y seguir sus instrucciones, estas se conocen como carga activa del virus, la cual puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo."[45]

---

[44] Consultable en http://www.iespana.es/iabot/ciencia/ definicion_virus.htm.
[45] Biblioteca de Consulta Microsoft Encarta, ***Op. Cit.***

Existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos. Un caballo de Troya aparenta ser algo interesante e inofensivo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos. Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras. Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

Para detectar la presencia de un virus pueden emplearse varios tipos de programas antivíricos. Los programas de rastreo pueden reconocer las características del código informático de un virus, como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Algunos programas de rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

Por su parte Jorge Vasconcelos Santillán, establece que “los virus son pequeños programas que dañan parcial o completamente los datos que contiene un sistema de cómputo y están diseñados para reproducirse (copiarse así mismos) y distribuirse dentro del sistema. Se les llama virus porque su forma de reproducción y propagación guarda ciertas semejanzas con sus equivalentes bioquímicos; sin embargo, no son virus reales, no afectan a las personas, ni se transmiten por contacto físico entre disquetes.”[46]

Los virus suelen ser elaborados por expertos en programación que desean robar información, sabotear sistemas de cómputo, proteger sus propios programas e incluso sólo por diversión. En la actualidad se han registrado más de 57,000 virus informáticos.

---

[46] Vasconcelos Santillán, Jorge, ***Informática I***, ***Computación Básica***, Editorial, Grupo Patria Cultural, S.A. de C.V., México, 2002, Págs. 80-81.

Los contagios se producen al copiar archivos contaminados de un sistema a otro, ya sea mediante discos o a través de las redes de cómputo. Los virus más modernos (macrovirus) pueden propagarse a través del correo electrónico: el programa dañino viaja como añadido del mensaje principal, por ejemplo de un documento de word, cuando el lector de correo detecta el archivo añadido automáticamente procede a iniciar el programa que puede leerlo (word, excel, son ejemplos), tras lo cual el virus entra en funcionamiento y comienza su labor destructiva.

Según algunos autores, fundamentalmente existen dos tipos de virus:

"1) Aquellos que infectan archivos. A su vez, estos se clasifican en:

- **Virus de acción directa**. Son aquellos que en el momento en el que se ejecutan, infectan a otros programas y
- **Virus residentes.** Al ser ejecutados, se instalan en la memoria del ordenador, infectan a los demás programas a medida que se accede a ellos.

2) Los que infectan el sector de arranque. Estos virus son residentes en memoria."[47]

Y existen muchas más clasificaciones según su comportamiento, siendo las citadas parte de las más significativas y reconocidas por la mayoría de los fabricantes de antivirus, tales como los Caballos de Troya, Gusanos, Bombas de Tiempo y que a continuación se de describen.

1.5.11.1. Gusano informático.

"Un gusano es un virus o programa autoreplicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo. Los gusanos

[47] June Jamrich Parsons y Dan Oja, ***Op. cit.,*** Pág. 185.

utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario."[48]

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Con la proliferación del tráfico de red y el correo electrónico, los gusanos se han vuelto una preocupación importante en la comunidad del cómputo, el gusano esta diseñado para pasar de una computadora a otra, casi todos los gusanos aprovechan las redes de comunicación sobre todo Internet, para viajar en el correo electrónico, por ejemplo el gusano Klez, el cual es un gusano del correo electrónico que se auto envía a todos los registrados en la libreta de direcciones de la computadora infectada.

1.5.11.2. Caballo de Troya (Troyanos).

Un Caballo de Troya es un programa computacional que aparenta realizar una función, éste no es lo mismo que un virus porque, a diferencia de éste, no esta diseñado para copiarse, los caballos de Troya roban contraseñas, eliminan archivos.

Son programas maliciosos que se ocultan en el interior de un programa de apariencia inocente. Cuando este último es ejecutado, el Troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado.

Habitualmente se utiliza para espiar a personas, usando esta técnica para instalar un software de acceso remoto que nos permita monitorear lo que alguien esta haciendo en cada momento.

[48] Breekman, George, ***Op. cit.,*** Pág. 286.

1.5.11.3. Bombas lógica o de tiempo.

Una bomba es un programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción.

A diferencia de un virus, una bomba lógica jamás se reproduce por si sola, las condiciones preprogramadas para su ejecución son:

- Día de la semana concreto.
- Hora concreta.
- Pulsación de una tecla o una secuencia de teclas concreta.

Sus acciones son:

- Borrar la información del disco duro.
- Mostrar un mensaje.
- Enviar un correo electrónico.

CAPÍTULO II

DELITOS INFORMÁTICOS.

2.1. Orígenes.

Pablo Andrés Palazzi escribió: “El cambio tecnológico que se ha vivido desde mediados de siglo, ha producido efectos en todas las áreas del quehacer humano. Cuando se habla de tecnología, no puede dejarse de hacerse alusión a la informática y a las telecomunicaciones. Estos dos fenómenos han hecho que la humanidad entrara a la era de la información.

El Derecho no escapa a la influencia de las nuevas tecnologías, ya que la informática resalta como uno de los campos que encuentran mayor aplicación en el quehacer cotidiano del hombre, jugando un papel preponderante, ya sea porque se utiliza como un medio para delinquir o porque ella es el objeto del delito en sí; estos delitos reafirman la necesidad de un estudio profundo de la materia, destacando las dificultades probatorias, la ironía de las empresas afectadas a denunciar el hecho por miedo a desprestigiarse, la posibilidad de programar su ejecución automática para determinada fecha y en general su inadecuación a las normas penales vigentes que han generado los avances tecnológicos.”[49]

De lo anterior, hemos comprendido que las últimas décadas, han sido el marco de una verdadera revolución en el desarrollo tecnológico, que ha hecho cambiar estilos de vida puesto que han construido las nuevas situaciones que el derecho debe de contemplar. Tal es el caso del empleo de los sistemas informáticos, el cual tiene multiplicidad de campos de actuación y puede realizarse en forma benéfica o nociva. De este modo el derecho debe una vez más reaccionar, intentando respuestas normativas que atienden a las causas de estas situaciones, previniendo y reprimiendo las conductas delictivas que involucra el empleo de la computadora. El desarrollo de los medios informáticos, ha permitido la generación de nuevos comportamientos antisociales y criminales sustentados

[49] ***Cfr.*** Palazzi Pablo Andrés, ***Delitos Informáticos,*** Editorial Ad Hoc, Buenos Aires, Argentina, 2000, Pág. 25-27.

con el vigoroso avance de la tecnología informática que por la magnitud de los valores e intereses en juego, exige la necesidad de definir los nuevos delitos informáticos. Todo ello para evitar una desprotección de la sociedad frente a los avances tecnológicos.

Al respecto Julio Téllez, señala: “es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre y no por la máquina como algunos pudieran suponer, encuentra sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es lógico pensar que de no existir las computadoras, estas acciones no existirían. Por otra parte, la misma facilitación de labores que traen consigo dichos aparatos propicia que, en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo, sin darse cuenta, una serie de ilícitos. Por último, por el mismo egoísmo humano se establece una especie de duelo entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionados, por ese deseo del hombre de demostrar su superioridad frente a las máquinas y en este caso específico, las computadoras.”[50]

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, como veremos más

[50] Téllez Valdés, Julio, ***Op. cit.***, Pág. 103.

adelante, sin embargo debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

2.2. Concepto.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales. A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, formulando diferentes denominaciones para indicar las conductas ilícitas en las que se usa un equipo informático, tales como “delitos informáticos”, “delitos electrónicos”, “delitos relacionados con los ordenadores”, “crímenes por ordenador”, “delincuencia relacionada con la computadora”, *“cibercrimen”.*

En este orden de ideas, en el presente trabajo se entenderá como “delitos informáticos” como todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, y que hacen uso indebido por cualquier medio informático.

2.2.1. Julio Téllez Valdés.

Señala que: “no es una labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos-penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, aún no ha sido objeto de tipificación, sin embargo, y habida cuenta de la necesidad de esto, se hace el distingo pertinente entre lo típico y lo atípico.

Dependiendo del caso, los delitos informáticos son actos ilícitos en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las

conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)."[51]

2.2.2. Carlos M. Correa.

Correa destaca el aspecto evolutivo del delito informático y al respecto señala:

"A través de los años se ha ido produciendo una evolución del concepto de protección de datos determinada por dos aspectos fundamentales: la evolución de las técnicas de información y la nueva configuración de derecho a la vida privada.

En los primeros años de aplicación de las leyes de protección de datos la discusión se centraba en la antítesis vida privada versus computadoras. En el actual estado tecnológico la protección de datos es una síntesis de los intereses individuales y sociales en juego.

La evolución de las técnicas informáticas hace necesario hablar de sistemas de información en lugar de ficheros y tener en cuenta las contradicciones que existen entre la vida privada y otras libertades esenciales."[52]

Correa recoge el concepto que establece Sieber:

"El uso de las computadoras y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso de las computadoras. Si bien no existe aún una medida exacta de la importancia de estas trasgresiones, es probable que su incidencia se acentúe con la expansión del uso de las computadoras. Los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas, tal como la interferencia en una red bancaria para obtener, mediante una orden electrónica un

[51] ***Ibidem.*** Pág. 104.
[52] Correa, Carlos M. citado por Nava Garcés, Alberto Enrique, ***Análisis de los Delitos Informáticos,*** Tesis para obtener el grado de Maestro en Derecho, en la Universidad Nacional Autónoma de México, Ciudad Universitaria, 2004, Pág. 50.

libramiento ilegal de fondos o la destrucción de datos. El tema plantea además, complejos perfiles para el derecho internacional cuando el delito afecta a más de una jurisdicción nacional."[53]

En relación a lo que comenta Carlos Correa, de que el tema plantea complejos perfiles para el derecho internacional cuando el delito afecta a más de una jurisdicción, es cierto, pues el lugar donde se ubica al sujeto activo y el lugar donde se verifica el resultado de su conducta desplegada, pueden en muchas ocasiones no coincidir, esto es parte de la esencia de estas conductas, su carácter transfronterizo, por lo que estamos frente a un problema de extraterritorialidad en los tipos informáticos el cual trataremos más adelante, pues este tema es abordado de manera preponderante por tratadistas como Palazzi.

2.2.3 Pablo Andrés Palazzi

Palazzi señala que la cuestión para precisar el concepto de delito informático, consiste en determinar qué papel juegan las computadoras en estos hechos ilícitos, prácticamente cualquier delito del Código Penal, desde el homicidio hasta el delito de balance falso pueden presentar alguna relación con la informática. Sin establecer una regla genérica, podemos afirmar que una computadora puede constituir un medio para cometer un delito o el objeto sobre el cual recaiga el mismo, el primer supuesto nos lleva a una ampliación de la forma en que un delito puede cometerse, entendemos que el aceptar el uso de la computadora como instrumento delictivo no importa aplicar analogía de ninguna especie sino adaptar la figura penal a los avances de la técnica.

Y ello resulta razonable pues el legislador no puede prever la infinidad de medios a través de los cuales es posible afectar un determinado bien jurídico penalmente protegido.

---

[53] Correa, Carlos, ***Derecho Informático***, Ediciones Depalma, Buenos Aires, Argentina, 1987, Pág. 295.

Debe señalarse, que el concepto de delito informático ha ido evolucionando con el tiempo y en relación a los avances tecnológicos, ya que se señala que los primeros delitos informáticos datan de la década de los setenta, cuyas noticias vienen de notas periodísticas. En la década de 1980 hicieron su aparición los casos de *hacking*, los virus informáticos y otras clases de programas destructivos. El peligro del *hacking* se hizo evidente en 1989 cuando una investigación criminal en Alemania detectó varios hackers que usaban redes internacionales para acceder a información americana e inglesa para venderla a los servicios secretos. En el mismo año, un virus escrito por un estudiante de informática de la Universidad de Cornell, Estados Unidos, infectó y dejó sin funcionamiento a más de 6,000 computadoras conectadas a *Internet*. A fines de la década de los ochenta surgió la denominada piratería informática, la manipulación de cajeros informáticos y el abuso de telecomunicaciones, que revelaron lo vulnerables que eran estos sistemas y la necesidad de prevenir y controlar esta nueva criminalidad en la sociedad de la información. De allí, se concluye que la noción de delito informático debe ser establecida como un concepto amplio, que se integra con novedosas formas delictivas relacionadas con la informática y las nuevas tecnologías.

Palazzi, adopta la definición realizada por un grupo de expertos de la Organización para la Cooperación y el Desarrollo Económico (OCDE) que define al delito informático como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos."[54]

Coincidimos con lo que Nava Garcés, señala al respecto de la definición que adopta Palazzi, al señalar que "la definición obliga a detenernos a recapitular porque se aleja de los elementos básicos del delito para formular un concepto genérico, discutible en varios aspectos, sobre todo en lo relativo a una conducta ilegal, la cual consideramos, interpretando en su totalidad la definición, sólo redunda en el carácter antijurídico de la conducta que transmite o procesa datos de manera ilegal, y puntualiza que a pesar de todo, considera que ésta es la

[54] ***Ibídem,*** Pág. 39.

acepción más próxima y acertada para establecer los rasgos genéricos del delito informático y al efecto lo define como toda conducta ilegal que involucra el procesamiento automático de datos y/o la transmisión de datos."[55]

2.2.4. María de la Luz Lima.

Dice que el delito electrónico en un sentido amplio es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin."[56]

Dicha autora, ve a la computadora como un fin de la conducta ilícita, esto nos lleva a pensar que las computadoras se pueden convertir en el objeto de la conducta reprochable cuando el daño está específicamente dirigido a ellas.

2.2.5. Miguel Ángel Davara Rodríguez.

Davara señala: "es necesario aceptar la expresión delito informático, para poder realizar el estudio de aquello que en la actualidad es una realidad y en un futuro muy cercano estará considerado como delito que se define como la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software."[57]

Por lo que hace a nuestra legislación penal, no prevé una definición de la expresión delitos informáticos, sin embargo, hace alusión a los sistemas o programas de cómputo, tal y como lo establece el artículo 231 fracción XIV, del

---

[55] Nava Garcés, ***Op. cit.***, Pág. 56.
[56] Lima Malvado, María de la Luz, ***Delitos Electrónicos***, en Criminalia, México, Academia Mexicana de Ciencias Penales, Porrúa, No. 1-6. Año L, Enero-Junio 1984, Pág. 100.
[57] Davara Rodríguez, Miguel Ángel, ***Derecho Informático***, 2ª Edición, Editorial Aranzadi, Pamplona, España, 1997, Pág. 318.

Nuevo Código Penal para el Distrito Federal y que será analizado en el capítulo IV de este trabajo:

Artículo 231.- *Se impondrá las penas previstas en el artículo anterior, a quien:*

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

De lo anterior, concluimos que dar un concepto de delito informático no es labor fácil, y que no existe un sólo concepto que defina lo que realmente es, estudiosos del tema lo han definido desde diferentes puntos de vista, sin embargo, tomando elementos de las definiciones anteriores nos permitimos dar un concepto de delitos informáticos, *como aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático, pues en su realización se valen de las computadoras como medio o fin para su comisión.*

2.3. Delitos Informáticos y los medios utilizados.

Porras Quintela señala: “hay personas que consideran que los delitos informáticos, como tales, no existen. Argumentan que tan sólo son delitos *normales* que en lo único que se pueden diferenciar, de otro delito cualquiera, es en las herramientas empleadas o en los objetos sobre los que se producen. Existen muchos otros delitos que difícilmente podemos tipificar con las leyes actuales. Y éstas rápidamente se tendrán que adaptar o redactar acorde a los nuevos tiempos. Si no, ¿Por qué se habla constantemente de lagunas o de falta de regulación si son los mismos delitos de siempre?. Un delito informático puede ser simplemente un *delito clásico* en un nuevo envoltorio.”[58]

[58] Porras Quintela, Manuel, citado por Nava Garcés, Alberto Enrique, ***Op. cit.***, Pág. 57.

Al respecto Andrés Cámpoli expresa: “en los delitos cometidos por medio de elementos informáticos, los cuales presentan una variada gama que pasa por los daños, las injurias, y calumnias, estafas y otros muchos, su bien jurídico protegido, ya se encuentran en su mayoría protegidos por medio de figuras como el robo, el fraude, etcétera contenidos en códigos penales. ¿Qué es entonces lo que nos separa de una correcta aplicación de las leyes penales preestablecidas?. Sólo se trata de un delito que se comete con un nuevo método o medio comisivo del delito y no como erróneamente se piensa de un nuevo delito que para que lo sea debe estar correctamente tipificado.”[59]

Coincidimos con lo que Andrés Cámpoli señala al respecto, de que los delitos informáticos dependen en su gran mayoría, de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que en una postura semejante nos llevaría a pensar por ejemplo, que si mañana se pudiese quitar la vida a alguien por medio de Internet habría que establecer una nueva figura penal, ya que el homicidio estaría cubriendo esta posibilidad: cuando en Derecho se lesiona el bien jurídico protegido, no importa cuál haya sido el medio utilizado, corresponde la aplicación de la ley penal vigente.

Por su parte Pérez Luño expresa “que la difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan bienes jurídicos y entrañan el consiguiente peligro social, o que sea la propia informática el objeto de atentados criminales: estas facetas compendian la noción genérica del “delito informático”, es decir, aquel conjunto de conductas criminales que se realizan a

[59] Cámpoli Andrés, Gabriel, ***Derecho Penal Informático en México***, Instituto Nacional de Ciencias Penales, México, 2004, Pág. 12.

través del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos."[60]

Sin embargo, compartimos la opinión de Nava Garcés, al considerar que el problema no está en la constitución del delito, sino en la forma de probar ese delito, ese es, el gran problema a vencer: lo etéreo de una página *Web*, la manera tan sencilla de enviar un virus a la red desde cualquier lugar del mundo (por ejemplo: el virus "*my doom*" diseñado, entre otras cosas para atacar a los fabricantes de antivirus y la empresa Microsoft). El problema estriba en encontrar al autor de ese delito, saber dónde cometió el delito y dónde afectó ese delito. Pero, cabe preguntarse: ¿se juzgará dónde se fabricó el virus o dónde hizo daño?, ¿ambas legislaciones lo comprenden como delito?.

Más allá de este aspecto nos encontraremos que los delitos informáticos tienen un ámbito de realización del que resulta un conflicto de leyes en el espacio, dándose un problema de extraterritorialidad. El problema de extraterritorialidad, así como la disociación temporal de los delitos informáticos, serán abordados de manera más amplia en los próximos puntos para una mejor comprensión del tema.

2.4. Clasificación de los Delitos Informáticos.

Una vez establecida la concepción de los delitos informáticos, observaremos las respectivas clasificaciones de los tratadistas citados.

2.4.1. Julio Téllez Valdés.

Hace una clasificación en atención a dos criterios: como instrumento o medio, o como fin u objetivo.

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

---

[60] ***Cfr.*** Pérez Luño, Antonio-Enrique, ***Ensayos de Informática Jurídica***, Fontamara. México, 1996, Pág. 18.

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera)

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeación o simulación de los delitos convencionales (robo, homicidio, fraude, etcétera).

d) “Robo” de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos tanto en la entrada como en la salida.

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del “Caballo de Troya”).

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método de conocido como la “técnica de salami”.

i) Uso no autorizado de programas de cómputo.

j) Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios, tales como “consulta a su distribuidor”.

k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles “virus informáticos”.

l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

m) Acceso a áreas informatizadas en forma no autorizada.

n) Intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo.- En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios (discos, cintas,etcétera).

e) Sabotaje político o terrorismo en que se destruye o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate).”[61]

2.4.2. Carlos M. Correa.

Este autor cita una antigua clasificación de Uhlrich Sieber y distingue las siguientes categorías:

a) fraude por manipulaciones de una computadora contra un sistema de procesamiento de datos;

b) espionaje informático y robo de software;

c) sabotaje informático;

d) robo de servicios;

e) acceso no autorizado a sistemas de procesamiento de datos.”[62]

2.4.3. Pablo Andrés Palazzi.

Acercándose más a la dogmática penal, realiza una clasificación acorde con el bien jurídico tutelado, es decir, elabora una clasificación de las distintas modalidades delictivas relacionadas con la informática, las cuales deben hacerse en relación al bien jurídico protegido y dentro de estas categorías, distinguir las acciones típicas que la vida cotidiana o la experiencia local o comparada dan noticia, de esta forma se centrarán las bases para fijar una adecuada política de reforma del Código Penal en materia de delitos informáticos que contemple las verdaderas necesidades que requiere la legislación criminal.

Así, establece:

---

[61] Cfr. Téllez Valdés, Julio, ***Op. cit.***, Pág. 105.
[62] Correa, Carlos, ***Op. cit.***, Pág. 296.

- Delitos contra el patrimonio.-

“La mayoría de los delitos cometidos por medio de ordenadores tienen relación con el patrimonio. En parte motivado por la delegación a máquinas o en cajeros automáticos para la realización de tareas cotidianas, y más recientemente el dinero electrónico. Además han aparecido nuevos bienes jurídicos que requieren nueva formas de protección. Uno de éstos, el más evidente, es la información, la cual puede ser sustraída, borrada, vendida, conocida en forma ilegal.

- Delitos contra la intimidad.-

La información ha adquirido un valor especial en los últimos años pues se trata de mercancía. Ello produce que se comercie con datos de carácter personal. A veces invadiendo de ese modo la intimidad de personas que desconocen que sus datos son objeto de tal intercambio.

Pero además de esta afectación directa al bien jurídico intimidad que tampoco está contemplado en el Código Penal, cabe señalar la existencia de nuevos medios tecnológicos que permiten acceder en lugares de la privacidad del individuo antes inaccesibles.

- Delitos contra la seguridad pública y las comunicaciones.-

No nos parece aventurado pensar que en un futuro no muy lejano la informática estará inmersa en nuestras vidas de una forma tal que seremos muy dependientes del acceso y el buen funcionamiento de una computadora para realizar cualquier tarea cotidiana. La interdependencia de las máquinas hará que el ataque a las mismas constituya un delito que supere la lesión al bien individual para afectar a un bien colectivo. Es aquí donde entran los delitos contra la seguridad pública, las comunicaciones y los medios de transportes.

Cuando se llega a un gran desarrollo informático, la paralización de un ordenador o red de computadoras relacionada con estos servicios podrá ocasionar

catástrofes nacionales e incluso mundiales. Un buen ejemplo de ello, inocuo pero importante para demostrar la fragilidad de los actuales medios de comunicación digital, ocurrió con el ataque a los sitios más concurridos en Internet. Se trató de un ataque organizado por un grupo de *hackers*.

- Falsificaciones informáticas.

Las falsedades cometidas por medios informáticos constituyen el antecedente de la comisión de un delito contra el patrimonio. Esto es así porque en general los documentos electrónicos no tienen un valor jurídico en sí mismos considerados por la carencia de un régimen legal que los contemple.

De allí que resulte necesario analizar nuevas formas de proteger a la fe pública cuando esta se instrumenta mediante ordenadores. El problema aquí es mucho más grave que los delitos tradicionales porque estas falsedades cibernéticas rara vez dejan huellas y si lo hacen, es posible programar el ordenador para que los elimine y dificulte la detención del delito.

- Contenidos ilegales en Internet.

El paso de un ámbito académico a un ámbito comercial de Internet, hizo que la red fuera invadida por una gran cantidad de material ilícito, como la propaganda discriminatoria, contenidos pornográficos y pedófilos inconvenientes para menores, teniendo en cuenta que éstos son los que más navegan por Internet."[63]

2.4.4. María de la Luz Lima.

Presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

[63] Palazzi, Pablo Andrés, ***Op. cit.,*** Pág. 43.

1) Los que utilizan la tecnología electrónica como **método** que son las conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

2) Los que utilizan la tecnología electrónica como **medio**, es decir, son las conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

3) Los que utilizan la tecnología electrónica como **fin**, que son las conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.4.5. Miguel Ángel Davara Rodríguez.

Davara Rodríguez señala que en todo delito informático, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito, una finalidad deseada que causa un perjuicio a otro, a un tercero.

Son nuevas posibilidades que nacen al utilizar la informática como herramienta en la realización de determinadas acciones dolosas que pueden ser consideradas como delictivas.

No obstante, concurren determinadas características, comunes a todos las conductas catalogadas como delitos informáticos, que nos permiten clasificarlas de acuerdo con la función y actividad que se realiza para cometerlos.

Estos delitos poseen unas especialidades que les hacen, en ocasiones, más difíciles de detectar y en otras, aún detectados, no son denunciados por múltiples razones y aún siendo denunciados, son difíciles de perseguir. Todo ello centra su actividad principal en el acceso y/o la manipulación de datos que se encuentran en soportes informáticos o de programas de computadoras utilizados en su procesamiento.

La manipulación mediante la informática puede provenir de dos vertientes diferentes:

a) acceso y manipulación de los datos, y
b) manipulación de los programas.

Así realiza una clasificación en base a seis acciones de acuerdo al fin que persiguen:

- "manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos,
- acceso a los datos y utilización de los mismos por quien no está autorizado a ello,
- introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas,
- utilización del ordenador y/o los programas de otra persona sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro,
- utilización del ordenador con fines fraudulentos y
- agresión a la "privacidad" mediante la utilización y procesamiento de datos personales con fin distinto al autorizado."[64]

Davara establece la importancia de revisar toda esta gama de conductas que derivan de las nuevas tecnologías de la información.

2.4.6. Tipos de delitos informáticos reconocidos por Naciones Unidas.

Dentro del seno de las Naciones Unidas se ha realizado un conglomerado de conductas susceptibles de encuadrarse como delitos informáticos, dichas conductas son las siguientes:

[64] Davara Rodríguez, Miguel Ángel, ***Op. cit.***, Pág. 320.

- Fraudes cometidos mediante manipulación de computadoras:

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

Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

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

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica de salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

- Falsificaciones informáticas:

Como objeto. Cuando se alteran datos de os documentos almacenados en forma computarizada.

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

- Daños o modificaciones de programa o datos computarizados.

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

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

Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa de gusano que subsiguientemente se destruirá puede dar instrucciones a un

sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su denotación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

- Acceso no autorizado a servicios y sistemas informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

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

- Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Con lo anterior, podemos recalcar que es prioritaria la atención que ha cobrado toda esta serie de conductas dañosas, cuya característica atopológica hace urgente su tratamiento en leyes que puedan circunscribir el problema.

2.5. Características.

Existen una serie de notas características del fenómeno de la criminalidad informática cuyo análisis resulta necesario para precisar el concepto de delito informático.

Julio Téllez Valdés, enuncia como características fundamentales que revisten este tipo de acciones las siguientes:

a) Son conductas criminógenas de cuello blanco en tanto que sólo determinado número de personas con ciertos conocimientos, en este caso técnicos, puede llegar a cometerlas.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) 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.

d) Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que los realizan.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presentencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

h) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

i) Ofrecen facilidades para su comisión a los menores de edad.

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

k) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Al respecto agregamos: se trata de conductas que pueden rebasar las fronteras geográficas y los alcances de las leyes.

Por su parte Davara Rodríguez señala: "los delitos informáticos poseen peculiaridades que les hacen de alguna manera *sui generis* en cuanto a la forma de ser cometidos y en cuanto a la detección de los mismos, llegando en algunos casos a ser prácticamente imposible de descubrir el beneficio producto de su actividad ilícita."[65]

Por lo que enuncia como propias y especiales de este tipo de acciones ilícitas y comunes a todas aquellas, las siguientes características:

- Rapidez y acercamiento, en tiempo y espacio, su comisión.

Las facilidades en el tratamiento y proceso de la información, con la posibilidad de realizar programas que actúen retardados o controlados en el tiempo, aprovechando las funciones del sistema operativo de la computadora, que permite activar o desactivar determinadas órdenes a la máquina de manera

[65] Davara Rodríguez, Miguel Ángel, ***Op. cit.***, Pág. 329.

dinámica, incluso flexible, dependiendo de una u otra circunstancia prevista de antemano, así como de las comunicaciones para poder, en tiempo real y fuera del alcance o control del operador, actuar en la forma deseada, permiten preparar acciones dolosas en perjuicio de otro, en tiempo y espacio distantes.

Estos delitos pueden ser realizados por una persona que se encuentre distante al lugar donde son cometidos, y llevando a cabo una actividad diferente. Debido a la posibilidad de actuación sobre los programas que pueden ser activados para actuar en un momento determinado, incluso en meses, desde el momento en que se preparó la acción, se puede lograr que la persona que lo haya realizado se encuentre lejos. Es esta una característica que dificulta, en múltiples ocasiones, la localización de la actividad y su relación con los hechos, llegando incluso a ocultar al verdadero impulsor y al que realiza la acción.

- Facilidad para encubrir el hecho.

Esas mismas facilidades enunciadas en el párrafo anterior y su utilización en la comisión del delito, ofrecen condiciones óptimas para encubrir el hecho. Es posible modificar, por ejemplo, un programa para que realice una actividad ilícita en beneficio del autor y establecer una rutina software que vuelva a modificar el programa, en forma automática, una vez realizado el hecho dejándole tal y como se encontraba al principio.

De esta forma, ni visualmente, ni con el análisis del programa, ni con el estudio del proceso, seria posible detectar lo que ha ocurrido y como se ha cometido el hecho. Solamente podíamos acudir al resultado para comprobar que la acción ha sido cometida. Pero como el resultado será la producción de un beneficio para su autor y un perjuicio para otro, es posible que no se pueda nunca comprobar que el hecho producido ha sido uno de los ilícitos que hemos considerado como delito informático.

- Facilidad para borrar las pruebas.

Existe una gran facilidad para borrar todas las pruebas que haría prácticamente imposible que se detectaran. En ocasiones, debido a la flexibilidad y dinámica propia del procesamiento informático, que impide detectar una determinada actividad o proceso con posterioridad a su realización y en otras ocasiones, debido a la facilidad para hacer desaparecer en forma fraudulenta, por medio de la manipulación de programas y datos incluso a distancia las actividades, operaciones, cálculos o procesos que han sido efectuados. Las pruebas que se pudieran conseguir en este aspecto, estarían en muchas ocasiones en soporte magnético o basadas en actividades informáticas con todas las dificultades ya conocidas.

Son éstas tres características especiales en la comisión de un delito por medios informáticos, las que nos inducen a pensar en la necesidad de un tratamiento autónomo que estudie las acciones delictivas cometidas por medios informáticos. Es claro que en todos los casos, existe una agresión a un bien jurídico protegido, el tema solamente gira alrededor de sí existe o no responsabilidad penal, si la acción dolosa está o no, penalmente tipificada. Lo que está claro es que, cuando existe el delito no se puede discutir sobre su procedencia, la cuestión es ver si existe o no, si está o no tipificado.

Contrario a lo establecido líneas arriba, todavía es posible detectar y comprobar el origen de un delito informático, lo que no significa que la tarea sea sencilla.

2.6. Dificultad para la investigación del delito informático.

El delito informático es más difícil de investigar que el delito tradicional, porque es novedoso, los tribunales no están preparados para investigar y detectar estas técnicas novedosas y el propio delito suele no dejar rastros.

“En el ambiente digital no quedan huellas visibles a simple vista, y si éstas existen es muy difícil imputarlas a una indeterminada persona. Por ello, en la

investigación del delito informático será necesario realizar pericias a impresoras, computadoras, archivos donde queda registrado el acceso a un determinado sistema informático por una determinada computadora y todo lo relacionado con las mismas, ya que son cuestiones novedosas que requieren cuerpos técnicos especializados."[66]

En su momento el especialista en delitos informáticos Nava Garcés, estableció en una conferencia la factibilidad de la comprobación de los delitos informáticos mediante el seguimiento de las "huellas digitales" o rastros que deja todo acceso a las tecnologías de la información.

2.7. El problema de la extraterritorialidad en los delitos informáticos.

El lugar donde se ubica al sujeto activo y el lugar donde se verifica el resultado de su conducta desplegada, pueden en muchas ocasiones no coincidir. Esto es parte de la esencia de estas conductas, su carácter transfronterizo.

Palazzi escribe:

"La criminología sostiene que tanto el factor espacio como el tiempo constituyen elementos de riesgo que el delincuente tendrá en cuenta al momento de cometer la acción ilícita. En los delitos cometidos a través de medios informáticos encontramos también las características de los delitos a distancia, entendidos éstos como aquellos en los cuales puede disociarse espacialmente la conducta delictuosa del resultado."[67]

Veamos un ejemplo. "Un software puede ser programado en cualquier lugar del planeta y puede producir sus efectos en cualquier otra parte. Ayuda esto la interconexión cada vez mayor que se da entre computadoras, por ejemplo los virus informáticos que se suelen encontrar en las computadoras personales son hechos en su mayoría en el exterior, por personas que residen allí y producen sus efectos en nuestro país.

---

[66] ***Cfr.*** Palazzi, Pablo Andrés, ***Op. cit.,*** Pág. 66.
[67] ***Ibidem***, Pág. 73.

La extraterritorialidad plantea problemas en cuanto a la competencia, que determinan dónde deberá sustanciarse el proceso y el juez que deberá intervenir. Más adelante, al abordar el tema de los delitos informáticos y su inclusión en diversas legislaciones nacionales y extranjeras podremos profundizar en ejemplos que actualizan lo referente a la extraterritorialidad.

En las leyes norteamericanas sobre delitos informáticos, en el capítulo de competencia, es lo bastante amplio como para poder permitir juzgar el delito informático en cualquier estado: conocidos como *long arm statutes* es decir, leyes de gran alcance que buscan evitar los efectos de las redes informáticas.

Otras leyes son más extensas en su jurisdicción y tienden aplicarse incluso más allá de sus fronteras, por ejemplo, la Ley de Delitos Informáticos de Malasia del año 1997 establece, bajo el título de Ámbito Territorial, que la ley se aplicará a cualquier individuo, con independencia de su nacionalidad e incluso que la ley tendrá efectos fuera de Malasia.

Lo cierto es que estos problemas de extraterritorialidad del delito van a ser cada vez más frecuentes. Un caso que ocurrió en Argentina fue el intento de traspasar la suma de 30 millones de dólares a una entidad financiera del Uruguay.

La maniobra fue frustrada porque uno de los empleados del banco escribió mal una de las claves, pero de haber ocurrido la transferencia ilícita, se habría planteado un complejo problema de competencia, ya que no se sabría a que juez le tocaría intervenir.

La dificultad para determinar el lugar de la comisión del delito en estos casos, ha llevado a nuestro más alto tribunal a decidir que en el caso de delitos cometidos a distancia y en diversas jurisdicciones deberá elegirse la jurisdicción atendiendo a las exigencias planteadas por la economía procesal la necesidad de favorecer, junto con el buen servicio de justicia, la defensa de los imputados.

Acostumbrados a determinar que un delito tiene un modo tiempo y lugar, podemos ver que esto constituye el refugio de los autores de un delito de esta especie, pues se puede determinar el lugar y el tiempo donde se causó la lesión al bien jurídico tutelado, sin embargo, lo difícil consiste en establecer el tiempo y el lugar en que se programó dicha lesión jurídica.

2.8. La disociación temporal.

La posibilidad de programar la ejecución del delito informático en una determinada fecha es otra de las características del delito informático. La disociación no es entonces sólo espacial sino también temporal.

Como las computadoras poseen un reloj interno que es alimentado con una batería, es posible determinar la fecha en que se activará el programa o se ejecutará una determinada instrucción. El caso más común es el de los virus informáticos denominados "Viernes 13", *"I love you",* etc., que se activan en una fecha clave.

Pero la programación de una acción para un tiempo determinado no sólo puede estar ligada con la comisión del delito, sino que puede construir una forma de obstruir la investigación del mismo. Por ejemplo, los programas que al detectar un acceso eliminan determinada información, o avisan del intento de acceso a alguien o al propio autor del delito, que de esta manera sabe que lo están investigando.

2.9. Problemas específicos que plantean Internet y las autopistas de la información al Derecho Penal.

El crecimiento exponencial de Internet desde su despegue comercial hasta la fecha ha sido increíble. No obstante su descomunal crecimiento, presenta sus flancos débiles relacionados con la seguridad.

Veamos algunos ejemplos de problemas que produce *Internet*:

La organización terrorista ETA distribuye información sobre sus actividades en servidores de *Internet* ubicados en otros países, pero no en España, para eludir un posible delito de apología de terrorismo. Según informó el responsable de la Unidad de Delitos Informáticos de la Guardia Civil, cualquier usuario español puede acceder sin apenas dificultades a estos servidores internacionales de *Internet* y consultar la información que en ellos ofrece la ETA.

Los mercados financieros internacionales interactúan tanto a través de las computadoras, como de los operadores en el piso del mercado y la ubicación física de los mismos ya no es relevante, lo cual, si bien ayudan a la actividad económica y traen ganancias extranjeras a otros países, pueden crear problemas cuando los delitos son cometidos en este mundo etéreo.

Palazzi es quien ejemplifica lo siguiente:

“El caso de Baring Brothers es un ejemplo de cómo la existencia de diversos elementos ubicados en diversas partes del mundo puede complicar la determinación de la jurisdicción y el Derecho aplicables. Indudablemente se van a producir problemas entre los tribunales que quieran reservar para sí la facultad de juzgar el delito que tenga algún punto de contacto con ellos.

Dado que un archivo de Internet puede ser accedido por cualquier persona a lo largo del mundo, la posibilidad de conexión con algún tribunal es enorme. Y esto implica un posible conflicto no sólo de normas jurídicas sino también de pautas sociales, culturales y económicas.

El articulo 1° del Código Penal argentino, establece que se aplicará por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en lugares sometidos a su jurisdicción y por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en el desempeño

de su cargo. Mediante esta norma se establece el principio de territorialidad de la ley penal argentina."[68]

La conexión con otros países puede producirse a través de Internet por acciones realizadas a través de *e-mail* o de páginas *web* cuyos efectos se radiquen en nuestro país.

Pero cuando se trata de comunicaciones a través de correo electrónico, parece que el lugar de comisión del delito será el determinante y en estos casos generalmente ello se produce donde se recibe la comunicación.

Cámpoli escribe: "El *ciberterrorismo* no es otra cosa que un acto clásico de terrorismo en el cual el autor utiliza la red o medios informáticos para cumplir sus objetivos, lo cual si bien puede en alguna medida dificultar la persecución de los que resultaren responsables por la impersonalidad del medio utilizado, no por ello debe ser tomado como simple hecho de *hacking o cracking*, el cual en la mayoría de los casos puede, según la legislación vigente en cada Estado, quedar impune."[69]

España ha sido objeto de un ataque terrorista significativo, lo ocurrido el 11 de marzo de 2004, tiene relación con nuestro tema en cuanto que se realizó a través de dispositivos electrónicos, que sirvieron para detonar a distancia los artefactos colocados en los diversos convoyes que estallaron esa mañana. A su vez, este tipo de actos, como ocurrió en Nueva York, pueden realizarse mediante las comunicaciones en red que pueden establecer los terroristas con total libertad; la tecnología sirve, como se ve en estos casos para cometer las conductas más perversas.

[68] Palazzi, Pablo Andrés. ***Op. cit.,*** Pág. 76.
[69] Cámpoli, Gabriel Andrés, citado por Nava Garcés, ***Op. cit.,*** Pág. 154.

2.10. Cooperación conjunta para combatir el delito informático.

El carácter totalmente descentralizado y no jerárquico de Internet, el hecho de no estar ninguna autoridad o control es la mayor ventaja de la red respecto de los usuarios. Pero desde el punto de vista legal ello constituye un grave problema. La ley penal se caracteriza por su aplicación territorial y choca con la dimensión transnacional de Internet. En razón de que Internet no reconoce límites geográficos y que los delitos traspasan las fronteras se ha tomado la conciencia de la necesidad de cooperación conjunta para combatir el delito informático.

En la Unión Europea existe preocupación por el fenómeno de la delincuencia a través de redes informáticas globales. Así, en la Iniciativa europea de comercio electrónico se sostiene que:

Un problema que cada día preocupa más es la aparición de la “ciberdelincuencia”, con delitos como lavado electrónico de dinero, las actividades de juego ilegal, la piratería informática o la violación de la propiedad intelectual. La cooperación internacional está ya muy avanzada en determinadas áreas fundamentales, como la lucha contra la delincuencia internacional organizada que se sirve de las nuevas redes de comunicación. Ante las nuevas formas de delincuencia informática y tecnológica que han aparecido en las redes mundiales (los delitos de piratería informática registrados están experimentando un crecimiento anual del 100%), las autoridades públicas han reaccionado enérgicamente. En Europa (Europol), así como en un contexto internacional más amplio se han creado grupos especiales y se ha reforzado la cooperación transfronteriza en áreas tan importantes como la localización y seguimiento (trap and trace) de delincuentes en línea y la ‘búsqueda y confiscación (search and seize) de pruebas digitales. También se están haciendo esfuerzos para armonizar la legislación penal en materia de delitos informáticos y evitar la aparición de paraísos digitales. A raíz del Consejo de Dublín, se creo un Grupo de Alto Nivel que está ultimando un plan de acción para luchar contra la ciberdelincuencia.

Estos esfuerzos revisten una importancia fundamental para incrementar la confianza en el comercio electrónico internacional.

Este movimiento internacional fue coronado en abril del 2000 con la reciente propuesta del Consejo de Europa de crear un tratado sobre delitos informáticos. El tratado no sólo incluye armonización de figuras penales sino también distintas figuras penales sino también distintas formas de cooperación entre las autoridades nacionales, tales como intercambio de datos en línea y acuerdos de extradición más efectivos.

Con esto se busca evitar lo que ocurrió con el virus escrito en Filipinas, y que infectó a ordenadores en los Estados Unidos y Europa: Filipinas carecía de leyes sobre delitos informáticos, lo que obstaculizó la posibilidad de extraditar a los creadores del virus.

2.11. Nuestra opinión.

Ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología informática, sin embargo, como hemos visto algunas legislaciones han atendido y regulado las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Como consecuencia de la proliferación informática y de su uso indebido, ha hecho que surjan nuevas conductas antisociales y como consecuencia nuevos delitos en materia informática a los cuales denominaremos “delitos informáticos”, dando origen a la impunidad que cometen los delincuentes en este tipo delitos.

Ante este desarrollo, ha surgido la necesidad de legislar sobre este tipo de ilícitos, dado a que los delitos tradicionales tales como fraude, robo, pornografía, etcétera, han pasado de ser formas tradicionales a formas no tradicionales, por el uso indebido de la computadora, lo que ha propiciado la necesidad de regulación por parte del derecho.

Hemos visto, que no existe un consenso en cuanto al concepto de delito informático, sin embargo, estudiosos del tema lo han tratado de definir desde diversos puntos de vista, en razón de que su misma denominación alude a una situación especial, ya que para poder hablar de delitos en el sentido de acciones típicas, es decir, tipificadas o contempladas en textos jurídicos penales, requiere que la expresión delitos informáticos este consignada en los códigos penales, lo cual aún, no se ha podido tipificar de manera adecuada.

Podemos concluir que los delitos informáticos, han alcanzado un alto índice delictivo, toda vez que la falta de tipificación de los mismos permite a los delincuentes realizarlos con toda impunidad, considero que los delitos informáticos van más allá de una violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de estos, no solamente se lesionan esos derechos sino otros como el derecho a la intimidad.

La falta de preparación de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de los sujetos pasivos de denunciar este tipo de ilícitos y las consecuentes pérdidas económicas entre otros aspectos más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada cifra negra.

CAPÍTULO III

LEGISLACIÓN INTERNACIONAL SOBRE DELITOS INFORMÁTICOS.

3.1. La problemática de los delitos informáticos en el ámbito internacional.

El crecimiento de la tecnología ha hecho que hoy en día recibamos constantemente los beneficios de los avances tecnológicos, en donde cada vez es más frecuente que personas, empresas, hospitales, universidades, industrias y el gobierno mismo se vuelvan dependientes de los avances de la misma; es indudable que las computadoras se han convertido en una herramienta indispensable para el desarrollo de la sociedad, sin embargo de los capítulos anteriores, hemos visto que se presenta un aspecto negativo, el surgimiento de conductas delictivas que han hecho de los sistemas informáticos instrumentos para delinquir.

Julio Téllez, escribe:

"El Derecho Penal de los Estados interesados en combatir esta nueva delincuencia, contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra sistemas de información perpetrados por particulares. La aproximación del Derecho en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y métodos disponibles en Derecho Penal."[70]

Estos ataques son transnacionales por su propia naturaleza y requieren de una cooperación internacional. La uniformidad de las legislaciones mejorará esta cooperación y garantizará que se cumpla la exigencia de doble incriminación (según la cual una actividad debe constituir un delito en los dos países en cuestión para que éstos colaboren a nivel judicial en el marco de una investigación penal).

[70] Téllez Valdés, Julio, ***Op. cit.***, 2001, Pág. 175.

Es por ello que surge la necesidad de adoptar medidas legislativas acorde al avance tecnológico como lo veremos en este capítulo, pues nuestro objetivo, es el de presentar todos aquellos elementos que han sido considerados por diferentes países los cuales disponen de una legislación para enfrentar la problemática de los delitos informáticos.

3.1.1. Estados Unidos.

Es uno de los países que más actividad legislativa ha tenido en materia de delitos cibernéticos para hacer frente a esta clase de delincuencia, debido en gran parte al desarrollo tecnológico que los caracteriza, siendo uno de los países que se encuentra al frente en esta materia.

Nava Garcés señala al respecto: "Estados Unidos, ha sido el ejemplo a seguir, cuando se trata de la diversificación de leyes. Cada estado cuenta con su propia legislación en diversas áreas, sin embargo, podremos observar que, a pesar de este aspecto tan característico del sistema federal, cuando sucedió un evento como el de los atentados a las torres gemelas en Nueva York, se optó por federalizar el tratamiento a las conductas realizadas a través de medios informáticos."[71]

Estados Unidos ya contaba desde 1986 con la Federal Abuse and Fraud Act (Ley Federal de Fraude y Abuso Computacional) que le brindaba un marco legal para defenderse de los delitos informáticos, pues contemplaba a nivel federal aquellos delitos destinados a afectar los sistemas de cómputo del gobierno federal. Sin embargo en 1994 adoptó la Fraud and related activity in connection with computer (18 U.S.C. 1030") (Ley Federal de Abuso Computacional), que se proscribe la transmisión de un programa información, códigos o comandos que causan daños a las computadoras, al sistema informático, a las redes, información, datos o programas. Esta ley fue un adelanto porque estaba en contra de los actos de transmisión de virus.

[71] Nava Garcés, ***Op. cit.***, Pág. 288.

La ley de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. La ley define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción puede ser una multa o un año de prisión.

El Congreso norteamericano promulgó el 24 de octubre de 2001 la llamada USA Ley *Patriot*, cuyo objetivo es el combate al terrorismo y puede aplicarse aunque la obtención de información sobre espías o terroristas extranjeros no constituya "el propósito" de una investigación, sino un "propósito significativo" de la misma. Dicha ley permite la vigilancia y cancelación de cuentas de correo electrónicas, si se tiene la sospecha que a través de las mismas, se lleva a cabo algún acto terrorista, aunque claro, debemos establecer que esta ley tiene fines más caros, pues para cumplir su objetivo (que es el combate al terrorismo) tiene la difícil tarea de supervisar Internet, las comunicaciones por cualquier medio y evitar con ello el financiamiento y las operaciones de grupos terroristas.

Ejemplo de la Ley *Patriot*: cualquier persona, mexicana, en territorio mexicano, que, mediante el uso de un servidor mexicano adquiera una cuenta de correo electrónico extranjero (*yahoo, hotmail, aol,* etc.), para enviar correos a sus compatriotas mexicanos que viven en México, puede ser objeto de supervisión por la Ley *Patriot* .

Ante esta cuestión, Morón Lerma escribe:

“El anonimato se ha configurado, es esta sociedad de la información como uno de los derechos del usuario de Internet, del “ciudadano electrónico”, expresión del derecho fundamental a la intimidad y al secreto de las comunicaciones, concretado en la necesidad de proteger el conocimiento que los otros pueden tener de los sitios consultados o visitados y en la de impedir la reconstrucción de

la personalidad digital que con la trazabilidad de dichos datos o huellas electrónicos se logra. Sin embargo, la articulación de instrumentos que permitan la detección, investigación y prueba de los ciberdelitos requiere la incorporación de medidas que no se limiten a trasladar los mecanismos de investigación propios del entorno analógico de Internet, sino que, por el contrario, se hallen específicamente concebidas y adaptadas a las peculiaridades de la realidad digital. Esto es, mecanismos que revistan idoneidad para aprehender y responder a las cambiantes condiciones en las que se perpetra la cibercriminalidad (volatilidad, carácter transfronterizo, rápida asimilación de progreso técnico y estructura descentralizada o anárquica). Ahora bien, la peculiaridad de Internet y la previsión de esos sofisticados instrumentos puede generar nuevos peligros y potenciales abusos (monitorización de la navegación e interceptación del correo electrónico) que vulneren, inadvertida e invisiblemente, las garantías dimanantes del derecho a la privacidad informática de los ciudadanos."[72]

Debemos mencionar que a pesar de ser uno de los países con más actividad legislativa en materia de delitos cibernéticos, aún no hay una legislación que de manera eficaz termine con este tipo de ilícitos, pues en un informe federal dado a conocer el 9 de marzo del 2004 en Washington, sugiere que aún pueden pasar años antes de que entre en vigor un régimen internacional eficaz sobre el cumplimiento de una ley para tratar con los delitos cibernéticos.

Sin embargo, el departamento de justicia de Estados Unidos ha estado trabajando con Canadá, México, países europeos y asiáticos sobre el tema de los delitos cibernéticos, con el propósito de llegar a establecer parámetros que hagan posible procesar o extraditar a los hackers o piratas electrónicos.

Hoy en día, en el Congreso norteamericano han prosperado leyes que contrarias a su denominación, permiten, de manera oficial a la empresa recopilar y divulgar datos personales tales como nombre, dirección y cualquier registro sobre actividades *online*, (cibernavegación), sin consentimiento del interesado, de igual

[72] Morón Lerma, Esther, citado por Nava Garcés, ***Op. cit.***, Pág. 291.

modo se autoriza la vigilancia e interceptación de las comunicaciones telefónicas y electrónicas sin previa orden judicial, cuando pueda existir un ataque inminente a través de un ordenador conectado a Internet o una amenaza inmediata sobre un interés relativo a la seguridad nacional.

3.1.2. Francia.

"La legislación francesa tiene sus antecedentes en materia informática, en los años setenta en la elaboración del estatuto legislativo general o llamado también "ley relativa a la informática, los ficheros y las libertades" del 6 de enero de 1978, posteriormente la segunda etapa comienza diez años después con la Ley número 88-19 del 5 de enero de 1988 sobre el fraude informático."[73]

Esta ley fue la primera legislación en materia de delitos cibernéticos en Francia para hacer frente a la delincuencia informática, en la cual se introdujo un capítulo al Código Penal francés que se titula "Sobre ciertas infracciones en materia informática", y comprende los siguientes delitos:

- ✓ Acceso fraudulento a un sistema de elaboración de datos.
- ✓ Sabotaje informático.
- ✓ Destrucción de datos
- ✓ Falsificación de documentos informáticos.
- ✓ Uso de documentos informáticos falsos."[74]

3.1.2.1. Acceso fraudulento a un sistema de elaboración de datos.

En el artículo 462,2 de la ley en comento 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 funcionario del mismo.

---

[73] Ramírez Acosta, Carlos, ***Delitos informáticos***, La Revista de la Seguridad, Año 5, Volumen 4, Número 42, Sistema Ópalo, México, 2002.

[74] Palazuelos, Silvia Guadalupe, ***Delitos informáticos, Propuesta para el Tratamiento de la Problemática en México,*** Aequitas, Revista Jurídica del Poder Judicial del estado de Sinaloa, Segunda Época, Número 32, México, 1999, Pág.76.

3.1.2.2. Sabotaje informático.

Se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos (artículo 462,3).

Sin embargo el delito de sabotaje se ha aplicado más bien tratándose de conductas contra el Estado.

3.1.2.3. Destrucción de datos.

A quien intencionadamente introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión se le es sancionado (artículo 462,4).

3.1.2.4. Falsificación de documentos informáticos.

En el artículo 462,5 se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

3.1.2.5. Uso de documentos informáticos falsos.

Se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462,5 (artículo 462,6).

Posteriormente en Francia se realiza otra reforma en materia informática, la Ley Número 92-685 del 22 de julio de 1992, importante reforma que establece disposiciones relativas a los atentados al sistema de procesamiento informatizado de datos, en el nuevo Código Penal, se contemplan siete artículos para regular los delitos informáticos del artículo 321-1 al 327-7, es de resaltar que en esta nueva legislación francesa tipifica nuevamente el acceso a sistemas en el artículo 323-1 que sanciona a quien acceda o se mantenga fraudulentamente, en todo o en parte de un sistema de proceso automatizado de datos, será sancionado de un año de prisión y una multa, si el resultado de este acceso ilícito de deriva de la modificación de datos, o de una alteración del funcionamiento del sistema, la pena se agrava.

"Sobre este artículo en particular, la doctrina francesa lo considera un delito obstáculo o de barrera, por hacer referencia a la figura autónoma del acceso ilícito, tipificado anteriormente en el artículo 462-2 de la Ley Número 88-19 del 5 de enero de 188 y consagrado actualmente en este aspecto."[75]

Actualmente Francia y otros países europeos establecen como condición para proporcionar informes de los archivos de sus cuerpos policíacos, que el país que la solicite cuente con la legislación protectora de la privacidad informática.

En Europa existe hoy día una creciente preocupación por regular la vida del ciberespacio, ya que en gran medida, muchas operaciones de diversa índole son producidas en ese terreno sin fronteras.

3.1.3. España.

La regulación normativa penal en materia de delitos cibernéticos en España tiene su antecedente más importante en la Ley Orgánica 10/1995, del nuevo Código Penal, expedida y promulgada el 23 de noviembre del mismo año, ley que sigue vigente y con la cual se pretende hacer frente a la delincuencia informática y en donde se han tipificado varias conductas delictivas, relacionadas con el uso de equipos de cómputo, reguladas dentro del Título X de "El honor, la intimidad personal y familiar y la propia imagen de las personas.

Es importante señalar que esta normatividad obedece al mandato constitucional del artículo 18 de la Constitución española, en el que establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."[76]

Dentro del Código Penal Español de 1995, se contiene un catálogo de delitos informáticos muy amplio para sancionar aquellas conductas que atentan contra diversos bienes jurídicos, así tenemos:

---

[75] Consultable en http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm.
[76] Constitución Española, Tercera edición, Editorial Aranzadi, S.A., España 2004, Página 477.

3.1.3.1. Ataques que se producen contra el derecho a la intimidad.

Los artículos del 197 al 201 del Código Penal, establecen el delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.

En dichos artículos se establece que la persona que para descubrir los secretos o vulnere la intimidad de otro, sin su consentimiento, se apodere de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

De igual forma es sancionado la autoridad o funcionario público, que aprovechándose de su cargo, realice cualquiera de las conductas que se describen en esos artículos, además con la de inhabilitación absoluta por tiempo de seis a doce años.

Esta legislación establece que para proceder por los delitos previstos en este capítulo, será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

3.1.3.2. Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.

En este apartado se hace referencia a la protección a la propiedad intelectual, especialmente a la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas, estableciendo que comete infracciones al que con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en

cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

3.1.3.3. Sabotajes informáticos.

El Código Penal español, define al delito de sabotaje informático, como aquel delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

3.1.3.4. Fraudes informáticos.

Son aquellos delitos de estafa, a través de la manipulación de datos o programas para la obtención de un lucro ilícito.

En el mencionado código se establece que comete estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Sin embargo, en dicho código se consideran reos de estafa los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. De igual forma el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio se le será sancionado con las penas previstas para tal conducta.

Enrique Orts Berenguer, escribe en general sobre los delitos informáticos en España:

“Algunas normas del Código Penal son susceptibles de abarcar determinadas conductas que suelen calificarse como delitos informáticos. Es de notar, sin embargo, que el análisis de esos tipos penales tan sólo entraña una visión sesgada de la amplia problemática que hoy plantea la utilización fraudulenta

de la tecnología informática, cuyo tratamiento no ha de ser sólo interdisciplinar sino también global, al menos en algunos aspectos.

Téngase en cuenta que la aparición de Internet ha dado lugar a numerosos delitos de carácter transfronterizo y a una criminalidad de alta tecnología, de carácter organizado, que actúa a través de la red (blanqueando los efectos procedentes del delito, cometiendo fraude en las transacciones comerciales, realizando espionaje económico, etc.), cuya persecución no encuentra tan solo trabas procesales, derivadas de las propias limitaciones a la aplicación ultraterritorial de las leyes nacionales, sino que conducen a veces a la impunidad de ciertas personas que contribuyen a la difusión de la información delictiva. En el orden procedimental, no resulta difícil a los delincuentes informáticos orillar la competencia de los Tribunales cuando actúan desde lo que suelen denominarse paraísos informáticos (esto es, países que no han ratificado los convenios internacionales de protección de los datos insertos en la red, y en los que no existe una regulación adecuada de estas conductas), toda vez que, en principio, la ley de cada estado alcanza hasta donde llegan los confines de su soberanía. Bien es verdad que los diferentes países suelen prever excepciones a esa regla general, basadas comúnmente en la nacionalidad del sujeto activo del delito y en la naturaleza de la infracción; como así lo hace el ordenamiento jurídico, en el que se faculta a los Tribunales españoles para conocer de algunos hechos realizados fuera del territorio nacional (bajo ciertas condiciones legales).

En concreto, cuando el delito sea cometido por un español (o persona que hubiese adquirido la nacionalidad española con posterioridad a la comisión del hecho), dejando no obstante la puerta abierta a cualesquiera otras infracciones que a través de tratados internacionales puedan incorporar a los enumerados. Con todo, quedan al margen de estas excepciones determinados delitos, como los

relativos a la propiedad intelectual que, en el ámbito virtual, presentan una particular importancia."[77]

De lo anterior, concluimos que esta Ley 10/1995 del Código Penal español, incorpora en varios de sus preceptos a los delitos informáticos, como es el caso del fraude informático, sabotaje informático, plagio o reproducción en materia de propiedad intelectual y el acceso no autorizado, el cual nosotros definimos como la simple introducción a sistemas de informáticos o a computadoras, infringiendo por supuesto medias de seguridad destinadas a proteger la información.

3.1.4. Alemania.

En Alemania, la denominada Segunda Ley para la lucha contra la Criminalidad Económica de 15 de Mayo de 1986, relaciona una variada gama de hechos punibles cometidos con medios electromagnéticos o informáticos o de la información como bien jurídico u objeto material de los mismos, acorde con la realidad tecnológica.

Las formas típicas del derecho alemán son:

- ✓ Espionaje de datos (Art. 202 a);
- ✓ Estafa informática (263 a);
- ✓ Utilización abusiva de cheques o tarjetas de crédito (266);
- ✓ Falsificación de datos con valor probatorio (269);
- ✓ Engaño en el tráfico jurídico mediante elaboración de datos (270);
- ✓ Falsedad ideológica (271);
- ✓ Uso de documentos falsos (273);
- ✓ Destrucción de datos (303 a) y
- ✓ Sabotaje informático (303).

[77] Orts Berenguer, Enrique y Margarita Roig Torres, ***Delitos informáticos y delitos comunes cometidos a través de la informática,*** Tirant lo Blanch, "colección los delitos", Valencia, España, 2001, Pág. 162.

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

Esta solución fue también adoptada en Austria, ya que en su legislación se contempla los delitos de destrucción de datos, refiriéndose no sólo a los datos personales sino también a los no personales y a los programas de cómputo, "se hace referencia a la estafa informática tipificado en el artículo 148 y que señala que a aquéllos individuos que con dolo causen un perjuicio patrimonial a terceros, sin embargo cabe mencionar que esta legislación contempla sanciones más fuertes para quienes en ejercicio de su profesión de especialistas en sistemas de cómputo, realicen este tipo de conductas, pero no contempla un artículo en donde se sancione el acceso no autorizado a sistemas y equipos informáticos."[78]

Es de esta manera que Alemania a partir de varias discusiones teóricas eligió por seguir el camino de la creación de nuevos tipos penales para combatir a la criminalidad informática, conductas que se tipificaron como ya hemos mencionado en la Segunda Ley para la Lucha contra la Criminalidad Económica del 15 de mayo de 1986, incluyendo nuevos preceptos penales en materia informática.

Se puede apreciar que en la legislación alemana, se ha tipificado el acceso ilícito a sistemas y equipos informáticos, en una modalidad de espionaje de datos, pues señala: el que, sin estar autorizado, se procurase para sí o para

[78] Mir Puig, Santiago, ***El Nuevo Derecho Penal Informático en Alemania***, ***Delincuencia Informática,*** Editorial Promociones y Publicaciones Universitarias, Barcelona, 1992, Pág. 105.

otros datos que no están destinados a él y que se hallan especialmente asegurados contra el uso indebido, será castigado con una pena de prisión de hasta 3 años de prisión o pena de multa.

Palazuelos señala que en opinión de estudiosos de la materia, “el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.”[79]

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de que bienes jurídicos merecedores de protección penal resultaban así lesionados. Entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo *modus operandi*, que no ofrece problemas para la aplicación a determinados tipos.

Debemos tener en cuenta que en esta legislación que el mismo medio donde se comete el delito puede servir para rastrear y atrapar al delincuente.

Palazzi da un ejemplo de ello y escribe: “es en el libro *The Cuckoo’s Egg,* de Cliff Stoll, donde el autor narra cómo siguió a lo largo de meses a varios hackers alemanes, que desde Hannover entraban a las redes americanas en

[79] Palazuelos, Silvia Guadalupe, ***Op. Cit.,*** Pág. 74.

busca de información para vender al gobierno ruso. Los ordenadores detectaban a través del rastreo de una clave determinada cuándo estos sujetos ingresaban. A partir de allí grababan todos sus movimientos dentro del sistema incluso llegaron a crear archivos falsos con supuesta información confidencial (con palabras tales como *military secrets)* para atraer a los hackers y poder rastrearlos mientras se encontraban en línea."[80]

Hoy la justicia alemana, ha dado a conocer que podrá perseguir penalmente a los autores de páginas Web racistas o que inciten al odio racial, confeccionadas desde el extranjero, toda vez que jueces de El Tribunal Supremo de Alemania, han discutido que estas páginas Web racistas están especialmente indicadas para alterar la paz social en Alemania, por lo que eso permite perseguir a sus autores.

3.1.5. Argentina.

Los primeros antecedentes de legislación informática, se localizan en materia de propiedad intelectual en la Ley número 11.723, promulgada en virtud del decreto número 165/94 del 8 de febrero de 1994, en donde se considera la acción de borrado o destrucción de un programa de computación. "Argentina propone cubrir el vacío legislativo con la creación de tipos penales para tipificar el acceso ilegítimo informático, el sabotaje informático, así como el fraude."[81]

A continuación se transcribe la ley argentina en materia de delitos informáticos, porque consideramos que es una de las leyes que más aborda y regula esta problemática:

Ley de delitos informáticos.

- **Acceso Ilegítimo Informático:**

[80] ***Cfr.*** Palazzi, ***Op. cit.,*** Pág. 70.
[81] ***Cfr.*** Fernández, Maricel, ***Delitos Informáticos***, La Revista La Ley, Año LXVI, Número 23, Buenos Aires Argentina, Febrero 2002, Pág. 2.

Artículo 1.- Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido. La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

- **Daño Informático**

Artículo 2.- Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Artículo 3.- En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:

1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;

3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

- **Fraude Informático**

Artículo 5.- Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

Disposiciones comunes

Artículo 6.- 1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.

Fundamentos.

La Tecno-era o Era Digital y su producto, la Sociedad de la Información, han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio-económica y provocando un rediseño de la arquitectura de los negocios y la industria. La Informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que, en la doctrina norteamericana, se denomina "computer dependency". Sin la informática las sociedades actuales colapsarían.

Es instrumento de expansión ilimitada e inimaginable del hombre y es a la vez, una nueva de forma de energía, e inclusive, de poder intelectual. Naturalmente que el Derecho, como orden regulador de conductas, no queda exento del impacto de las nuevas tecnologías, destacándose la imposibilidad de

adaptar dócilmente los institutos jurídicos vigentes y los viejos dogmas a estos nuevos fenómenos.

De igual manera, las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución. La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Atendiendo a las características de esta nueva "era" y sus implicancias ya descriptas, consideramos que el bien jurídico tutelado en los delitos informáticos es la información en todos sus aspectos (vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiendo que su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todo sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etcétera).

En definitiva, se entiende por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con su flujo o tratamiento, contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas.

Dentro de estas modalidades de afectación del bien jurídico tutelado, hay tres tipos de delitos básicos, con sus correspondientes agravantes, a saber:

a) El acceso ilegítimo informático o intrusismo informático no autorizado (hacking) que supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad;

b) El daño o sabotaje informático (cracking), conducta ésta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información; y

c) El fraude informático, hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero, que se incluye en esta ley por su propia especificidad que impone no romper la sistemática de este proyecto de ley especial y por la imposibilidad de incorporarla a los delitos contra la propiedad contemplados en el Código Penal.

La ley argentina, abraza el principio de la mínima intervención en materia penal, buscando incriminar únicamente las conductas que representen un disvalor de tal entidad que ameriten movilizar el aparato represivo del estado.

A) Acceso Ilegitimo Informático

Se ha optado por incorporar esta figura básica en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático. Es una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización así se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

En cuanto a los elementos subjetivos de la figura, se añade un ánimo especial del autor para la configuración del tipo, que es la intencionalidad de acceder a un sistema de carácter restringido, es decir, sin consentimiento expreso o presunto de su titular. Se contempla en el segundo párrafo, la pena de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información,

como modalidad más gravosa de afectación del bien jurídico tutelado por la circunstancia que supone la efectiva pérdida de la exclusividad de la información.

Por último, se contempla como agravante de ambas modalidades de esta figura delictiva, la circunstancia que los sistemas o datos informáticos sean concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, en cuyo caso la pena prevista va desde los seis meses hasta los seis años de prisión. En esta hipótesis resulta palmario el fundamento de la agravante por la importancia que los sistemas e información comprometida involucran para el correcto funcionamiento de servicios vitales para la nación, sin los cuales se pondría en jaque la convivencia común, en especial en los núcleos urbanos.

B) Daño o Sabotaje Informático

La jurisprudencia sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño, pues el concepto de cosa es sólo aplicable al soporte y no a su contenido (CNCrimCorrec., Sala 6ta, 30/4/93, "Pinamonti, Orlando M.", JA 1995-III-236). Dicha solución es aplicable también a los datos o información almacenada en un soporte magnético.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, Caballos de Troya, gusanos, cáncer, bombas lógicas y otras amenazas similares.

La figura proyectada constituye un delito subsidiario, ya que la acción de dañar es uno de los medios generales para la comisión de ilícitos, pero esta subsidiariedad está restringida exclusivamente a los casos en que el delito perpetrado por medio de la acción dañosa esté "más severamente penado".

Asimismo, la ley prevé figuras gravadas, previendo especialmente las consecuencias del daño como, por ejemplo, el producido en un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

En segundo término, se protege la información de valor científico, artístico, cultural o financiero de las universidades, colegios, museos y de toda administración publica, establecimiento público o de uso público de todo género. La especialidad de la información protegida y la condición pública o de uso público de los establecimientos amerita agravar la pena en estas hipótesis.

En tercer lugar, la conducta se agrava cuando el daño recae sobre un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Aquí, la trascendencia pública, inmanentes a las obligaciones del estado en materia de seguridad interior y exterior, salud y prestación de servicios públicos, justifican que la sanción penal se eleve por sobre el límite impuesto por la figura básica.

Por último, se contempla como resultado, la producción de una la lesión, grave o gravísima, o la muerte de alguna persona, que pudiere ocurrir con motivo de un daño a un sistema o dato informático, elevándose la pena en función de la elevada jerarquía jurídica que reviste la integridad física de los seres humanos.

Hacemos notar que el Derecho comparado ha seguido los mismos lineamientos, pues frente a la evolución de los sistemas informáticos, las legislaciones penales debieron adaptarse a los nuevos bienes inmateriales.

C) Fraude Informático

Se ha pensado el delito de fraude informático como un tipo autónomo y no como una figura especial. En este sentido, se entendió que en el fraude informático, la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude: el ánimo de lucro y

el perjuicio patrimonial fruto de una transferencia patrimonial no consentida sin que medie engaño ni voluntad humana viciada. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial.

El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

D) Disposiciones Comunes.

Como artículo 6°, bajo el título de Disposiciones Comunes, se ha creído necesario, por el tipo de ley especial de que se trata, redactar un glosario que facilite la comprensión de la terminología utilizada por esta ley.

Se definen en las disposiciones comunes, los dos términos centrales, en torno a los cuales giran los tipos definidos, con el mayor rigorismo a los fines de acotar los tipos en salvaguarda del principio de legalidad, pero, a la vez, con la suficiente flexibilidad y vocabulario técnico, con el objeto de no generar anacronismos en razón de la velocidad con la que se producen los cambios tecnológicos, tratando de aprehender todos los fenómenos de las nuevas tecnologías de la información.

Se ha podido comprobar, fruto de debates que se producen en otras latitudes, que la inmensa cantidad de las conductas ilegitimas que se buscan reprimir atentan ya sea contra uno u otro de estos dos conceptos definidos. Consiguientemente se decidió siguiendo la Convención del Consejo de Europa sobre Cybercrimen que, demarcando con nitidez ambos conceptos y haciéndolos jugar dentro de la tipología elegida, se lograba abarcar en mayor medida las

conductas reprochables, sin perder claridad ni caer en soluciones vedadas por principios centrales del derecho penal: a saber, Principio de legalidad y Principio de Prohibición de la Analogía.

Independientemente de lo manifestado, se debe tener presente que sí bien el dato informático o información, tal cual está definido en esta ley especial, es sin duda de un intangible, y que solo o en conjunto con otros intangibles puede revestir cierto valor económico o de otra índole, no debe, por ello, caerse en el error de sin mas asociarlo a lo que en los términos del Derecho de la Propiedad Intelectual se entiende por obra protegida. (*vgr.* software). Si bien una obra protegida por el régimen de la Propiedad Intelectual, puede almacenarse o transmitirle a través de red o de un sistema informático y eventualmente ser objeto de una conducta de las descripta por esta ley, no toda información según se define aquí es una obra de propiedad intelectual y por ende goza del resguardo legal que otorga de dicho régimen de protección especial.

Común a las disposiciones de acceso ilegítimo, daño y fraude informáticos, se ha entendido que el delito se ve agravado cuando quien realiza las conductas delictivas es aquél que tiene a su cargo la custodia u operación del sistema en razón de las responsabilidades y deberes que le incumben, puesto que usa sus conocimientos, status laboral o situación personal para cometer cualesquiera de los delitos tipificados por la presente ley.

Para el tratadista Gabriel Andrés Cámpoli, la legislación argentina sobre los delitos informáticos se detuvo esencialmente en el debate conceptual: “por medio de” y “en contra de”, explicando lo siguiente: los equipos como medios comisivos (por medio de) o como objetos materiales del delito (en contra de). El citado autor, para efecto de una mejor comprensión respecto al debate conceptual que hace, creo las siguientes construcciones gramaticales:

a) Delitos cometidos por medio de aparatos electrónicos.
b) Delitos cometidos en contra de aparatos electrónicos.
c) Delitos cometidos por medio de equipos informáticos.

d) Delitos cometidos en contra de equipos informáticos.

Cámpoli escribe:

"Se observa que sólo los equipos dotados de la capacidad de procesar datos pueden por regla general ser utilizados como medios comisivos de acciones que afecten bienes jurídicos que a la sociedad le pueda interesar brindarle mayor protección (la penal). ¿Entonces que es lo que nos separa de una correcta aplicación de las leyes penales preestablecidas? Sólo la pretendida falta de legislación en materia de delitos informáticos, y digo pretendida porque esto no es así, ya que al perpetrarse el delito a través del uso de medios informáticos no se está sino en presencia de un nuevo método comisivo del delito y no como erróneamente se piensa de un nuevo delito que para que lo sea debe estar correctamente tipificado.

En resumen, los delitos informáticos, en su gran mayoría dependen, para su persecución penal de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, por ejemplo, que si mañana se pudiese quitar la vida a alguien por medio de Internet habría que establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cual sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica."[82]

Argentina es uno de los países que más trabajado en materia de delitos cibernéticos, sin embargo la legislación Argentina, contempla varias figuras penales vigentes que tipifican ciertas conductas ilícitas informáticas, que se encuentran reguladas en diferentes ordenamientos.

[82] ***Cfr.*** Cámpoli, Gabriel Andrés, ***Op. cit.***, Pág. 12-14.

3.1.6. Chile.

En Chile se promulgó en 1993 la Ley 19.223 en la que se estipulan los delitos informáticos.

En dicha ley se establece, que el que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, impida, obstaculice o modifique su funcionamiento, así como aquel que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, o simplemente el que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información sufrirá la pena de presidio menor en su grado medio a máximo.

Al respecto, Rodolfo Herrera Bravo escribe sobre la ley chilena:

“En junio de 1993 entró en vigencia en Chile la Ley 19.223 sobre delitos informáticos, un cuerpo legal que consta de 4 artículos. La Ley 19.223, que, no obstante ser pionera en la región al abordar expresamente el delito informático, adolece de muchas deficiencias de forma y de fondo, que me llevan a considerarla como desafortunada.

1.- Una primera reflexión surge en relación al concepto de delito informático. De la relación entre delito e informática surgen dos tipos de ilícitos, los delitos computacionales y los delitos informáticos. Cuando los delincuentes de delitos tradicionales comienzan a utilizar como un medio específico de comisión a las tecnologías de la información, se produce una informatización de los tipos tradicionales, naciendo el delito computacional, que en realidad se trataría sólo de ilícitos convencionales que ya están regulados en el Código Penal. Sin embargo, también se crean conductas nuevas, no contempladas en los ordenamientos penales por su especial naturaleza, lo que hace necesario crear nuevos delitos, llamados delitos informáticos.

Es así como entendemos por delito informático a la acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información. Por lo tanto, únicamente estaremos ante un delito informático cuando se atenta dolosamente contra los datos digitalizados y contra los programas computacionales contenidos en un sistema; otros casos parecidos, serán sólo delitos computacionales que no ameritan la creación de un nuevo ilícito penal.

Al respecto, la Ley n°19.223 confunde esta distinción y trata como delito informático a algunos delitos computacionales. Esto tiene como consecuencia, que en esos casos en vez de actualizar el tipo tradicional contenido en el Código Penal, que habría sido lo correcto crea una supuesta nueva figura. El problema que produce es comparable con la situación de considerar como delitos distintos el robo de una lámpara y el de una impresora, pese a que se trata de un mismo delito.

2.- Otra idea surge en relación al bien jurídico protegido por los delitos informáticos. En la moción presentada al Congreso se indicó que se buscaba proteger un nuevo bien jurídico: la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

Y respecto al nuevo bien jurídico creado por la Ley n°19.223, es discutible, porque ni el mismo legislador lo entiende con claridad, fue inadecuado aludir a la información en cuanto tal,

Pero donde se aprecia la confusión del legislador con mayor claridad es en el hecho que, si bien se indicó a la información (en la forma incorrecta que explicamos) como el nuevo bien jurídico, durante la tramitación se sostuvo que el sistema informático es un nuevo bien jurídico que se quiere proteger, el cual difícilmente puede asimilarse a otros penalmente protegidos. Es claro el desconocimiento sobre la delincuencia informática, por no distinguir dentro del sistema informático entre el hardware y el software.

Es común observar en parte de la doctrina mucha confusión para determinar el bien jurídico, porque no se limitan exclusivamente a los delitos informáticos, sino que también consideran a los computacionales, que al ser delitos convencionales ya tienen un bien jurídico específico. Por ejemplo, los atentados contra el hardware tienen claramente como bien jurídico al patrimonio.

Y respecto al nuevo bien jurídico creado por la Ley 19.223 es discutible, porque ni el mismo legislador lo entiende con claridad. Citando la opinión del profesor Renato Jijena Leiva, expuesta en el VI Congreso Iberoamericano de Derecho e Informática, fue inadecuado aludir a la información en cuanto tal, sin otorgarle carga o contenido valórico, sin reparar en que no todo conjunto organizado de datos reviste igual importancia Además, la ubicación del texto fuera del Código Penal es una desafortunada técnica legislativa. En la Ley 19.223, no se contemplan las figuras de *hacking* directo o la de fraude informático. Tampoco se refiere a la copia ilegal de programas, cuyo delito se encuentra tipificado en la Ley 17,336 sobre Propiedad Intelectual."[83]

3.2. La problemática de los delitos informáticos en el ámbito nacional.

En el contexto nacional se han dado algunos avances legislativos en materia de delitos informáticos; sin embargo, debemos de señalar que aún el tratamiento de estos delitos es muy precario en México, del análisis legislativo nacional se desprende que con excepción del Código Penal del estado de Aguascalientes, Baja California, Chiapas, Colima, Distrito Federal, Morelos, Oaxaca, Puebla, Sinaloa, Querétaro, Tabasco, Tamaulipas, Zacatecas y en el federal, este tipo de conductas no estarían tipificadas en nuestro país, ya que en ellos se tipifican las conductas ilícitas derivadas del uso de los sistemas informáticos, pues si bien es cierto, que el nivel de informatización nacional no es tan pronunciado como en otros países, al menos es suficiente como para un

[83] ***Cfr.*** Herrera Bravo, Rodolfo, ***Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley chilena 19.223***, ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998.

adecuado análisis y tratamiento por la vía del Derecho, ya que México también ha sido objeto de varios ilícitos cibernéticos, como veremos más adelante.

Como hemos dicho, hoy en día son escasas las legislaciones locales que han incluido en sus catálogos penales los llamados delitos informáticos, pero aún no se ha destacado que la computación suele ser el medio comisivo en la realización de ilícitos ya sancionados, pero con el aspecto de intangibilidad que trae aparejada esta tecnología. Tantos códigos como entidades federativas permiten hoy día el aprovechamiento de estas lagunas legislativas por parte de la nueva delincuencia informática.

Es por ello, que cada vez más existe la necesidad de legislar en materia de delitos informáticos en México, ya que la expansión y considerable demanda entre la población mundial, de las computadoras, dan como resultado un constante incremente en el número de usuarios y como consecuencia de ello el potencial delictivo aumenta en toda la esfera relacionada con la informática, pues es un objeto que se ve principalmente amenazados por delincuentes con habilidad en materia informática.

3.2.1. Código Penal del Estado de Sinaloa.

El Estado de Sinaloa, fue el primero en tipificar este tipo de conductas mediante el decreto 539 publicado en el Diario Oficial número 131 del 18 de octubre de 1992, que incorporó al Código Penal el artículo 217 sobre materia informática con el objeto de prevenir el manejo ilícito de los sistemas informáticos en el Estado, e incluyó en el Título décimo referente a los delitos contra el patrimonio, en el capítulo V, el cual transcribiremos textualmente dada la importancia de éste:

El Código Penal estatal sinaloense establece:

Título Décimo
"Delitos contra el patrimonio."
Capítulo V
Delito Informático.

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

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

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

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

Cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

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

Al respecto Nava Garcés, escribe:

“En Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado. De tal modo que podemos advertir, que la legislatura creadora del artículo en comento tuvo la tarea

de enfrentar el debate sobre el bien jurídico tutelado, debido a las diferentes formas de comisión de los delitos informáticos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad, el honor, la fama pública, la certeza de los actos jurídicos.

Si una persona logra introducirse en el correo electrónico de otra persona, sin el consentimiento de ésta, con el fin de enterase del contenido de las comunicaciones, está claro que no lesiona el bien jurídico patrimonial de la persona afectada.

Sin embargo, consideramos desafortunado el hecho que en una sola fracción se contemplara el elemento subjetivo del injusto en dos ocasiones, pues la conducta requerida consiste en el uso o ingreso a una base de datos, luego señalada de manera casuística, al establecer: sistemas de computadores o red de computadoras o a cualquier parte de la misma. Para establecer los dos elementos aludidos con las fórmulas siguientes:

a) con el propósito de diseñar, ejecutar o alterar un esquema o artificio.

b) con el fin de defraudar, obtener dinero, bienes o información.

Sobre este particular el legislador debió establecer al inciso a) como la conducta y al inciso b) como el elemento subjetivo del injusto, o bien al inciso a) como el medio comisivo.

Por cuanto hace a la fracción II, ésta tiende sólo a prever lo relativo al daño o robo de información, mediante una formulación casuística."[84]

Si bien es cierto, que el Código Penal de Sinaloa es el primero en tipificar a los delitos informáticos en nuestro país, también es el único en incluir la terminología "delito informático".

[84] Nava Garcés, ***Op. cit.***, Pág. 243.

Al respecto el autor Ríos Estavillo sostiene que “este artículo aún cuando se encuentre tipificado en el Código Penal del estado de Sinaloa, no es un delito informático, ya que si bien es cierto que cumple con el elemento de tipicidad al haber encuadramiento de la conducta con la descripción hecha en la ley, también es cierto que no satisface el resto de los elementos formales y materiales que caracterizan a ese tipo de ilícitos, por lo tanto, desde un punto de vista de la técnica penal, sí es delito para el Estado de Sinaloa por estar establecido en su ordenamiento punitivo, pero desde la perspectiva de la técnica informática no llega a plasmar plenamente su descripción.”[85]

Consideramos que en esta ley, se exige que los actos se realicen con le propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información y esto excluye casi la mayoría de las conductas posibles, ya sea por falta de una o de otra condición, puesto que si por ejemplo, quien altera sin fin de defraudar u obtener dinero, bienes o información no queda dentro del tipo y quien con fin de hacerlo ni altera ni diseña ni ejecuta un esquema o artificio tampoco lo está.

3.2.2. Código Penal Federal.

Con fecha 17 de mayo de 1999 se publicaron en el Diario Oficial de la Federación las reformas al Código Penal Federal que incluyeron la creación de tipos penales en materia informática, es de destacarse que el legislador consideró que era necesario proteger la integridad, privacidad y confidencialidad de la información que se encuentra almacenada y procesada en los sistemas y equipos de cómputo, es significativo también resaltar que en la exposición de motivos de esta reforma, el legislador considera a estos nuevos tipos penales como “delitos informáticos”.

Alfredo Sánchez Franco escribe:

[85] Ríos Estavillo, Juan José, ***Op. cit.,*** Pág. 127.

"Este es el caso de la ley penal mexicana, en la que mediante reformas de fecha 17 de mayo de 1999 publicadas en el Diario Oficial de la Federación, se crearon en la especie, los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal, que en lo medular, tipifican comportamientos de los llamados hackers o *crackers* que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. En este cuerpo normativo federal se sanciona el que un sujeto tenga acceso ilegal a dichos sistemas y los altere, dañe, modifique o provoque pérdida de información contenida en tales sistemas.

Sin embargo, en mi opinión, la complejidad y costo económico que representará el acreditar ante un juez penal un comportamiento ilícito que se ejecuta en el escenario virtual de la Internet o el Internet y sus herramientas virtuales, rebasa en mucho, los buenos deseos del legislador mexicano, reflejados en la reforma penal citada."[86]

El gran problema de los llamados delitos informáticos será la comprobación de los mismos, lo que de ninguna manera puede ser un pretexto para su constitución dogmática.

El Código Penal Federal establece:

Título Noveno.
Revelación de secretos y acceso ilícito a sistemas y equipos de informática.
Capítulo II
Acceso ilícito a sistemas y equipos de informática.

ARTICULO 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.

[86] Sánchez Franco, Alfredo Ensayo No. 1 sobre el tema de investigación indicado, en el Master en Derecho Penal, Constitución y Derechos por la Universidad Autónoma de Barcelona, España (U.A.B.), México, 2002-2003.

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.

ARTICULO 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida 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.

ARTICULO 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida 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.

ARTICULO 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida 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.

ARTICULO 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 pérdida 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 artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 211 bis 6.- Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este Código.

ARTICULO 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Jesús Antonio Molina Salgado hace una crítica sobre esta legislación:

“La legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país. Algunos de los defectos del Código Penal Federal en esta área son los siguientes:

a) Contempla que constituye el delito sólo si se accede un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los

medios económicos para proteger su computadora con un mecanismo de seguridad. ¿O qué acaso el que tu computadora esté conectada al Internet significa que cualquiera puede justificadamente, borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad?

b) El Código Penal no define qué debe entenderse por mecanismo de seguridad. ¿Qué es un mecanismo de seguridad de un sistema informático?, ¿Un *password*? ¿Un candado contra robo (físico)?, ¿Un *firewall*?, ¿Un sistema criptográfico de llave pública?, o simplemente ¿Tener la computadora encerrada en un cuarto bajo llave o con un guardia de seguridad a un lado?. Esta vaga redacción sin duda traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.

c) Nuestro código no contempla todos los tipos más comunes de ataques informáticos. El Capítulo II adicionado en virtud de la reforma del 17 de mayo de 1999, de entrada está titulado de manera incorrecta: Acceso Ilícito a Sistemas y Equipos de Informática. Aunque su articulado (Arts. 211 bis 1 al 7) no habla en todo momento de acceso ilícito, el título del capítulo sí enfoca su contenido a accesos ilícitos precisamente.

El problema radica en que muchos ataques informáticos se perpetran sin necesidad alguna de acceder directamente un sistema informático. El mejor ejemplo es el ataque de Denegación de Servicios (Denial of Services o Distributed Denial of Services), cuyo objetivo no es modificar, destruir o provocar pérdida de información, como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar un servidor temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas mientras el servidor está caído."[87]

Si bien es cierto que organizaciones delictivas realizan este tipo de conductas, también es cierto que existen particulares que no obtienen provecho alguno con el acceso a ciertos bancos de información. Volvemos al caso de quien

[87] Molina Salgado, Jesús Antonio, ***Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial,*** Colección: Breviarios Jurídicos, Porrúa, México, 2003, Pág. 69-70.

ingresa de manera ilícita a la cuenta de correo electrónico de otra persona, para conocer el contenido de sus comunicaciones, lo único transgredido es la intimidad del dueño de la cuenta, aunque no haya manifestación o indicio del acceso clandestino.

Por cuanto hace al conjunto de normas penales, debemos decir que es un buen inicio para combatir esta clase de delincuencia, elevando a nivel federal este tipo de conductas, sin embargo, debe existir un trabajo para que todo cuanto se refiera a la materia informática sea de competencia federal, frente a legislaciones como la sinaloense, o contra el intento de legislación del Distrito Federal.

Regularmente bajo el título que corresponda dentro del Código Penal, se establece el bien jurídico que tutela, por ejemplo “Delitos contra la vida y la integridad corporal”, Delitos contra la moral pública y las buenas costumbres” “delitos contra la salud”, etc., en el caso que nos ocupa, el título señala: “Revelación de secretos y acceso ilícito a sistemas y equipos de informática. Esto, no deja en claro cuál es el bien jurídico tutelado y esto ocurre porque si el fin fuera proteger el patrimonio, entonces la ubicación de los delitos sería errónea, a pesar de que, dentro de los mismos se establece, entre otras conductas, el daño a los sistemas.

Es importante señalar que en este tipo de legislaciones, no se especifica qué se debe entender por sistema o equipo de informática, y éstos sólo podrán ser tutelados por la ley punitiva si se encuentran protegidos previamente por un mecanismo de seguridad. Ante la multiplicidad de formas que puede tener el uso de la tecnología informática, debe realizarse una disposición general que abarque al uso de las computadoras como el medio comisivo y, en ese contexto, instrumentar los convenios internacionales para sancionar este tipo de conductas en la escala en que suceden.

Sin embargo, con todo y sus defectos o vicios, esta conducta o actividad ilícita es sancionable en los términos señalados en el mismo Capítulo II del Código Penal Federal, las acciones relacionadas con este llamado delito informático

pueden, como en el caso de cualquier delito federal, iniciarse por medio de la presentación de una querella o una denuncia de la parte ofendida ante las autoridades judiciales.

A raíz de esta incipiente regulación en el Código Penal Federal de delitos informáticos y como consecuencia de la creciente ola de ilícitos en este rubro, a nivel estatal esta surgiendo la voluntad de normar lasa conductas criminógenas relacionadas con los medios informáticos, como es el caso del Código Penal del Estado de Sinaloa.

Esta voluntad de regular los ilícitos informáticos es sin duda un gran avance por parte de nuestros legisladores. No se debe olvidar sin embargo, que existen muchos otros ilícitos relacionados con la informática que pueden y deben también ser considerados para regulación y sanción por parte de las leyes penales.

Por otra parte, el Código Penal Federal contempla en el título Vigésimo Sexto concerniente a los “Delitos en materia de Derechos de Autor”, otra conducta que podría considerarse como delito informático, aunque no esta tipificada como tal, es el caso del artículo 424 bis fracción II, en cuyo texto se tipifica la conducta que tenga como propósito de fabricar con una finalidad lucrativa un dispositivo o sistema cuyo objetivo sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Asimismo, es importante señalar que al realizarse la reforma a la Ley Federal de Derechos de Autor el 24 de diciembre de 1996, misma que entro en vigor el 24 de marzo de 1997, se incorporó a este ordenamiento la protección de las creaciones en materia informática como serían los programas de computación y las bases de datos, ley que protege y reconoce los derechos de autor respecto a estos programas de cómputo y de compilaciones como serían, las bases de datos.

3.2.3. Nuevo Código Penal para el Distrito Federal.

Cabe también destacar que la forma realizada el día 17 de septiembre de 1999, al Código Penal para el Distrito Federal, adicionó una fracción que sanciona la conducta que realice un acceso ilícito o no autorizado a los sistemas o programas de informática del sistema financiero, sin embargo, dicha fracción no es más que una supuesta figura de fraude informático, fracción que contempla el artículo 231 fracción XVI del Nuevo Código Penal para el Distrito Federal y que hoy es tema del presente trabajo, mismo que será analizado en el próximo capítulo y el cual transcribiremos textualmente dada la importancia de éste:

En el Nuevo Código Penal para el Distrito Federal se lee:

Capítulo III
Fraude.

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

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

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

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

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

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

[...]

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

Es importante señalar, que aún cuando nuestro Código Penal, no establece que se trate de una conducta equiparada al fraude, se entiende que estamos en presencia de este tipo de conducta, al ubicarla el legislador inmediatamente después del delito de fraude, estableciendo que se le impondrán las penas previstas en el artículo anterior, de lo cual consideramos un primer error. Pues el acceso ilícito a un sistema informático, no es de ninguna manera sinónimo de un engaño (elemento requerido en el tipo básico de fraude), pues al efecto, las máquinas por su propia naturaleza no son susceptibles de caer en este tipo de errores o falsas concepciones de la realidad, como sucede con las personas físicas.

Maggiore establece lo siguiente: "para engañar a alguien se requiere, la posibilidad de caer o no en ese engaño, tener la capacidad para reconocer el error, lo que de ninguna manera acontece con los sistemas computacionales, hasta el día de hoy; de tal modo que se hace imposible que los elementos de esa índole que conforman la estructura del fraude: error, falsa representación, engaño, motivación, voluntad, decisión, disposición, puedan actualizarse en un sistema carente de las condiciones psicológicas correspondientes."[88]

El acceso ilícito a un sistema informático, con el fin de realizar operaciones, transferencias o movimientos de dinero o valores, no puede

[88] Maggiore, Giuseppe, ***Derecho Penal,*** Vol. I, 2ª reimpresión de la 2ª Edición, Editorial Temis, Bogotá, Colombia, 2000, Pág.125.

considerase como una especie de fraude, sino de robo, un robo por medio electrónico o informático en el que se utiliza a la computadora como herramienta o medio comisivo, para transferir dinero (acto de disposición), problemática que abordaremos en el siguiente capítulo y que es el tema principal de este trabajo de investigación por la importancia que tiene, debiera ser observada para una futura y correcta reforma, en la que no existan tantas lagunas legislativas para sancionar penalmente una conducta.

Es así, que la propuesta del presente trabajo se enfoca a ubicar correctamente el artículo en comento, como veremos más adelante, no se trata de un equiparable a fraude como erróneamente lo han establecido nuestros legisladores, sino que estamos en presencia de un delito de robo por medio electrónico o informático, en el que la computadora es el medio o instrumento para la comisión de conductas ilícitas.

Como ya se ha mencionado, la computadora no es susceptible de engañársele, ésta funciona bajo instrucciones o comandos que le son dadas por una persona, las cuales se materializan bajo un programa,[89]por lo tanto una computadora depende en su totalidad de las instrucciones que le son dadas, mismas que no pueden ser erróneas o falsas, pues una computadora no acepta datos falsos para poder tener acceso a ella, por tal motivo resulta equívoco pensar que para tener acceso a una computadora, se haga por medio del engaño.

De acuerdo a lo dispuesto por el artículo 230 del Nuevo Código Penal para el Distrito Federal, comete delito de fraude, el que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, por lo que nos queda muy claro, que el supuesto que marca la fracción XIV del artículo 231, corresponde al delito de robo que se da por un medio electrónico, siendo su conducta típica el apoderamiento de la cosa (dinero o valores), sin consentimiento

[89] Entendiéndose por "*Programa*", el conjunto de instrucciones que dirigen a una computadora para la ejecución de una serie de operaciones, con el objetivo de realizar tareas específicas.

de quien legalmente puede otorgarlo (sistema financiero), pero este tema lo abordaremos de manera amplia en nuestro próximo capítulo, en el que haremos un análisis dogmático del artículo 231 fracción XIV.

Recientemente la Suprema Corte de Justicia de la Nación, se pronunció sobre el particular, pero refiriéndose a la incompetencia de la Asamblea Legislativa para crear leyes que se refieran al sistema financiero mexicano, lo cual es otro problema que se presenta en el artículo que se analiza, al ubicarlo el legislador en el Nuevo Código Penal para el Distrito Federal, siendo lo correcto ubicarlo en el Código Penal Federal, por lo tanto proponemos, su adecuada ubicación en la legislación penal federal.

Este criterio se apoya en la jurisprudencia que sostiene la Segunda Sala de la H. Suprema Corte de Justicia de la Nación, visible en el Semanario Judicial de la Federación, Época 5a., Tomo XXXII, página 2021, cuyo tenor literal es el siguiente:

> ***INSTITUCIONES DE CRÉDITO, LEGISLACIÓN SOBRE LAS.-*** *La soberanía de las entidades de la Federación se encuentra limitada por las estipulaciones de la Constitución; y en materia de instituciones de crédito, sólo el Congreso de la Unión tiene facultades para legislar, según lo establece el artículo 73, fracción X, de la Constitución Federal. Si corresponde al Congreso de la Unión la facultad de legislar en materia de intermediación y servicios financieros, compete también a las autoridades federales, esto es, al presidente de la República, reglamentar las leyes que al efecto se dicten y emitir actos administrativos, ya sean generales o individuales a las dependencias del Poder Ejecutivo Federal (Secretaría de Hacienda y Crédito Público y Comisión Nacional Bancaria y de Valores), por lo que en tal virtud, al haber expedido el Reglamento de Seguridad y Protección Bancaria para el Municipio de Guadalajara, el H. Ayuntamiento de ese Municipio ha incurrido en una clara invasión de la esfera de competencia federal, procediendo en consecuencia, se resuelva por parte de esa H. Suprema Corte de Justicia de la Nación que dicho reglamento resulta violatorio de la Constitución General de la República.*

El 17 de junio de 2003, pudimos leer lo siguiente: “La Suprema Corte de Justicia de la Nación declaró inconstitucional el delito de “fraude por acceso informático al sistema financiero” incluido indebidamente por la Asamblea

Legislativa del Distrito Federal en el Código Penal capitalino. Por tres votos contra dos y luego de una cerrada discusión que tomó cuatro sesiones, la primera Sala de la Corte consideró que por ser una conducta que afecta al sistema financiero, únicamente el Congreso de la Unión puede legislar sobre el tema.

Los Ministros de la mayoría declararon que el artículo 387 fracción 22 del anterior Código Penal es inconstitucional, ante la falta de competencia legal de la Asamblea Legislativa del Distrito Federal para regular esta materia."[90]

3.2.4. Policía cibernética en México.

En México, tomando en cuenta la dificultad probatoria de los delitos informáticos, se ha formado la Coordinación Interinstitucional de Combate a Delitos Cibernéticos formado por: la Presidencia de la República, la Procuraduría General de la República, la Procuraduría General de Justicia del Distrito Federal, la Policía Federal Preventiva, el Centro de Investigación y Seguridad Nacional, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Seguridad Pública (a través de la Policía Federal Preventiva), E-México, la Universidad Nacional Autónoma de México, la Asociación Mexicana de Internet, la Secretaría del Trabajo y Previsión Social, Teléfonos de México, Avantel, Alestra y la Alianza Mexicana de Cibercafés, A.C.

3.2.4.1. Antecedentes de la Policía Cibernética.

Ejerciendo sus atribuciones legales y para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

[90] Fuentes, Víctor, "Revocan reforma sobre fraude cibernético", en el Diario Reforma, México, 17 de junio de 2003.

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de cómputo, el *hackeo,* la venta de armas y drogas por Internet y el ciberterrorismo las cuales son amenazas para la sociedad.

La Secretaría de Seguridad Pública mediante la Policía Federal Preventiva, contribuye con su granito de arena para proteger el entorno de la red Internet y en ese esfuerzo, requiere apoyo de la ciudadanía por lo que invitamos a los que quieran proteger a los niños en particular, y sobre todo a los interesados en la seguridad de la red, hagan contacto con nosotros para que nos ayuden.

3.2.4.2. Actividades de la Policía Cibernética.

- “Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos utilizando computadoras.
- Realización de operaciones de patrullaje anti-hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

- Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve una cultura de legalidad, respeto y seguridad en la red.
- Integrar un equipo especializado en delitos cibernéticos a fin de hacer este medio electrónico un lugar seguro para el intercambio de información. Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.
- Utilizar Internet como un instrumento para identificar a los delincuentes que cometen este tipo de delitos.
- Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.
- Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.
- Ofrecer seguridad en la navegación en la Internet para los menores, ya que existen peligros en ella.
- Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.
- Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.
- Identificar y combatir el crimen organizado dedicado al tráfico de menores.
- Establecer técnicas adecuadas para la búsqueda y localización oportuna de niños extraviados, perdidos y/o robados.
- Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.
- Desintegrar y proponer a disposición del Agente del Ministerio Público a las bandas de pedófilos dedicadas a la explotación sexual de menores y a la pornografía infantil.

- Acciones de operación con autoridades locales, federales e internacionales."[91]

3.2.4.3. Propuestas de la Policía Cibernética.

La Policía Cibernética da una serie de propuestas para prevenir este tipo de ilícitos en nuestro país.

a) Capacitación constante del personal en investigaciones de alta tecnología y técnica forense.

b) Promoción de una cultura de la seguridad respecto a delitos cibernéticos.

c) Fomentar la creación, desarrollo y capacitación de unidades policiales de los tres niveles de gobierno para el combate a delitos cometidos por computadora y en contra de menores de edad.

d) Base de datos sobre incidencia y análisis de delitos involucrando equipos y sistemas de cómputo.

e) Cooperación pública y privada, local e internacional.

f) Legislación cibernética debe determinar las actividades criminales a perseguir.

g) Penalizar como grave cualquier delito cibernético.

h) Obligar la restitución del daño a la víctima.

Llegamos a la conclusión, de que esta nueva Policía Cibernética desarrolla una Base de Datos Nacional para la identificación de patrones, rangos, preferencias y *modus operandi* de los casos reportados de menores extraviados, desaparecidos, abusados sexualmente, explotados, traficados y prostituidos, además de la integración de un Banco Nacional de Datos sobre pedofilia y agresores sexuales.

Realmente este tipo de policía atiende a la parte más visible que pasa por la Internet, puesto que revisa, navega, por las páginas en las que se muestran

[91] Consultable en www.ssp.gob.mx.

imágenes de pornografía infantil. Luego de detectarlas, busca los enlaces hasta descubrir desde que servidor se generan dichas imágenes. Si éste último se encuentra en territorio nacional, entonces lo informa al Ministerio Público de la Federación para que se inicie la averiguación previa correspondiente y con ello se requiera al juzgador para que obsequie la orden de cateo a efectuarse en el lugar donde se generan las imágenes. Solo entonces se encontrará al responsable y, tal vez a quienes agredieron sexualmente a los menores involucrados en las imágenes. También, como se trata de páginas electrónicas donde suele requerirse el depósito de dinero mediante la aportación de datos de la tarjeta de crédito, se rastrea la cuenta concentradora y así conocer la identidad de quien recibe (y quien potencialmente es el autor de esto) el dinero por permitir el acceso a la página electrónica.

CAPÍTULO IV

ANÁLISIS DOGMÁTICO DEL ARTÍCULO 231 FRACCIÓN XIV DEL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

4.1. Tipo penal descrito en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal.

Antes de desarrollar el tipo penal descrito en el artículo 231 fracción XVI del Nuevo Código Penal para el Distrito Federal, resulta necesario establecer que el mismo se encuentra ubicado en el Titulo Décimo Quinto de los Delitos contra el Patrimonio, inmediatamente después del delito de fraude.

En el Nuevo Código Penal para el Distrito Federal se prevé lo siguiente:

Capítulo III
Fraude.

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

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

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

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

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

Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores.

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

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

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

III. Venda a dos personas una misma cosa, sea mueble o inmueble, y reciba el precio de la primera, de la segunda enajenación o de ambas, o parte de él, o cualquier otro lucro, con perjuicio del primero o del segundo comprador;

IV. Al que se haga servir alguna cosa o admita un servicio en cualquier establecimiento comercial y no pague el importe debidamente pactado comprobado;

V. En carácter de fabricante, comerciante, empresario, contratista o constructor de una obra, suministre o emplee en ésta materiales o realice construcciones de calidad o cantidad inferior a las estipuladas, si ha recibido el precio convenido o parte de él, o no realice las obras que amparen la cantidad pagada;

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

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

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

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

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

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

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

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

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

En este caso, es aplicable lo dispuesto en el párrafo segundo de la fracción anterior. Las instituciones y organismos auxiliares de crédito, las de fianzas y las de seguros, así como los organismos oficiales y descentralizados autorizados legalmente para operar con inmuebles, quedan exceptuados de la obligación de constituir el depósito a que se refiere la fracción anterior.

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

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

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

4.2. Análisis dogmático del artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal.

Es importante señalar, que aún cuando nuestro Código Penal, no establece que se trate de una conducta equiparada al fraude, se entiende que estamos en presencia de este tipo de conducta, al ubicarla el legislador inmediatamente después del delito de fraude, estableciendo que se le impondrán las penas previstas en el artículo anterior, lo que consideramos un primer yerro legislativo.

El acceso a un sistema informático no es de ninguna manera sinónimo de un engaño (elemento requerido en el tipo básico de fraude), pues al efecto, las máquinas, por su propia naturaleza no son susceptibles de caer en este tipo de errores o falsas concepciones de la realidad, como sucede con las personas físicas. En el fraude, se dan dos conductas, la primera es el engaño y la segunda es el aprovecharse del error, teniendo como resultado el alcanzar un lucro indebido, cuestión que no sucede que en este tipo penal que hoy se analiza.

Es necesario analizar desde luego la estructura del delito contemplado en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, desde esa perspectiva podremos apreciar su conformación así como sus alcances, pues una de las mayores preocupaciones de la sociedad es enfrentarse a una conducta antisocial que, aun cuando es catalogada y reprochada, no se encuentra tipificada como delito.

4.2.1. Concepto de delito.

En ocasiones, parecen existir nuevos delitos no comprendidos en nuestro código punitivo, sin embargo, vistos a la luz de su propia esencia encontramos que la tecnología no es una forma de nueva conducta, sino un medio para ejercitar las ya conocidas.

Para ello, es necesario recurrir a la Teoría del Delito. El tratadista argentino Eugenio Zaffaroni en su *Manual de Derecho Penal,* señalaba el doble

valor que posee la Teoría del Delito, primero por su utilidad y segundo, por su necesidad, así escribió: "se llama teoría del delito a la parte de la ciencia del Derecho Penal que se ocupa de explicar qué es el delito en general, es decir cuáles son las características que debe tener cualquier delito."[92]

Por su parte, Giuseppe Maggiore ubica a esta teoría dentro de la Teoría General del Derecho: "Si la teoría del delito es ciencia, con los mismos títulos que la ciencia general del Derecho, debe tener una estructura sistemática y una organización lógica que respondan a criterios de rigurosa necesidad, sin embargo, las dificultades pueden ser superadas, si tenemos presente que la teoría del delito, como la del derecho, depende de la lógica."[93]

Esto es, que a través de la lógica entraremos al estudio de aquellos caracteres que tiene todo delito.

El delito una vez comprendido desde esta perspectiva y aun cuando todavía no ha quedado definido, debe observarse como un ente propio de la ciencia del derecho, que contendrá aquellas conductas humanas tachadas de antisociales, en un tiempo y espacio determinados. Para la lógica quedan las tareas de definir y de dividir al delito como tal, entendiendo que al definir, establece cuáles son sus aspectos esenciales y al dividir, clasifica al delito por dichos caracteres.

La palabra delito deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley.

Al respecto, el doctor Castellanos Tena señala: “para Carrara el delito no es un ente de hecho, sino un ente jurídico, porque su esencia debe consistir

---

[92] Zaffaroni, Eugenio Raúl, ***Manual de Derecho Penal***, Parte General, 4ª Reimpresión de la 4ª Edición, Cárdenas Editor y Distribuidor, México, 1998, Pág. 333.
[93] Maggiore, Giuseppe, ***Derecho Penal***, Vol. I, 2ª reimpresión de la 2ª edición, Temis, Bogotá, Colombia, 2000, Pág. 268.

necesariamente, en la violación del Derecho, llama al delito infracción de la ley, en virtud de que un acto se convierte en delito únicamente cuando choca entre ella, pero para no confundirlo con el vicio, o sea el abandono de la ley moral afirma su carácter de infracción a la ley del estado y agrega que dicha ley debe ser promulgada para proteger la seguridad de los ciudadanos, pues sin tal fin carecería de obligatoriedad, pues da seguridad a los ciudadanos."[94]

Para Edmundo Mezger, el delito "es una acción típicamente antijurídica y culpable."[95]

Mientras que Cuello Calón dice que el delito es: "la acción humana antijurídica, típica, culpable, y punible."[96]

Por su parte, Jiménez de Asúa define al delito como "como el acto típicamente antijurídico, culpable sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal."[97]

Francisco Carrara, principal exponente de la Escuela Clásica, define al delito "como la infracción de la ley del estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso."[98]

En el Nuevo Código Penal para el Distrito Federal, se suprime la definición que contemplaba el artículo 7° del anterior, Código Penal para el Distrito Federal, y que contempla el artículo 7° del Código Penal Federal:

Artículo 7º.- Delito es el acto u omisión que sancionan las leyes penales.

---

[94] Castellanos Tena, Frenando, ***Lineamientos elementales del Derecho Penal,*** 45ª Edición, Porrúa, México, 2004, Pág. 125.
[95] Mezger Edmund, citado por Jiménez de Asúa Luis, ***Lecciones de Derecho Penal,*** Editorial Pedagógica Iberoamericana, México 1995, Pág.133.
[96] Cuello Calón, Eugenio, citado por Castellanos Tena, ***Op. cit.***, Pág. 129.
[97] Jiménez de Asúa Luis, ***Teoría del Delito,*** Editorial Iure Editores, México 2003, Pág.5.
[98] Carrara Francisco, citado por Castellanos Tena, ***Op. cit.***, Pág.125.

En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar precedente.

Actualmente en el Nuevo Código Penal para el Distrito Federal, sólo se habla en su Capítulo I, del Título Segundo, Libro Primero, de las formas de comisión del delito que analizaremos más adelante, lo cierto es que ahora, con éste nuevo código, será aún más difícil contemplar los nuevos delitos o mejor dicho los nuevos medios para ejercitar conductas ilícitas ya conocidas, como lo es la tecnología, lo que consideramos una falta frente al problema que ahora abordamos y que requiere no sólo la protección nacional sino internacional, debido al impacto que ha tenido.

En este orden de ideas, sólo la conducta del hombre puede cometer un delito, pero para que esa conducta sea considerada como delito debe adecuarse a un tipo penal, por lo tanto debe una conducta forzosamente estar tipificada en un ordenamiento punitivo para ser considerada como delito.

Por lo tanto, debemos entender por "tipo" la descripción que el legislador hace de una conducta en un precepto con el propósito de tipificar las conductas que sean consideradas delictivas, por lo que el tipo penal, lo define Eugenio Zaffaroni como el "instrumento legal, lógicamente necesario y de naturaleza predominante descriptiva, que tiene por función la individualización de conductas humanas penalmente relevantes (por estar penalmente prohibidas)."[99]

Por lo anterior, consideramos conducente volver hacer mención de algunos conceptos que sobre delito informático hemos abordado con mayor profundidad en el Capítulo II, esto con el objeto de tener más claro este término del cual hacemos referencia en reiteradas ocasiones en el presente trabajo.

[99] Zaffaroni, Eugenio Raúl, ***Op. cit.***, Pág.391.

Como ya lo hemos visto, se considera que no existe una definición propia de los delitos informáticos, sin embargo muchos expertos en el tema se ha ocupado de proporcionar un concepto de delito informático, aún cuando no existe una definición con carácter universal.

Téllez Valdés, nos dice que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos-penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, aún no ha sido objeto de tipificación, sin embargo y habida cuenta de la necesidad de esto, se hace el distingo pertinente entre lo típico y lo atípico.

Así dependiendo del caso, los delitos informáticos son actos ilícitos en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico).

Palazzi, adopta la definición realizada por un grupo de expertos de la Organización para la Cooperación y el Desarrollo Económico (OCDE) que define al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos, la ventaja de esta definición es que no sólo se limita al delito informático sino a toda la delincuencia relacionada con la informática y las nuevas tecnologías. Establece, que para precisar el concepto de delito informático se debe determinar qué papel juegan las computadoras en estos hechos ilícitos, prácticamente cualquier delito del Código Penal, desde el homicidio hasta el delito de balance falso pueden presentar alguna relación con la informática.

Para María de la Luz Lima, el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las

computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.

Davara Rodríguez, dice que el delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada acabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea a sea hardware o software.

Carlos M. Correa, puntualiza: "el uso de las computadoras, y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador."[100]

Tomando elementos de las definiciones anteriores, nos hemos permitido formular un concepto de *delitos informáticos*, como aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático que para su realización, se valen de las computadoras como medio o fin.

Debe destacarse, que el concepto de delito informático se ha caracterizado por ser la acción delictiva en la cual la computadora es solo el instrumento para cometer el ilícito, es importante subrayar que la mayoría de los autores coinciden en que es indispensable apelar, para que estas conductas sean sancionadas y así evitar que estas acciones queden impunes, así como tipificar estas nuevas conductas que se presentan con el avance de las nuevas tecnologías y de esta manera crear nuevo tipos penales o adecuarlos en los tipos ya tradicionales.

[100] Correa, Carlos, ***Op. cit***, Pág. 295.

4.2.2. Clasificación de los delitos.

El jurista mexicano Fernando Castellanos Tena, realizó una síntesis de la clasificación de los delitos, misma que ha reproducido con claridad y sencillez, por lo que a continuación, se señalan las diferentes clasificaciones que se han hecho del delito, atendiendo los siguientes criterios:

a) En función de su gravedad.

De acuerdo a la gravedad de las infracciones penales, se han hechos diversas clasificaciones. Según una división tripartita se clasifican en *crímenes, delitos* y *faltas*.

Entendiéndose por *crímenes* las conductas antisociales propiamente dichas, es un episodio que tiene un principio, un desarrollo y un fin en el proceso de la conducta del agente, en esta división se consideran crímenes los atentados contra la vida.

Por *delitos* entendemos las conductas así establecidas por la legislación penal y las *faltas* serán las infracciones de orden administrativo como los reglamentos, para el Código Penal sólo existen delitos, quedando la sanción de las faltas, en la esfera de competencia de las autoridades administrativas.

De acuerdo a ésta clasificación, el artículo 231 fracción XIV, es un delito porque se encuentra establecido como tal, por nuestra legislación penal del Distrito Federal.

b) Según la conducta del agente.

Por la conducta del agente o la manifestación de la voluntad, los delitos pueden ser de *acción* y de *omisión.*

Los de *acción* se cometen mediante un comportamiento positivo, en ellos se viola una ley prohibitiva, es decir, es una actividad encaminada a efectuar un

resultado típico, los delitos de acción se presentan cuando el agente incurre en una actividad o hacer, la conducta típica consiste en un comportamiento positivo, por ejemplo el robo por apoderamiento, el homicidio por estrangulamiento.

Por lo que hace a los delitos de *omisión*, "estos delitos constituyen figuras delictivas que se integran solo con el no hacer exigido por la ley penal que implica la conducta omisiva del deber jurídico, con el cual el agente, no evita la lesión al bien jurídico protegido."[101]

"En los delitos de omisión el objeto prohibido es una abstención del agente, consiste en la no ejecución de algo ordenado por la ley, estos violan una ley dispositiva, en tanto los de acción infringen una prohibitiva." [102]

La conducta consiste en una inactividad, la omisión se integra por medio de la abstención del agente de no hacer algo, a su vez, los delitos de omisión se subdividen en *omisión simple y comisión por omisión*.

En los de *omisión simple*, sólo hay una violación jurídica, no se produce un resultado material por la omisión del agente, son delitos de resultado formal solamente, mientras que los delitos de *comisión por omisión* consisten en una abstención que producen un resultado material, dicho en otros términos, es una inactividad por parte del agente que tiene como resultado, un daño al objeto jurídico, a modo de ejemplo se cita el caso de una enfermera que priva de la vida a un paciente por no administrarle un medicamento que es vital para su sobre vivencia.

La acción implica un comportamiento positivo, los delitos de omisión implican una penalidad a la abstención del agente y la comisión por omisión implica un deber incumplido. Edmundo Mezger, explica las formas de la acción; el hecho de comisión y el hecho de omisión de la siguiente manera:

---

[101] Malo Camacho, Gustavo, ***Derecho Penal Mexicano,*** 2ª Ed., Porrúa, México, 1998, Pág. 312.
[102] Castellanos Tena, ***Op. cit.***, Pág.135.

"El hecho punible como acción en sentido amplio abarca dos formas de conducta humana: los hechos de comisión (actividad positiva) y los hechos de omisión (conducta pasiva, omisión). La acción en sentido amplio abarca ambos hechos, y en sentido estricto solamente los hechos de comisión. Aún el uso que se hace de la palabra acción en la vida cotidiana tiene este doble significado: la madre que deja morir de hambre a su hijo (mediante omisión) comete una acción (en sentido amplio), pero ella no mata a su hijo con una acción (en sentido estricto), sino con una omisión."[103]

En el caso típico que nos ocupa, sustentamos que es un delito de *acción*, en virtud de que el sujeto activo tendrá que manifestar su conducta mediante un comportamiento positivo, la conducta típica se exterioriza mediante una acción y nunca por una omisión, este tipo de delito no pude ser de omisión, por el tipo de conducta que lleva a cabo el agente, forzosamente para realizar el acceso ilícito a un sistema de cómputo, es indispensable que el sujeto activo realice o haga uso de un comportamiento para dar una serie de instrucciones, disposiciones y ordenamientos técnicos a través de los comandos de la computadora y de esta forma poder tener acceso al sistema o equipo de informática del sistema financiero que haya decidido el sujeto activo acceder, e indebidamente realice operaciones, transferencias o movimientos de dinero o valores.

c) Por el resultado.

Los delitos se clasifican en *formales* y en *materiales*. "Los delitos formales también se les denomina delitos de simple actividad o de acción y a los materiales se les llama de resultado o de resultado material."[104]

Lo anterior, se da según los cambios producidos por el mundo fenomenológico, esto es, los delitos *formales* son aquellos en los que sólo hay un resultado jurídico, se agota el tipo penal en el movimiento corporal, o en la omisión

[103] Mezger, Edmund, ***Derecho Penal***, *Parte General*, 2ª Edición, Cárdenas Editor y Distribuidor, México, 1990, Pág. 103.
[104] Castellanos Tena, ***Op. cit.***, Pág.137.

del sujeto, son delitos de mera conducta ya que se sanciona la acción u omisión en sí misma, no es necesario que se produzca una alteración en la estructura o funcionamiento del objeto material. Los autores ejemplifican el delito formal con el falso testimonio, la portación de arma prohibida.

Al respecto, Porte Petit señala que "existe un resultado material cuando se produce una mutación en el mundo exterior de la naturaleza, física, fisiológica, psíquica o económica descrita por el tipo."[105]

En cambio, en los delitos *materiales* hay una transformación de las cosas en el mundo fenomenológico, siendo aquellos en los cuales para su integración se requiere la destrucción o alteración de la estructura o del funcionamiento del objeto material, por ejemplo el homicidio, daño en propiedad ajena.

El delito contemplado en el artículo 231 fracción XIV, es un delito de *resultado material,* porque se exterioriza con el comportamiento del sujeto activo, provocando la disminución o alteración del patrimonio del sujeto pasivo.

d) Por el daño o lesión que causan.

Los delitos se clasifican según la forma de afectar al bien jurídico y pueden ser de *daño* o de *peligro*.

Se dice que un delito es de *daño* o lesión "cuando causan un daño directo y efectivo en el bien jurídicamente tutelado por la norma penal violada."[106]

Para el penalista Malo Camacho en estos delitos la conducta típica "genera la afectación por vía de la destrucción o disminución o molestia de un bien jurídico."[107]

---

[105] Porte Petit Candaudap, Celestino, ***Apuntamientos de la parte general del Derecho Penal,*** 18ª Edición, Porrúa, México, 1999, Pág. 260.
[106] Pavón Vasconcelos, Francisco, ***Manual de Derecho Penal Mexicano,*** 13ª Edición, Porrúa, México, 1994, Pág. 265.
[107] Malo Camacho, Gustavo ***Op. cit.***, Pág. 317.

Los de *peligro*, son aquellos delitos en los cuales el resultado consiste en una amenaza de daño para el bien jurídicamente protegido, por lo tanto no se causa una destrucción, sólo una amenaza, por lo tanto no causan un daño directo, sólo los ponen en peligro, como el abandono de personas.

En el caso del artículo 231 fracción XIV, la afectación que sufre el objeto jurídico es de *daño*, porque el sujeto activo al acceder ilícitamente a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, causa un daño directo al bien jurídicamente tutelado por la norma penal, que en este caso es el patrimonio de cualquiera de las instituciones que conformen el sistema financiero.

e) Por su duración.

De acuerdo con el artículo 17 del Nuevo Código Penal para el Distrito Federal, atendiendo a su momento de consumación, puede ser:

I. *Instantáneo*: cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción legal;

II. *Permanente o continuo*: cuando se viola el mismo precepto legal, y la consumación se prolonga en el tiempo; y

III. *Continuado*: cuando con unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo, se concretan los elementos de un mismo tipo penal.

"El delito de llama *instantáneo* cuando la acción se extingue en un solo momento, es decir, cuando coincide con la consumación."[108]

"El instantáneo se perfecciona en un sólo momento, este delito puede realizarse mediante una acción compuesta de varios actos o movimientos, existe

[108] Maggiore, Giuseppe, ***Op. cit.***, Pág. 295.

una acción y una lesión jurídica, por ejemplo el homicidio que se actualiza con el momento de la muerte o el robo."[109]

El tipo penal contemplado en el artículo 231 fracción XIV, es un delito instantáneo, porque su consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción legal, que son el acceder ilícitamente a los sistemas o programas informáticos del sistema financiero.

f) Por el elemento interno o culpabilidad.

Los delitos se clasifican en *dolosos* y *culposos.* El artículo 18 del Nuevo Código Penal para el Distrito Federal, establece que las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente.

Obra dolosamente el que, conociendo los elementos objetivos del hecho típico de que se trate, o previniendo como posible el resultado típico, quiere o acepta su realización.

Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación de un deber de cuidado que objetivamente era necesario observar.

Castellanos Tena establece, que el delito es doloso "cuando se dirige a la voluntad consciente a la realización del hecho típico y antijurídico, como el robo, en donde el sujeto decide apoderarse y se apodera, sin derecho del bien mueble ajeno."[110]

Por lo que respecta a los delitos culposos, estos se presentan cuando el delito se comete sin la intención de realizarlo, ocurre debido a negligencia, falta de cuidado, imprevisión, imprudencia, produciendo un resultado típico por violar un deber de cuidado.

---

[109] Castellanos Tena, Fernando, ***Op. cit.***, Pág. 138.
[110] ***Ibidem***, Pág.141.

El delito contemplado en artículo 231 fracción XIV, es un delito eminentemente *doloso*, porque el sujeto activo debe tener la voluntad conciente de cometer el hecho delictivo, realiza la conducta típica con pleno conocimiento y voluntad al efectuar el acceso ilícito un sistema informático.

g) Por su estructura.

En función su estructura, los delitos se clasifican en *simples* y *complejos*.

Son *simples* aquellos en los cuales la lesión jurídica es única, Ignacio Villalobos establece que son simples "aquellos delitos que se producen por un solo sujeto, con un solo acto, como la lesión que se causa por un disparo de arma de fuego, con una sola forma de culpabilidad."[111]

Los delitos *complejos* son aquellos, en los cuales la figura jurídica consta de la unificación de dos infracciones, cuya fusión da nacimiento a una figura delictiva nueva, superior en gravedad a las que la componen, es decir, consta más de una afectación y da lugar a un delito diferente y de mayor alcance en la punibilidad, como en el caso del robo y homicidio calificado.

En el caso del tipo penal que nos ocupa, se trata de un delito *simple*, porque sólo se viola un interés jurídicamente protegido que es el patrimonio y porque se da en un solo acto y por un sujeto.

h) Por el número de actos.

Por el número de actos integrantes de la acción típica, los delitos se denominan unisubsistentes y plurisubsistente.

[111] Villalobos, Ignacio, ***Derecho Penal Mexicano***, *Parte General*, 5ª Edición, Porrúa, México, 1990 Pág. 249.

Los *unisubsistentes*, se forman por un solo acto. Los *plurisubsistentes*, son cuando se integran por la concurrencia de varios actos, bajo una sola figura. El delito se da a veces mediante diversos actos y en otros mediante uno sólo, como ocurre con el homicidio.

El artículo 231 fracción XIV, es un delito *plurisubsistente*, en virtud de que el tipo penal se tendrá por consumado con los diversos actos del sujeto, ya que accesa ilícitamente al sistema informático y realiza indebidamente operaciones, transferencias, o movimientos de dinero o valores, que en su conjunto forman una sola acción.

i) Por el número de sujetos.

Esta clasificación atiende a la unidad o pluralidad de sujetos que intervienen para ejecutar el hecho descrito en el tipo y pueden ser *unisubjetivos o plurisubjetivos*.

En los primeros, el tipo penal requiere de la existencia de un solo sujeto, en cambio, los segundos contemplan la existencia de varios sujetos para configurar el hecho punible, tenemos por ejemplo, la asociación delictuosa, la violación tumultuaria, la pandilla, etc., en el caso de los unisubjetivos, como ejemplo podemos citar el delito de peculado, "porque la conducta típica observa su comisión por un solo sujeto activo, tal es el caso del robo perpetrado por una sola persona."[112]

Los delitos plurisubjetivos para su concurrencia, el tipo penal requiere de la integración de dos o más sujetos en la comisión del ilícito.

El delito que se analiza, es un delito *unisubjetivo*, es suficiente la participación de un sólo sujeto para satisfacer el tipo penal y de esta forma realizar el acceso ilícito a los sistemas o programas de informática del sistema

[112] Malo Camacho, Gustavo ***Op. cit.***, Pág.316.

financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores.

j) Por la forma de persecución.

Estos delitos pueden ser de *querella* (requiere queja de la víctima o del ofendido) o de *oficio*, en los que la autoridad está obligada a actuar con independencia de los ofendidos.

"Los delitos perseguibles previa denuncia (conocidos como perseguibles de oficio), pueden ser formulados por cualquier persona, y son aquellos en los que la autoridad está obligada a actuar, por mandato legal, persiguiendo y castigando a los responsables, con independencia de la voluntad de los ofendidos."[113]

En los delitos perseguibles de oficio cualquier persona que tenga conocimiento de un delito puede denunciar el ilícito o poner a disposición de las autoridades competentes al presunto responsable, "bastará que dicho funcionario esté informado por cualquier medio, para que de inmediata, quede obligado a practicar las investigaciones necesarias que le permiten concluir, en su momento si la conducta o hecho de que tiene conocimiento, constituye una infracción penal."[114]

Los delitos de querella, sólo se persiguen a petición de parte, o sea, por medio de querella del sujeto pasivo o de sus legítimos representantes, como en el caso del fraude, abuso de confianza.

De acuerdo con el artículo 246 de nuestro Código Penal, el delito previsto en el artículo 231 fracción XIV, se perseguirá de *querella*, sin embargo, consideramos que por tratarse del sistema financiero, debiera perseguirse de oficio.

---

[113] ***Ibidem***, Pág. 144.
[114] Colín Sánchez, Guillermo, ***Derecho Mexicano de Procedimientos Penales***, 18ª Edición, Porrúa, México, 2001, Pág. 316.

k) Por la materia.

Pueden ser comunes, *federales, oficiales, militares y políticos*, para dilucidar sobre la materia, debemos atender al ordenamiento de donde emana el tipo delictivo y de la autoridad determinada para sancionarlo.

Los delitos *comunes* constituyen la regla general, son aquellos que se formulan en leyes dictadas por legislaturas locales de cada entidad federativa, los *federales* son los formulados por el Congreso de la Unión, los *oficiales* son los que comete un empleado o funcionario público en el ejercicio de sus funciones, los delitos *militares* afectan la disciplina del Ejército, los *políticos*, no han sido definidos de manera satisfactoria. Generalmente se incluyen todos los hechos que lesiona la organización del Estado en sí misma o en sus órganos o representantes.

Por lo que respecta al delito previsto en el artículo 231 fracción XIV, es un delito del fuero *común*, toda vez que está previsto en el Nuevo Código Penal del Distrito Federal, lo que consideramos otro error legislativo, ya que por tratarse del sistema financiero, debe ubicarse en el Código Penal Federal.

l) Por su clasificación legal.

El Libro Segundo del Nuevo Código Penal para el Distrito Federal, reparte los delitos en veintisiete Títulos a saber: Delitos contra la vida y la integridad corporal, Procreación asistida, inseminación artificial y manipulación genética, Delitos de peligro para la vida o la salud de las personas, Delitos contra la libertad personal, Delitos contra la libertad y la seguridad sexuales y el normal desarrollo psicosexual, Delitos contra la moral pública, Delitos contra la seguridad de la subsistencia familiar, Delitos contra la integridad familiar, Delitos contra la filiación y la institución del matrimonio, Delitos contra la dignidad de las personas, Delitos contra las normas de inhumación y exhumación y contra el respeto a los cadáveres o restos humanos, Delitos contra la paz, la seguridad de las personas y la inviolabilidad del domicilio, Delitos contra la intimidad personal y la

inviolabilidad del secreto, Delitos contra el honor, Delitos contra el patrimonio, Operaciones con recursos de procedencia ilícita, Delitos contra la seguridad colectiva, Delitos contra el servicio público cometidos por servidores públicos, Delitos contra el servicio público cometido por particulares, Delitos en contra del adecuado desarrollo de la justicia cometidos por servidores públicos, Delitos cometido (sic) por particulares ante el ministerio público, autoridad judicial o administrativa, Delitos cometidos en el ejercicio de la profesión, Delitos contra la seguridad y el normal funcionamiento de las vías de comunicación y de los medios de transporte, Delitos contra la fe pública, Delitos contra el ambiente y la gestión ambiental, Delitos contra la democracia electoral, Delitos contra la seguridad de las instituciones del Distrito Federal.

El delito contemplado en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, se encuentra ubicado en el Libro Segundo, Titulo Décimo Quinto de los Delitos contra el Patrimonio, inmediatamente después del delito de fraude.

4.3. Elementos del delito.

Algunos autores al entrar al estudio de los elementos del delito, se refieren también a los presupuestos del delito. Para el penalista Celestino Porte Petit, “son aquellos antecedentes jurídicos, previos a la realización de la conducta o del hecho descritos en el tipo y de cuya existencia depende el título de delito respectivo.”[115]

Sin embargo, es a Sauer a quien debemos la clasificación de los aspectos positivos y negativos del delito. Los elementos positivos son aquellos aspectos posibles de integrar a la figura delictiva, cada elemento corresponde un aspecto negativo que impide dicha integración. Al delito se le contrapone lo que no es.

Estos caracteres o aspectos, nos permiten sólo para efectos expositivos, ubicar los elementos que conforman de manera básica al delito y a su vez,

[115] Celestino Porte Petit, citado por Pavón Vasconcelos Francisco, ***Op. cit.***, Pág. 193.

establecer el concepto del mismo, como una conducta típica, antijurídica, culpable y punible.

Siguiendo las teorías clásicas y neoclásicas encontramos los siguientes, que a continuación analizaremos.

Aspectos positivos	**Aspectos negativos**
a) Conducta	Ausencia de conducta
b) Tipicidad	Atipicidad
c) Antijuridicidad	Causas de justificación
d) Imputabilidad	Causas de inimputabilidad
e) Culpabilidad	Causas de inculpabilidad
f) Condicionalidad objetiva	Falta de condición objetiva
e) Punibilidad	Excusas absolutorias

4.3.1. Conducta.

"La conducta es el comportamiento humano voluntario, positivo o negativo encaminado a un propósito. Sólo la conducta humana tiene relevancia para el Derecho Penal, el acto y la omisión deben corresponder al hombre, porque únicamente es posible el sujeto activo de las infracciones penales, es el único ser capaz de voluntariedad."[116]

Carranca y Trujillo señala que: "la conducta es, así, el elemento básico del delito. Consiste en un hecho material, exterior, positivo o negativo, producido por el hombre."[117]

Como se puede apreciar de los conceptos que acabamos de transcribir, la conducta se constituye como el elemento básico del delito, en función de que es el

[116] Castellanos Tena, Fernando, ***Op. cit.***, Pág. 149.
[117] Carranca y Trujillo, Raúl, ***Derecho Penal Mexicano***, *Parte General*, 21ª edición, Porrúa, México, 1988, Pág.275.

primer elemento de éste, tanto en su aspecto positivo o negativo, misma que se puede manifestar mediante una acción u omisión.

Para expresar este elemento del delito, se han usado diversas denominaciones en la doctrina tales como: conducta, acto, acontecimiento, acción o hecho, para los efectos de la presente investigación llamaremos a este primer elemento del delito: conducta o acción.

En el tipo penal previsto en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, la conducta consiste en accesar, entrar o introducirse a los sistemas o programas de informática del sistema financiero e indebidamente se realicen operaciones, transferencias o movimientos de dinero, lo que consideramos otro error, pues el legislador hace uso de sinónimos cuando se refiere a la conducta que realiza el sujeto activo, “accese, entre o se introduzca” son sinónimos de la palabra introducir.

Es importante volver a señalar, que aún cuando en nuestro Código Penal no establece que se trate de una conducta equiparada al fraude, se entiende que estamos en presencia de este tipo de conducta, al ubicarla erróneamente el legislador inmediatamente después del delito de fraude. El acceso ilícito a un sistema informático, no es de ninguna manera sinónimo de engaño ni de error, (elementos requeridos en el tipo básico de fraude), pues al efecto, las máquinas por su propia naturaleza no son susceptibles de caer en errores o falsas concepciones de la realidad, como sucede con las personas físicas.

Maggiore establece lo siguiente: “para engañar a alguien se requiere, la posibilidad de caer o no en ese engaño, tener la capacidad para reconocer el error, lo que de ninguna manera acontece con los sistemas computacionales, hasta el día de hoy; de tal modo que se hace imposible que los elementos de esa índole que conforman la estructura del fraude: error, falsa representación, engaño,

motivación, voluntad, decisión, disposición, puedan actualizarse en un sistema carente de las condiciones psicológicas correspondientes."[118]

El acceso ilícito a un sistema informático, con el fin de realizar operaciones, transferencias o movimientos de dinero o valores, no puede considerase como una especie de fraude, sino de robo, un robo por medio electrónico o informático en el que se utiliza a la computadora como herramienta o medio comisivo, para llevar a cabo esa conducta ilícita que es precisamente el acceso indebido a los sistemas o programas de cómputo del sistema financiero, para realizar operaciones, transferencias o movimientos de dinero o valores (acto de disposición).

Es así, que la propuesta del presente trabajo se enfoca a ubicar correctamente el artículo en comento, pues estamos en presencia de un delito de robo por medio electrónico o informático, en el que como ya dijimos, la computadora es el medio o instrumento para la comisión de la conducta ilícita, antes descrita.

A una computadora no se le puede engañar, ésta funciona bajo instrucciones o comandos que le son dadas por una persona, las cuales se materializan bajo un programa, por lo tanto una computadora depende en su totalidad de las instrucciones que le son dadas, mismas que no pueden ser erróneas o falsas, pues para accesar a ella, sólo deben introducirse datos que son válidos para el sistema, por tal motivo resulta equívoco pensar que para tener acceso a una computadora, se haga por medio del engaño.

Y son precisamente los *hacker*, los que se introducen a los sistemas informáticos ajenos, sin autorización y de forma secreta, para la obtención de nombres de usuario y claves de acceso (*login* y *password*),[119]empleando programas que por medio de la fuerza prueban miles de posibles passwords hasta

[118] Maggiore, Giuseppe, ***Op. cit.***, Pág.125.
[119] ***Password o login***: Es la palabra de paso, contraseña, que se define como un conjunto de caracteres alfanuméricos, para verificar la autenticidad de la autorización expedida a un usuario a quien le permiten el acceso a la información de un sistema.

encontrar alguna válida, o el acceso a través de agujeros en la seguridad de la computadora. De esta forma no sólo se logra entrar en el sistema sino que se obtiene un control total sobre dicho sistema informático, que es lo realmente peligroso.

El artículo 230 del Nuevo Código Penal para el Distrito Federal, establece que comete delito de fraude, el que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero.

La problemática que se presenta en el delito previsto en el artículo 231 fracción XIV, es que lo han ubicado inmediatamente después del tipo penal de fraude, por lo que nos surge una pregunta: ¿A quién se realiza el engaño?. Al respecto, numerosos autores norteamericanos, sostienen que el engaño se realiza a la máquina pues consideran que la introducción de datos falsos en una computadora equivale al engaño sobre un humano, otros establecen que el engaño sólo se da de hombre a hombre.

Sin embargo es erróneo pensar en engañar a una máquina o computadora, en virtud de que el engaño según la Real Academia de la Lengua Española significa:

"Del Lat. vulg. *in-gannare*, burlar, hacer creer lo que no es verdad, equivocarse, incurrir en error involuntario."[120]

Por lo que consideramos, que quien sufre el engaño es necesariamente una persona, pues sólo ésta puede apreciar que los hechos sean verdaderos o no, puede discernir entre lo que es cierto y lo que es falso, en el caso que se analiza, la computadora, es sólo el instrumento por medio del cual se lleva a cabo la conducta ilícita, por lo tanto no puede engañársele a una máquina.

[120] Diccionario de la Lengua Española, Real Academia Española, ***Op. cit.***, Pág. 417.

Palazzi señala: “la informática plantea dos problemas fundamentales al delito de robo. El primero lo hallamos en el objeto del robo y el segundo es el referente a la acción típica del desapoderamiento y los medios comisivos que dicha acción permite. En cuanto al objeto del robo se ha discutido arduamente, sobre la posibilidad de apoderamiento de bienes tales como la electricidad, los pulsos telefónicos o las señales de video y más recientemente sobre los registros de un sistema computarizado que representen un depósito bancario o un determinado valor económico. Sosteniendo que el valor económico de los bienes permitía incluirlos dentro del concepto de “cosa” y por ende su apoderamiento es susceptible de reproche en materia penal.”[121]

Contrario a lo establecido por Palazzi, se ha establecido que no pueden incluirse dentro del concepto de cosa los registros informáticos representativos de un valor, como los registros bancarios electrónicos, ya que la alteración de estos datos con el fin de apropiarse de un valor patrimonial caen dentro del tipo de fraude, incluyéndose dentro de esta figura, los casos en que mediante el acceso a una computadora el sujeto se apropia o copia algún dato.

Cuestión con la que estamos en total desacuerdo, pues al introducirse de manera ilícita a los sistemas o programas de informática y en nuestro caso al sistema financiero mexicano para realizar operaciones, transferencias o movimientos de dinero o valores, estamos hablando de que el sujeto realiza un apoderamiento sin consentimiento de quien legalmente pueda otorgarlo, por lo tanto se da el delito de robo por un medio electrónico y no por fraude como equívocamente lo han ubicado nuestros legisladores, en el Nuevo Código Penal para el Distrito Federal, siendo este, otro problema que presenta el artículo que hoy se analiza, ya que como lo hemos mencionado antes, la Asamblea Legislativa es incompetente para crear leyes que se refieran al sistema financiero mexicano, por lo tanto, el legislador tuvo que haberlo ubicado dentro del Código Penal Federal.

[121] Palazzi Pablo Andrés, ***Op. cit.***, Pág. 87.

La otra cuestión que surge, es el desapoderamiento por medio electrónico, al respecto Palazzi escribe: “surge a simple vista la duda respecto de las nuevas formas dinerarias inmateriales tales como el dinero electrónico, las transferencias bancarias automatizadas o las disposiciones registrables por computadoras, el auge de transacciones electrónicas aseguran que cada vez serán más los casos relacionados con este tipo de delitos. La idea de desapoderamiento, requiere en primer lugar, el desapoderamiento de quien ejercía la tenencia de la cosa, lo cual implica quitarla de la llamada esfera de custodia, que no es otra cosa que la esfera dentro de la que el tenedor puede disponer de ella, hay desapoderamiento cuando la acción del agente, al quitar la cosa de aquella esfera de custodia, impide que el tenedor ejerza sobre la misma sus poderes de disposición.

Sin embargo, este desapoderamiento por medio electrónico, no basta pues es necesario el apoderamiento material de la cosa por parte del agente, el desapoderamiento no implica por sí mismo el apoderamiento, este último se caracteriza por la posibilidad de que el agente pueda realizar sobre la cosa actos materiales de disposición y que haya tenido su origen en la propia acción, por haber carecido antes de ella.”[122]

Los tribunales argentinos han dicho que el apoderamiento necesita desde el punto de vista objetivo el acto material de obtención de la cosa, que para configurar el tipo penal de robo, basta con que el sujeto activo se apodere de la cosa sin estar legitimado, quitándola a quien la posea independientemente del título por el cual éste la tuviere, que sólo se exige el apoderamiento de la cosa como acto material de obtenerla, que para apoderarse del objeto deseado es forzoso llegar hasta donde se encuentre ese objeto, y que para configurar el apoderamiento es necesario que la cosa esté bajo el poder de hecho de alguna persona, se ha dicho también que el término “apoderase”, significa tener la cosa en poder con libre disponibilidad y no se limita al momento de aprehenderla sino que comprende su consumación, al sacarla de la esfera de custodia del dueño, que para que existe desapoderamiento, basta el desplazamiento de la cosa de la

[122] ***Ibidem***, Pág. 89.

persona del propietario a la del ladrón para que sea posible afirmar que en determinado momento el dueño de la cosa no habría podido hacer actos materiales de disposición.

"El fraude puede describirse de forma general, como el hecho por medio del cual una persona toma, a raíz de un error provocado por la acción de otra persona, una disposición patrimonial perjudicial, que pretende convertir en beneficio propio o de un tercero. La secuencia causal en el fraude, es la siguiente: la persona despliega una actividad engañosa que induce en error a una persona, quien en virtud de ese error, realiza un acción que resulta perjudicial para un patrimonio, la conducta punible es, pues, la de defraudar por medio del engaño. El aprovechamiento de las máquinas automatizadas usadas como medios de expendio de bienes y servicios planteó otros problemas. La tradicional ecuación del delito de fraude (engaño-error-disposición patrimonial) a la que aludimos no era aplicable a estos sistemas desde que el concepto jurídico de error sólo podía referirse a la mente humana. Es ésta la que es engañada en la defraudación."[123]

Ello llevó a una opinión generalizada respecto de la exclusión del delito de fraude cuando cualquier máquina o computadora fuera usada como medio para la comisión del delito. El modo de operar del fraude es el de la inducción en error de su víctima, ya que un fraude que no opere a través del error, no puede tener por efecto un acto de propiedad patrimonialmente perjudicial.

Determinar si es posible aplicar el fraude a las máquinas o sistemas automatizados implica demostrar la aplicación del error, pues para que se configure el delito de fraude es necesaria la voluntad viciada de la víctima, originada por el engaño del autor, la falta de voluntad expresa o tácita, es decir cuando el apoderamiento se ha efectuado contra la voluntad de la víctima dará lugar al delito de robo.

[123] ***Cfr.*** Palazzi, ***Op. cit.***, Pág. 89.

Palazzi establece una serie de elementos que tienen que tomarse en cuenta para determinar si existe delito de fraude en las manipulaciones a los sistemas informáticos.

- “Presencia de un engaño previo al despojo patrimonial. El engaño es producido por el sujeto activo y aquí es la máquina la engañada, no la que comote el fraude.

- El sujeto activo debe desplegar una maquinación que induce al error a la víctima. El error consiste en un falso juicio que realiza la persona sobre la realidad. Corresponderá entonces en lo que sigue determinar si puede equipararse el sistema lógico de una computadora al de la mente humana que aparece errada en el fraude.

- Esa inducción al error hace que ésta preste voluntariamente una contraprestación en virtud del engaño sufrido. Es decir que hay una disposición patrimonial o una entrega de la cosa, corresponderá analizar si esa disposición patrimonial puede ser realizada por una computadora, en este caso la respuesta es afirmativa.

- El engaño debe provocar el error y, éste a su vez, determinar la prestación, esto es, el perjuicio material efectivo, es decir, que debe haber una relación de casualidad entre todos los elementos.”[124]

Como es posible apreciar, el problema radica en averiguar si puede equipararse el sistema lógico de una computadora al de la mente humana, errada en el fraude.

Ahora bien, si la persona jurídica es en definitiva la perjudicada patrimonialmente, debemos ver si la máquina, que reemplaza al hombre, puede incurrir en error, para ello debemos definir el concepto “error”, de acuerdo con la

[124] ***Ibidem***, Pág. 101.

Real Academia de la Lengua Española, el error "*es inducir a otro a tener por cierto lo que no lo es, valiéndose de palabras o de obras aparentes y fingidas.*"[125]

Davara Rodríguez, establece que "el acceso de una persona no autorizada a los datos que se encuentran en soportes informáticos se está produciendo cada vez más, motivado por la falta de seguridad de los sistemas y de formación de las personas que en ellos operan, facilitando más, si cabe, por las posibilidades que ofrecen las modernas técnicas de comunicación que permiten el conocimiento manejo y transferencia de información entre sistemas, con máxime garantías y mínimo de riesgo, el problema se origina en lo que se denomina las tres P: patrimonio, propiedad y privacidad, tres aspectos que deben establecerse indiscutida y formalmente a los datos y sistemas informáticos, comenzando por extender el concepto de patrimonio, incluyendo específica y exhaustivamente a los datos y la disponibilidad de los mismos, demarcando la existencia de una propiedad lícita de esta entidad "datos" y estableciendo sin lugar a dudas que se confiere el mismo grado crucial de privacidad que a cualquier otra propiedad como una carta, o archivos particulares."[126]

Las computadoras o los sistemas informáticos no actúan por su cuenta, sino que siguen las órdenes con las que fueron programadas, por lo tanto resulta equívoco pensar que puede engañársele o aprovecharse del error de una computadora, para introducirse a un sistema o programa informático del sistema financiero, para realizar indebidamente operaciones, transferencias o movimientos de dinero o valores, como lo han establecido nuestros legisladores en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal.

El avance de las ciencias informáticas, ha creado una red de computadoras donde individuos y empresas publican información, venden productos y servicios y realizan un sinnúmero de actividades, pero debido al libre

[125] Diccionario de la Lengua Española, Real Academia Española, ***Op. cit.***, Pág. 417.
[126] Davara Rodríguez, Miguel Ángel, ***Op. cit.***, Pág. 324.

acceso y la apertura de la red puede conducir a situaciones donde se intente delinquir.

Como respuesta al incremento de casos de *hacking*, se fueron reformando las normas penales para incluir a ese acceso no autorizado a sistemas informáticos como un delito autónomo, como ocurrió en Estados Unidos, España, no cabe duda que existe la necesidad de tipificar penalmente y de manera adecuada el acceso ilegítimo a sistemas informáticos.

De lo antes señalado y de acuerdo a la definición de delito de fraude, nos queda claro que el supuesto que marca la fracción XIV del artículo 231, es un delito de robo que se da por un medio electrónico, siendo su conducta típica el acceso ilícito a los sistemas o programas informáticos del sistema financiero para realizar operaciones, transferencias o movimientos de dinero o valores, por lo tanto nuestra propuesta es el de ubicarlo en el capítulo correspondiente a robo, que se encuentra en el mismo Título Décimo Quinto de los Delitos contra el Patrimonio. En ese tenor encontramos la siguiente referencia:

Novena Época
Instancia: TERCER TRIBUNAL COLEGIADO DEL CUARTO CIRCUITO.
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: VII, Enero de 1998
Tesis: IV.3o.18 P
Página: 1167

ROBO. TRANSFERENCIA DE FONDOS MEDIANTE SISTEMA DE CÓMPUTO. *La sola transferencia de fondos que se haga mediante el sistema de cómputo, sin el consentimiento de la persona autorizada, es suficiente para considerar que se surte el delito de robo, toda vez que tal transferencia a favor de persona distinta a la institución bancaria afectada, trae como consecuencia que nazca a cargo de esta última la obligación de responder económicamente por dicha operación, lo que implica que el numerario transferido ha salido del patrimonio del afectado y ha pasado a formar parte del patrimonio de una persona distinta, sin que el primero pueda recuperarlo por su sola voluntad, ya que esto constituiría una actitud ilícita.*

TERCER TRIBUNAL COLEGIADO DEL CUARTO CIRCUITO.
Amparo en revisión 80/97. María Ivonne Medrano González y otros. 27 de mayo de 1997. Unanimidad de votos. Ponente: Enrique Cerdán Lira. Secretario: Raúl Alvarado Estrada.

De lo anterior, observamos que el delito que contempla el artículo 231 fracción XIV del Nuevo Penal para el Distrito Federal, es un delito de **robo**, como lo ha sostenido la Suprema Corte de Justicia de la Nación, por el hecho de que una persona realice una transferencia de fondos mediante el sistema de cómputo, sin el consentimiento de la persona autorizada, es suficiente para considerar que se surte el delito de robo, pues dicha operación, implica que el numerario transferido ha salido del patrimonio del afectado y ha pasado a formar parte del patrimonio de una persona distinta, sin que el primero pueda recuperarlo por su sola voluntad, y eso constituye una actitud ilícita.

Lo cierto es que los sistemas informáticos están reemplazando al hombre y lo suplantan en ese control de seguridad que antes realizaban los humanos. Las intromisiones informáticas son cada vez más frecuentes, siendo esto una violación a la privacidad.

Nava Garcés señala: "las conductas perseguibles o bien susceptibles de reproche social en el ámbito de la computación son muy variadas, van desde el simple robo de información, hasta el daño patrimonial más severo en los sistemas de cómputo y financieros de una entidad, pero algo tienen en común: la expresión de dicha conducta por medio de un sistema electrónico empleado con esos fines."[127]

4.3.2. Ausencia de Conducta.

Consiste en el aspecto negativo de la conducta y se presenta cuando para la realización de un delito esta se encuentra ausente, ya que es necesaria la presencia de una acción humana en sus formas de acción u omisión y en caso de faltar, no se configurará el delito por ser la conducta la base del delito, por lo que

[127] Nava Garcés, ***Op. cit.***, Pág. 175.

cabe hacer mención del principio de *nullum crimen sine actione* (no hay delito sin acción).

"Es pues, la ausencia de conducta uno de los aspectos negativos o mejor dicho impeditivos de la formación de la figura delictiva, por ser la actuación humana, positiva o negativa, la base indispensable del delito como de todo problema jurídico."[128]

Algunos autores consideran como causas de ausencia de conducta, por parte del sujeto activo, a la vis absoluta o fuerza física, exterior o irresistible, a la vis mayor o fuerza mayor, los cuales tienen diferencias que radican en razón de si procedencia, ya que la primera deriva de una fuerza material proveniente del hombre, lleva a cabo un hacer o movimiento corporal o en su caso, permanece inactivo también involuntariamente, esto es, que una persona aplique a otra una fuerza física y con ello se produzca un resultado prohibido por la ley, sin embargo, esta fuerza física debe ser irresistible, ya que si para el sujeto es posible oponerse o responder a esa fuerza, ésta será entonces resistible.

La fuerza mayor o vis mayor, es una fuerza material o física que proviene de la naturaleza o de los animales.

En ambas el sujeto realiza una actividad o inactividad que no quería ejecutar, se da la ausencia de conducta por parte del sujeto activo, ya que no existe voluntad de querer realizar el movimiento corporal.

Los actos reflejos son movimientos corporales involuntarios, si el sujeto puede controlarlos o por lo menos retardarlos, ya no funcionan como factores negativos del delito. Es decir son aquellos movimientos musculares, que son reacciones inmediatas e involuntarias a un estímulo externo o interno, sin intervención de la conciencia.

[128] Castellanos Tena, ***Op. cit.***, Pág. 163.

Algunos autores han señalado que también son causas de ausencia de conducta los movimientos fisiológicos, que son consecuencia de las reacciones naturales del cuerpo como el sueño y sonambulismo, la sugestión, la hipnosis y la narcosis, la inconsciencia y los actos reflejos, y la fuerza irresistible, como ya lo hemos visto.

En el caso del sueño, el sujeto se encuentra en un estado de reposo tanto físico como mental, por lo cual no tiene dominio de sus movimientos, no existe la voluntad del sujeto por encontrarse en ese estado y cualquier movimiento involuntario que realice será son la manifestación de su voluntad consciente y a falta de esta no se configurará el delito.

En el sonambulismo, el sujeto también carece de voluntad por realizar los movimientos corporales involuntarios debido al estado de inconciencia en las que se encuentra el sujeto, no es así en el hipnotismo, que "se da cuando con una serie de manifestaciones del sistema nervioso producidas por una causa artificial,"[129]el hipnotismo se dará siempre y cuando se hipnotice sin su consentimiento y realice una conducta tipificada como delito, por lo que en tales fenómenos psíquicos el sujeto realiza la actividad o inactividad sin voluntad por hallarse en un estado en el cual su conciencia se encuentra suprimida.

En el caso del tipo penal que se analiza, no se presenta ninguna de las causas de ausencia de conducta, ya que es un delito evidentemente de acción, misma que se constituye por una serie de actos propios, pensados y razonados, el sujeto activo necesita realizar un movimiento corporal para llevar a cabo su comisión con el fin de llegar al resultado que se ha propuesto, que en este caso será un beneficio para sí o para un tercero.

Además, como lo hemos mencionado, este delito en específico, no se constituye por un solo acto, sino por una serie de éstos que en su conjunto conforman una acción, ya que debido a los diferentes métodos informáticos que se

[129] Pavón Vasconcelos, Francisco, ***Op. cit.***, Págs. 293-294.

utilizan para accesar a los sistemas o programas informáticos del sistema financiero se requiere de todo un proceso que es un conjunto de pasos para vulnerarlos.

4.3.3. Tipicidad.

La tipicidad es uno de los elementos esenciales del delito cuya ausencia impide su configuración, sin embargo es necesario señalar que no debe confundirse el tipo con la tipicidad, "el tipo es la creación legislativa, la creación que el estado hace de una conducta en los preceptos penales, y la tipicidad es la adecuación de una conducta concreta con la descripción legal formulada en abstracto, basta que el legislador suprima de la ley penal un tipo, para que el delito quede excluido."[130]

Al tipo se le ha denominado: figura típica, figura delictiva, tipo legal, conducta típica, por su parte Pavón Vasconcelos señala que tipo "es la descripción concreta hecha por una ley de una conducta a la que en ocasiones se suma un resultado, reputada como delictuosa al conectarse a ella una sanción penal."[131]

De acuerdo a lo anterior, entendemos por tipo, la descripción legal de un delito con la que se pretende proteger uno o varios bienes jurídicos relevantes tanto para la persona individual como para la sociedad y de cuya existencia depende la tipicidad.

Por otra parte la tipicidad "es el encuadramiento de una conducta con la descripción hecha en la ley, la coincidencia del comportamiento con el descrito por el legislador, es por lo tanto, la adecuación de un hecho a la hipótesis legislativa."[132]

"La tipicidad como elemento del delito, requiere de ser distinguida del tipo, con el que usualmente es confundida. El tipo penal es la expresión jurídica,

[130] Castellanos Tena, ***Op. cit.***, Pág. 167.
[131] Pavón Vasconcelos, Francisco, ***Op. cit.***, Pág. 294.
[132] Castellanos Tena, ***Op. cit.***, Pág.167.

mediante la cual el legislador expresa la conducta antisocial y la tipicidad el proceso mediante el cual podemos adecuar una conducta al tipo."[133]

Raúl Carrancá y Trujillo al abordar el tema de la tipicidad, nos explica:

"La acción antijurídica ha de ser típica para considerarse delictiva. A lo dicho sobre el particular sólo hemos de añadir que la acción ha de encajar dentro de la figura de delito creada por la norma penal positiva pues de lo contrario al faltar el signo externo distintivo de la antijuridicidad penal, que lo es la tipicidad penal, dicha acción no constituiría delito. Pero puede existir la tipicidad penal sin que exista acción antijurídica, como ocurre con las causas de justificación en las que hay tipicidad y también juridicidad, por lo que el delito no existe. Por esto puede decirse así mismo que la antijuridicidad es elemento constitutivo del delito pero no lo es del tipo.

La conducta humana es configurada hipotéticamente por el precepto legal. Tal hipótesis legal constituye el tipo. El tipo legal es la abstracción concreta que ha trazado el legislador, descartando los detalles innecesarios para la definición del hecho que se cataloga en la ley como delito (Jiménez de Asúa). Y la tipicidad es la adecuación de la conducta concreta al tipo legal concreto."[134]

Para el maestro español Mariano Jiménez Huerta, el tipo "es la descripción de conducta que a virtud del acto legislativo, queda plasmada en la ley como garantía de libertad y seguridad y como expresión técnica del alcance contenido de la conducta injusta del hombre que se declara punible."[135]

El tipo penal implica, el juicio previo mediante el cual el legislador ha valorado aquellas conductas antisociales que, a su parecer merecen una sanción, por tanto, en esta descripción se conjuga la valoración del bien jurídico tutelado, los fines.

---

[133] Nava Garcés, ***Op. cit.***, Pág. 177.
[134] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág. 422.
[135] Jiménez Huerta, Mariano, ***Derecho Penal Mexicano***, Tomo I, 6ª edición, Porrúa, México, 2000, Pág. 21.

Por lo que respecta a México, el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, dispone que en los juicios del orden criminal queda prohibido imponer por simple analogía y aún por mayoría de razón pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata.

Del análisis de esta disposición constitucional, se puede deducir que no se puede aplicar determinada sanción, por lo que es indispensable que exista el elemento de tipicidad, que es uno de los elementos esenciales del delito, en virtud de que no puede considerarse una conducta aún siendo ilícita como delito, en virtud de que no puede considerarse una conducta aún siendo ilícita como delito, sino esta tipificada en un ordenamiento penal como delito, con lo cual nos damos cuenta de que la conducta debe adecuarse exactamente a la conducta descrita en el tipo penal, ya que en caso contrario se estaría violando este precepto constitucional que nos indica que no se configura el delito sino hay tipicidad de la conducta o acción del sujeto activo,

Se dice que un acto es típico cuando se puede encuadrar una conducta perfectamente en cualquier tipo legal, la tipicidad se encuentra apoyada en el sistema jurídico mexicano por diversos principios supremos entre los que destacan el de *nullum poena sine lege* (no hay pena sin ley) y *nullum crime sine lege* (no hay delito sin ley), con lo que el sujeto activo debe encuadrada exactamente en una disposición expresa en la ley, descrita en un tipo penal, para que pueda ser sancionada esa conducta y de esta forma la tipicidad constituye una garantía de legalidad para el sujeto activo, en la inteligencia de que una conducta no puede ser delictiva, en tanto no esté comprendida en un tipo penal.

El tipo penal del delito objeto de la presente investigación, se encuentra previsto en el artículo 231 fracción XIV, pues es la creación que hace el estado de una conducta.

A continuación y para un mayor análisis del tipo es necesario referirnos a los elementos que lo constituyen, los cuales son objetivos, subjetivos y normativos.

4.3.3.1. Elementos Objetivos.

Son aquellos elementos susceptibles de ser apreciados por los sentidos y que describen la conducta que puede ser imputada a una persona, los que pueden ser esenciales y que no deben faltar en ningún tipo y los accidentales que pueden aparecer al lado de los esenciales y que también deber ser satisfechos en el tipo concreto en que aparezcan para poder considerar la tipicidad de la conducta."[136]

Los elementos objetivos son los siguientes:

1. Sujeto activo.
2. Sujeto pasivo.
3. Objeto material.
4. La conducta (acción u omisión).
5. Resultado material
6. Lesión o peligro del bien jurídico tutelado, que es el interés individual o colectivo protegido en el tipo.
7. Especiales medios o formas de realización, por ejemplo la violencia.
8. Modalidades o referencias de lugar, espacio o tiempo.

El **sujeto activo**, es la persona que lleva a cabo los elementos delimitados en cada tipo penal.

Carrancá y Trujillo, define al sujeto activo del delito de la siguiente manera: "es quien lo comete o participa en su ejecución. Sólo la persona humana es posible sujeto activo de la infracción, pues sólo ella puede actuar con voluntad y

[136] Malo Camacho, Gustavo ***Op. cit.***, Pág. 303.

ser imputable. La responsabilidad penal es personal. Nuestro Derecho Penal se sustenta sobre el principio universalmente consagrado que reconoce a la persona humana como único sujeto activo."[137]

Muñoz Conde señala:

"Sujeto activo.- El delito como obra humana siempre tiene un autor, aquél que precisamente realiza la acción prohibida u omite la acción esperada. Normalmente en el tipo se alude a dicho sujeto con expresiones impersonales como "el que" o "quien". En estos casos, sujeto activo del delito puede ser cualquiera (delitos comunes), al margen de que después pueda o no ser responsable del delito en cuestión dependiendo de que tenga o no las facultades psíquicas mínimas necesarias para la culpabilidad."[138]

El sujeto activo en el tipo penal que nos ocupa, se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común, con grandes conocimientos informáticos.

Palazzi señala que "para denominar a esta clase de sujetos activos se suele hablar de *hackers, phreackers* y toda clase de delincuentes cibernéticos, caracterizados por un saber informático especial. Es cierto que existe un grupo de personas dedicadas a *hackear* computadoras, que pueden llegar a ser clasificados como un grupo con tendencia a delinquir en este tipo de delitos por su personalidad y conocimientos técnicos, pero es un mito que el delincuente informático deba forzosamente poseer conocimientos profundos en la materia."[139]

La computación se halla tan extendida hoy en día, que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a una computadora, incluso desde su casa, puede realizar un delito informático, el caso más típico es el del cajero que desvía fondos mediante la computadora que usa para contabilizar el dinero que recibe o ingresa falsamente un monto en una

[137] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág. 264.
[138] Muñoz Conde Francisco, citado por Nava Garcés, ***Op. cit.***, Pág. 208.
[139] Palazzi, ***Op. cit.***, Pág. 68.

cuenta, o del empleado de seguridad que conoce los códigos de acceso al sistema y los utiliza en su provecho.

En esta facilidad de cometer delitos por medio de computadoras han tendido un papel muy importante la expansión del acceso a cualquier sistema informático debido a las redes informáticas.

Lo cierto es que desde el punto de vista de la experiencia, podemos a firmar que los autores del delito cometido por medios informáticos tienen un perfil que en la mayoría de los casos suele ser clasificado, a partir de la experiencia comparada e incluso la nacional, en los siguientes grupos:

Clase de delito.	**Sujetos**
Delitos patrimoniales contra bancos y entidades financieras	Empleados, en especial cajeros o personal del área de sistemas, ex empleados, terceros o cómplices.
Delitos de acceso ilegítimo o delito de daño menores.	Hackers, phreakers, usuarios descontentos
Daño o sabotaje informático.	Empleados de la empresa, o espías profesionales o industriales.
Violaciones a la privacidad, tratamiento ilícito de datos personales	Investigadores privados, empresas de marketing, agencias de informes crediticios y de solvencia patrimonial.
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos	Piratas informáticos o también usuarios, empresas que realizan competencia.

En definitiva dice Palazzi, “el delincuente informático no tiene necesariamente profundos conocimientos de computación, sino que es inducido a delinquir por la oportunidad que se le presenta frente al uso diario de las

computadoras y la impunidad que éste le brinda o por lo conocimientos que éste tiene frente al resto del personal."[140]

El **sujeto pasivo**, es el titular del bien jurídico protegido por la norma. El autor Muñoz Conde establece: "el sujeto pasivo es el titular del bien jurídico. No siempre coincide el titular del bien jurídico protegido en el tipo legal con el sujeto sobre el que recae la acción típica. Así, por ejemplo, en la estafa sujeto pasivo es el perjudicado patrimonialmente por el engaño, pero el engaño puede recaer sobre otra persona (un empleado, administrador, etc.)."[141]

Se ha señalado que los bancos figuran entre las víctimas de los delitos con computadoras por el uso creciente de transferencias de fondos en forma electrónica, lo que moviliza grandes cantidades de dinero, si bien la aparición del dinero electrónico ha creado nuevas modalidades de defraudación, también ofrece nuevas formas de protección como el encriptado de claves y *passwords.*

Además de las entidades financieras, el Estado es otra de las víctimas de esta novedosa criminalidad informática. Ello ha llevado a constituir agravantes cuando la lesión del bien jurídico sea propiedad del Estado.

En nuestra opinión, actualmente cualquiera que persona puede ser víctima de delito informático, sin embargo en el tipo penal que se analiza, el sujeto pasivo lo es el sistema financiero.

El **objeto material**, lo constituye la persona o cosa sobre quien recae el daño o peligro, la persona o cosa sobre la que se concreta la acción delictuosa, es decir, es el ente corpóreo hacia el que se dirige la actividad descrita en el tipo penal, este objeto, debemos distinguirlo del **objeto jurídico** que es el bien protegido por la ley y que el hecho o la omisión lesionan.

---

[140] ***Idem***.
[141] Muñoz Conde Francisco, citado por Nava Garcés, ***Op. cit.***, Pág. 208.

En el tipo penal contemplado en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, el objeto material son los recursos (dinero o valores) del sistema financiero, el objeto jurídico es el patrimonio, que es el bien jurídicamente protegido por la ley penal.

"En todo tipo hay una acción, entendida como comportamiento humano (acción u omisión), que constituye el núcleo del tipo, su elemento más importante. La acción viene descrita generalmente por un verbo (matare, causare una lesión, etc.), que puede indicar una acción positiva o una omisión. Cuando el tipo sólo exige la realización sin más de una acción, estamos ante los delitos de mera actividad (injuria, falso testimonio, etc.) o, en su caso, de mera inactividad (omisión pura). En otros casos exige, junto a la realización de la acción, la producción de un resultado material de lesión o puesta en peligro de un bien jurídico (delitos de resultado). Esta distinción puede llevar a confusiones, ya que todo delito consumado tiene un resultado constituido por la realización del tipo pero cuando aquí se habla de resultado se alude al resultado como modificación producida en el mundo exterior, separa espacial y temporalmente. Entre delitos de consecuencias dañosas y delitos de acciones dañosas, ya que solo en los primeros es necesario demostrar una causalidad entre la acción humana y el resultado, pero debe de tenerse en cuenta que a veces el resultado es sólo un peligro, lo que da lugar a la distinción entre delitos de lesión y delitos de peligro."[142]

Malo Camacho define a la acción a través de la conducta, señalando lo siguiente: "la conducta, por definición, es el elemento objetivo del delito, unida al resultado en los delitos de resultado material, en cuyo caso será necesario, también, que haya quedado previamente acreditada la causalidad entre ellos, para que los mismos puedan ser atribuibles, al tipo penal correspondiente."[143]

---

[142] ***Idem.***
[143] Malo Camacho, Gustavo ***Op. cit.***, Pág 341.

En el tipo penal, que se analiza, la conducta consiste en el acceso ilícito a los sistemas o programas de informática del sistema financiero para realizar indebidamente operaciones, transferencias o movimientos de dinero o valores.

El **resultado material**, es cuando hay una transformación de las cosas en el mundo fenomenológico, siendo aquellos en los cuales para su integración se requiere la destrucción o alteración de la estructura o del funcionamiento del objeto material.

En el artículo 231 fracción XIV, el resultado material se exterioriza con el apoderamiento indebido que se hace del dinero o valores del sistema financiero mediante el acceso ilícito a los sistemas o programas informáticos de éste, aún cuando los recursos no salgan de la institución financiera de la que se trate.

Medios o formas de realización, en numerosos casos, los tipos exigen determinados medios, para que pueda darse la tipicidad deben concurrir los medios que exija el tipo correspondiente.

En nuestro Código Penal, encontramos diversos tipos que requieren medios comisivos, los cuales constituyen los medios empleados (uno o varios) para alcanzar el resultado establecido en el tipo.

En el artículo 231 fracción XIV, es la computadora el medio o fin para realizar la conducta, que es el acceso ilícito a los sistemas o programas del sistema financiero, para realizar indebidamente operaciones.

Las **modalidades o referencias de lugar, espacio o tiempo**, en el caso que nos ocupa, no hace referencia a dichas circunstancias, sin embargo haremos alusión a ellas, toda vez que es una de las características que identifica a este tipo de delitos, por lo general en donde se realiza la acción u omisión se produce el resultado, en ciertos delitos la conducta y el resultado no coinciden en lo referente al tiempo o al lugar de la comisión del delito, como lo es el tipo penal que se analiza.

Por lo general, el acceso se efectúa normalmente desde un lugar exterior, sin embargo este tipo de delitos informáticos, se realizar en cualquier tiempo y en cualquier lugar.

4.3.3.2. Elementos subjetivos y normativos.

Los elementos subjetivos, son los aspectos subjetivos del tipo que se reconocen, son los ánimos, propósitos, que el propio legislador ha descrito en el tipo. Estos elementos hacen referencia al contenido de la voluntad, al conocimiento, motivación e interés exclusivo de determinada persona que rige su conducta y son los siguientes:

1. Dolo
2. Culpa

Los elementos normativos, "son las valoraciones de tipo jurídico inmersas en el tipo penal, por ejemplo: cuando el tipo contiene vocablos como "indebidamente" (porque requiere la valoración de si la acción fue realizada dentro de lo debido o no), "ilícitamente" (porque se debe hacer el examen sobre la licitud), "clandestinamente" (porque de su estudio depende que una acción pueda ser considerada como ilícito penal o no."[144]

Son aquellas expresiones que utiliza el legislador en la elaboración de los tipos penales y que deben ser valoradas para captar su sentido, entendidas.

Los elementos subjetivos del injusto reciben ese nombre, debido a la base subjetiva de los fines que tiene el sujeto para realizar la conducta reprochable, estos fines son distintos del dolo, en tanto que éste supone sólo la representación y aceptación de la conducta reprochada por la ley penal.

En resumen, la tipicidad se presentará, cuando la conducta se adecué al tipo previsto en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, que establece:

[144] Nava Garcés, ***Op. cit.***, Pág. 220.

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

4.3.4. Atipicidad.

La atipicidad se presenta cuando hay ausencia de la adecuación de la conducta de una persona al tipo, se exterioriza cuando falta alguno de los elementos del tipo penal como sería la falta de referencias temporales o espaciales que exige el tipo, la falta del bien jurídico tutelado, la falta de sujetos activos o pasivos, la falta de objeto material y no se realice la acción típica por lo medios comisivos señalados por la ley.

Es necesario, hacer una distinción entre ausencia de tipicidad y ausencia de tipo, "hay atipicidad, en cambio, cuando el comportamiento humano concreto, previsto legalmente en forma abstracta, no encuentre perfecta adecuación en el precepto por estar ausente alguno o algunos de los requisitos constitutivos del tipo. Atipicidad es, la ausencia de adecuación típica."[145]

Porte Petit establece, que "hay ausencia de tipo cuando una conducta o hecho no están descritos en una norma penal."[146]

Esta hipótesis, podemos apoyarla en el principio de *nullum, crime,nulla poena sine lege* (no hay delito, no hay pena sin ley), *nullum, crime sine tipo* (no hay delito sin tipo) o *nulla poena sine tipo* (no hay pena sin tipo), ya que sólo puede ser delito aquello previsto en un tipo penal de un ordenamiento penal.

Son causas específicas de atipicidad:

a) Ausencia de calidad o del número exigido por el tipo en cuanto a los sujetos activos o pasivos;

---

[145] Pavón Vasconcelos, ***Op. cit.***, Pág. 322.
[146] Porte Petit Candaudap, ***Op. cit.***, Pág. 365.

b) Ausencia del objeto material o del objeto jurídico, o bien existiendo éste no se satisfacen las exigencias de la ley por cuanto a sus atributos;

c) Cuando habiéndose dado la conducta, están ausentes las referencias temporales o espaciales exigidas por el tipo;

d) Cuando no se dan en la conducta los medios de comisión señalados por la ley, y

e) Cuando están ausentes los elementos subjetivos del injusto, requeridos expresamente por el tipo legal.

f) Por falta de los elementos normativos.

De acuerdo a lo establecido en la fracción II del artículo 29 del Nuevo Código Penal para el Distrito Federal, se señala que se excluye del delito cuando falte alguno de los elementos que integran la descripción legal del delito de que se trate, por lo tanto en cuanto al tipo penal que se analiza pueden presentarse las siguientes atipicidades:

1. Ausencia de la calidad en el sujeto pasivo.- Pues el sujeto se encuentra restringido o limitado, debido a que puede cometerse este tipo de conducta en otras personas morales ya sean privadas como son las empresas o las públicas como la Tesorería del Distrito Federal, toda vez que el tipo sólo hace alusión a los sistemas o programas informáticos del sistema financiero

2. Ausencia del objeto material.- En este caso, sería los datos informáticos respecto del dinero o valores que se manejen en las instituciones del sistema financiero.

3. Ausencia del objeto jurídico.- Es decir, la falta de patrimonio y si éste no existe, se estará ante una atipicidad.

4. Ausencia del propósito.- Que es la de obtener un beneficio para sí o para un tercero, ya que si el sujeto accesa a los sistemas o programas informáticos del sistema financiero, sin obtener ningún beneficio, no constituye un delito, siendo necesario realizar operaciones, transferencias o movimientos de dinero o valores indebidamente.

4.3.5. Antijuricidad.

Para Eugenio Cuello Calón, la antijuridicidad "presupone un juicio sobre la oposición entre el hecho realizado y la norma jurídica; juicio eminente objetivo, pues recae exclusivamente en la acción ejecutada."[147]

Es el juicio de valoración que recae sobre una conducta o hecho típico que destruye o pone en peligro el bien jurídicamente protegido, es decir, radica en la violación del valor o bien protegido a que se contrae el tipo penal respectivo, en los tipos penales se señalan los valores que es necesario amparar, una conducta es antijurídica cuando vulnera dichos bienes o valores.

Generalmente se acepta como antijurídico lo contrario al derecho, de tal manera que para que una conducta sea considerada como delictiva, debe estar en oposición a una norma penal que prohíba o pueda ordenar su ejecución, la antijuricidad presupone un juicio, una estimación respecto de la oposición existente entre la conducta humana y la norma penal, siendo esta una contradicción entre la conducta del hombre y las normas del derecho, incluyendo por supuesto las penales.

Por lo que se considera a una conducta antijurídica, cuando ésta no se encuentra amparada por alguna causa de justificación, es una conducta que va en contra de lo establecido en la norma jurídica.

El tipo penal en comento, prevé una conducta antijurídica, porque es una conducta que va en contra de lo establecido en la norma jurídica.

4.3.6. Causas de Justificación.

Para Jiménez de Asúa, son causas de justificación "las que excluyen la antijuridicidad de una conducta que puede subsumirse en un tipo penal, esto es aquellos actos u omisiones que revisten aspecto de delito, figura delictiva, pero en

[147] Cuello Calón, Eugenio, ***Derecho Penal***, Tomo I, 18ª Edición, Editorial Bosch, Casa Editorial, S.A. Barcelona, Pág. 284.

los que falta, sin embargo, el carácter de ser antijurídicos, de contrarios al derecho, que es el elemento más importante del crimen."[148]

Castellanos Tena, establece que las causas de justificación "son aquellas condiciones que tienen el poder de excluir la antijuricidad de una conducta típica, representan un aspecto negativo del delito, en presencia de alguna de ellas falta uno de los elementos esenciales del delito a saber: la antijuricidad."[149]

Las causas de justificación, denominadas igualmente causas de licitud, justificantes, causas eliminatorias de la antijuricidad o causas de exclusión, se caracterizan por constituir el elemento negativo de la antijuricidad, ya que excluyen a la misma, el sujeto que actúe conforme a derecho, no se le podrá exigir responsabilidad alguna, por el hecho de que existe una norma que le autoriza o le impone una conducta determinada, pero cuando una persona rebasa los lineamientos de una conducta legitimada por una justificante, se da la ilicitud, ya que mientras la causa de justificación excluye la antijuricidad del comportamiento, el exceso queda situado dentro del ámbito delictivo.

Las causa de justificación se han agrupado al lado de otras causas que anulan el delito o que impiden su configuración, catalogándolas el Nuevo Código Penal como causas de exclusión del delito, pero las mismas son causas de licitud:

1.- La legítima defensa.

Pavón Vasconcelos establece: la legítima defensa "es la repulsa inmediata, necesaria y proporcionada a una agresión actual e injusta, de la cual deriva un peligro inminente para bienes tutelados por el Derecho."[150]

La legítima defensa se encuentra prevista en el artículo 29 fracción IV del Nuevo Código Penal para el Distrito Federal, que establece lo siguiente:

---

[148] Jiménez de Asúa, Luis, ***Lecciones de Derecho Penal***, Editorial, Pedagógica Iberoamericana, Colección Clásicos del Derecho, México, 1995, Pág. 184.
[149] Castellanos Tena, ***Op. cit.***, Pág.183.
[150] Pavón Vasconcelos, ***Op. cit.***, Pág. 327.

Legítima defensa.- Se repela una agresión real, actual o inminente y sin derecho, en defensa de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa empleada y no medie provocación dolosa suficiente e inmediata por parte del agredido o de su defensor.

Se presume que existe legítima defensa, salvo prueba en contrario, cuando se cause un daño a quien por cualquier medio trate de penetrar o penetre, sin derecho, al lugar en que habite de forma temporal o permanente el que se defiende, al de su familia o al de cualquier persona respecto de las que el agente tenga la obligación de defender, a sus dependencias o al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación. Igual presunción existirá cuando el daño se cause a un intruso al momento de sorprenderlo en alguno de los lugares antes citados en circunstancias tales que revelen la posibilidad de una agresión."

Los elementos de la legítima defensa, se desprenden, de la noción legal, como elementos de la legítima defensa los siguientes a) la existencia de una agresión; b) un peligro de daño, derivado de ésta, y c) una defensa, rechazo de la agresión o contraataque para repelerla. Por otra parte los casos en que la defensa es inexistente son los siguientes:

a) Cuando la agresión no reúna los requisitos legales señalados,

b) Cuando la agresión no haga surgir un peligro inminente para los bien protegidos,

c) Cuando el agredido haya provocado la agresión, dando causa inmediata y suficiente para ella.

2.- Estado de Necesidad.

El estado de necesidad, es una situación de peligro actual para los intereses protegidos por el Derecho, en la cual no queda otro remedio que la

violación de los intereses de otro, jurídicamente protegidos, el estado de necesidad es por consiguiente un caso de colisión de intereses.

Esta causa de justificación se encuentra tipificada en el mismo artículo 29 fracción V del Nuevo Código Penal para el Distrito Federal, y establece:

Estado de necesidad.- Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el sujeto, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo.

3.- Cumplimiento de un deber y ejercicio de un derecho.

Toda conducta o hechos tipificados en la ley constituyen, situaciones prohibidas, por contenerse en ellas mandatos de no hacer (de abstención), más cuando se realizan en el cumplimiento de un deber o en el ejercicio de un derecho adquieren carácter de licitud, excluyendo la integración del delito y eliminando toda responsabilidad penal.

El Código Penal establece en la fracción VI del artículo 29, como excluyente del delito el cumplimiento de un deber y ejercicio de un derecho:

Cumplimiento de un deber o ejercicio de un derecho.- La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional de la conducta empleada para cumplirlo o ejercerlo;

El cumplimiento de un deber, es cuando se cumple con la ley, no se ejecuta un delito por realizar el hecho típico, se acata el mandato legal.

4.- Consentimiento del interesado.

Esta causa de justificación se encuentra prevista en el artículo 29 fracción III y que a la letra dice:

Consentimiento del titular.- Se actúe con el consentimiento del titular del bien jurídico afectado, o del legitimado legalmente para otorgarlo, siempre y cuando se cumplan los siguientes requisitos:

a) Que se trate de un bien jurídico disponible;

b) Que el titular del bien jurídico, o quien esté legitimado para consentir, tenga la capacidad jurídica para disponer libremente del bien; y

c) Que el consentimiento sea expreso o tácito y no medie algún vicio del consentimiento.

Se presume que hay consentimiento, cuando el hecho se realiza en circunstancias tales que permitan suponer fundadamente que, de haberse consultado al titular del bien o a quien esté legitimado para consentir, éstos hubiesen otorgado el consentimiento.

En el delito contemplado en el artículo 231 fracción XIV del Nuevo Código Penal, habrá antijuricidad cuando la conducta del sujeto activo se introduzca ilícitamente a los programas o sistemas informáticos del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores.

En el caso de las causas de justificación, no se presentan causas de justificación en este tipo de delito, tomando en consideración lo siguiente:

- Legítima defensa.- No se presenta en virtud de que para que se integre esta causa de justificación, se necesita repeler una agresión, real, actual o inminente y sin derecho en protección de bienes jurídicos propios o ajenos, pero en el caso concreto del tipo penal que analizamos, es imposible que el hecho delictuoso se cometa reaccionando a una agresión determinada. Asimismo,

tampoco se puede presentar las presunciones de legítima defensa prevista en artículo 29 fracción IV.

- Estado de necesidad.- La conducta que despliega el sujeto activo en el delito de contemplado en el artículo 231 fracción XIV, no puede amparase bajo el hecho de que actuó por salvaguardar un bien jurídico propio o ajeno de ante actual e inminente y que por ello se lesione el bien jurídico, lo anterior, en razón de que es un delito doloso, en donde se quiere y acepta el resultado por lo tanto no se produce el resultado por una circunstancia de peligro.

- Cumplimiento de un deber jurídico o ejercicio de un derecho.- En nuestra opinión, en este delito, el agente tampoco puede alegar un cumplimiento de un deber, puesto que no hay ningún ordenamiento jurídico penal que ordene o imponga que para que una persona obtenga un beneficio para si o para un tercero, por cualquier medio accese de manera ilícita a los programas informáticos del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o recursos, independientemente de que los recursos no salgan de la institución.

- Consentimiento del interesado.- Esta causa excluyente, gira alrededor de los denominados bienes disponibles y aunque el patrimonio es considerado por algunos autores como un bien disponible, no podemos determinar que en este delito el sujeto pasivo o titular del bien jurídico titulado, pueda dar su consentimiento y así resulte afectado su patrimonio, además de que en ese delito en particular, las técnicas informáticas utilizadas para su comisión son muy diversas y evidentemente ignoradas por el afectado.

Pero en el supuesto en que el sujeto pasivo proporcionare su consentimiento para que el agente lleve a cabo operaciones, transferencias o movimientos de dinero o valores, independientemente de que no salgan de la institución financiera de que se trate, entonces si podrá operar la causa de excluyente del delito.

4.3.7. Imputabilidad.

Castellanos Tena establece: “para ser culpable un sujeto, precisa que antes sea imputable, si en la culpabilidad, interviene el conocimiento y la voluntad, se requiere la posibilidad de ejercer esas facultades, para que el individuo conozca la ilicitud de su acto y si quiere realizarlo, debe tener la capacidad de *entender* y de *querer*, de determinarse en función de aquello que conoce, luego la aptitud (intelectual y volitiva) constituye el presupuesto necesario de la culpabilidad. Por eso la imputabilidad, se debe considera como el soporte o cimiento de la culpabilidad y no como un elemento del delito, como pretenden algunos especialistas.”[151]

Se define a la imputabilidad como la capacidad de entender y de querer en el derecho penal.

Por su parte el maestro Raúl Carrancá y Trujillo, señala que será imputable “todo aquel que posea, al tiempo de la acción, las condiciones psíquicas exigidas, abstracta e indeterminadamente por la ley para poder desarrollar su conducta socialmente, todo el que sea apto e idóneo o jurídicamente para observar una conducta que responda a las exigencias de la vida en sociedad humana.”[152]

Por lo tanto, sólo puede ser culpable el sujeto que sea imputable, esto es, que para que una conducta en su doble aspecto, acción u omisión, pueda ser atribuida a un sujeto, debe demostrarse el elemento psíquico de la conducta que lo ligue a su acto.

Como fundamento de la imputabilidad, se han sostenido durante largos siglos los principios del libre albedrío y de la responsabilidad moral, estimándolos inmutables, la libertad es un atributo indispensable de la voluntad, de tal suerte que ésta no puede existir sin aquélla, del mismo modo que no puede haber

[151] Castellanos Tena, ***Op. cit.***, Pág. 217.
[152] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág.222.

materia sin gravedad. La imputabilidad se fundó así, en el concurso de la inteligencia y de la libre voluntad humana. En consecuencia, donde faltara el libre albedrío o libertad de elección, no cabría aplicación de pena alguna cualquiera que fueran las circunstancias de la acción y las condiciones propias del sujeto.

La imputabilidad es la capacidad jurídica de entender y querer en el ámbito penal, que se conforma con la conciencia y voluntad necesarias para que la persona pueda responder de sus propios actos y ser sujeto de las disposiciones penales. La responsabilidad, da origen a una situación jurídica en la que el individuo imputable se encuentra en una posición de dar cuenta de su actuar a la sociedad y quienes están en tal posibilidad, son aquellos que tienen desarrollada la mente y no padecen alguna anomalía psicológica que los imposibilite de alguna manera a entender y querer.

Actiones liberae in causa.

Se llaman *actiones liberae in causa* las que en su causa son libres, aunque determinadas en sus efectos. Se producen cuando la acción se decidió en estado de imputabilidad, pero el resultado se produjo en estado de inimputabilidad.

En nuestro derecho las *actiones liberae in causa* son consideradas como dolosas, sin prueba en contrario, a virtud de que el dolo se presume *juris et de jure* cuando el imputado previó o pudo prever la consecuencia (necesaria y notoria del hecho u omisión en que consistió el delito) por ser efecto ordinario del hecho u omisión y estar al alcance del común de las gentes.

La imputabilidad debe existir en el momento de la ejecución del hecho, pero en ocasiones el sujeto, antes de actuar, voluntaria o culposamente se coloca en situación inimputable y en esas condiciones produce el delito.

A estas acciones se les llama *actiones liberae in causa* (libres en su causa, pero determinadas en cuanto a su efecto), por ejemplo, alguien que

decide cometer homicidio y para darse ánimo bebe con exceso y ejecuta el delito en estado de ebriedad, aquí sin duda existe causa de imputabilidad, entre el acto voluntario y su resultado.

Requisitos de la conducta libre en su causa son:

a) Un sujeto con previa capacidad
b) Una conducta que produce o no evita el estado de inimputabilidad;
c) Una conducta dolosa o culposa, previa al estado de inimputabilidad;
d) Un estado de inimputabilidad por parte del sujeto, y
e) producción o no de un resultado típico.

4.3.8. Inimputabilidad.

La imputabilidad es soporte básico y esencial de la culpabilidad, sin aquella no existe ésta y sin culpabilidad no puede configurarse el delito, por lo que la imputabilidad es indispensable para la formación de la figura delictiva.

Como hemos visto líneas arriba, la imputabilidad es calidad del sujeto referida al desarrollo y la salud mental, la inimputabilidad constituye el aspecto negativo de la imputabilidad. “Las causas de inimputabilidad son, todas aquellas capaces de anular o neutralizar, ya sea el desarrollo o la salud de la mente, en cuyo caso el sujeto carece de aptitud para la delictousidad.”[153]

La inimputabilidad, se manifiesta como la falta de capacidad para conocer y comprender el carácter ilícito de la acción, esto es, “la inimputabilidad supone, consecuentemente la ausencia de dicha capacidad y por ello incapacidad para conocer la ilicitud del hecho o bien para determinarse en forma espontánea conforme a esa comprensión.”[154]

[153] Castellanos Tena, ***Op. cit.***, Pág. 223.
[154] Pavón Vasconcelos, Francisco, ***Imputabilidad e Inimputabilidad***, 4ª Edición, Porrúa, México, 2000, Pág.101.

El artículo 29 en la fracción VII, establece la inimputabilidad y la acción libre en su causa de la siguiente manera:

Inimputabilidad y acción libre en su causa.- Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el sujeto hubiese provocado su trastorno mental para en ese estado cometer el hecho, en cuyo caso responderá por el resultado típico producido en tal situación.

Cuando la capacidad a que se refiere el párrafo anterior se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 65 de este Código.

Interpretando esta fracción a, se desprende que en el momento de realizarse la acción típica, el sujeto activo debe poseer la capacidad de percibir la magnitud de su actuación, esto es, no debe de padecer dicho sujeto de algún problema de carácter mental o intelectual, asimismo, dicha circunstancia no debe ser provocada dolosa o culposamente por parte del sujeto activo, para no responder por determinado resultado, así como también el agente no hubiese previsto dicha circunstancia.

En este sentido, el sujeto activo no tiene la capacidad de entender o no tiene la salud mental suficiente, en consecuencia no se le puede imputar o atribuir determinada conducta, debido al desequilibrio de su salud mental ya sea que se deba a diversos factores, como alguna enfermedad cerebral, trastorno mental, la edad del sujeto o por un desarrollo intelectual deficiente que no le permite entender la ilicitud de su proceder, si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que cometió, por las circunstancias anteriormente señaladas.

La mayoría de edad, también se ha considerado una causa de inimputabilidad, en base a un criterio de inmadurez mental, por lo que la

inimputabilidad de los menores de edad implica la imposibilidad de que queden sujetos a los procedimientos jurisdiccionales regulares, en nuestro país en el artículo 12 del Nuevo Código Penal para el Distrito Federal, se establece la edad penal, señalando que las disposiciones del Código, se aplicarán a todas las personas a partir de los dieciocho años de edad, sin embargo se aplica al caso concreto, la Ley para el tratamiento de menores infractores, para el Distrito Federal en materia común y para toda la República en materia Federal, en la que es establece en su artículo 6°, que el Consejo de menores es competente para conocer de la conducta de las personas mayores de 11 y menores de 18 años de edad:

ARTICULO 6o.- El Consejo de Menores es competente para conocer de la conducta de las personas mayores de 11 y menores de 18 años de edad, tipificada por las leyes penales señaladas en el artículo 1o. de esta Ley. Los menores de 11 años, serán sujetos de asistencia social por parte de las instituciones de los sectores público, social y privado que se ocupen de esta materia, las cuales se constituirán, en este aspecto, como auxiliares del Consejo.

Cuando el menor alegue tener la calidad de indígena, la misma se acreditará con su sola manifestación. Cuando exista duda de ella o fuere cuestionada, se solicitará a las autoridades comunitarias la expedición de la constancia que acredite la pertenencia del individuo a un determinado pueblo comunidad (sic).

La competencia del Consejo se surtirá atendiendo a la edad que hayan tenido los sujetos infractores, en la fecha de comisión de la infracción que se les atribuya; pudiendo, en consecuencia, conocer de las infracciones y ordenar las medidas de orientación, protección y tratamiento que correspondan, aun cuando aquéllos hayan alcanzado la mayoría de edad.

En el ejercicio de sus funciones el Consejo instruirá el procedimiento, resolverá sobre la situación jurídica de los menores y ordenará y evaluará las

medidas de orientación, protección y tratamiento que juzgue necesarias para su adaptación social.

En el caso del tipo penal previsto en el artículo 231 fracción XIV será imputable, el sujeto activo que en el momento de cometer el hecho delictivo, haya tenido la capacidad de querer y entender en el ámbito penal, al momento de realizar el hecho típico, el sujeto activo tiene la capacidad de comprender el carácter ilícito de su actuar o de conducirse de acuerdo a esa comprensión, no padeciendo ningún trastorno mental o desarrollo intelectual retardado.

El sujeto activo, es por lo tanto una persona que necesita tener determinada capacidad intelectual para poder realizar la conducta típica, por lo que debe ser imputable, es decir, debe tener la capacidad de querer y entender, toda vez que para consumar el ilícito se requiere que el sujeto activo tenga un elevado coeficiente intelectual para poder producir el resultado típico, ya que las personas que cometen estas conductas delictivas, requieren de conocimientos en tecnología informática, para poder accesar a los sistema o programas.

Ahora bien, en el aspecto negativo que es la inimputabilidad, anula la capacidad del sujeto, para comprender el carácter ilícito de su conducta o de conducirse conforme a esa comprensión, ya sea por padecer trastorno mental o desarrollo intelectual retardado, que en este delito, no se da ninguno de los supuestos de inimputabilidad.

La minoría de edad, como hipótesis de inimputabilidad, es dable en este tipo penal, ya que la acción puede ser realizada por un menor de edad con conocimientos en informática, en la inteligencia de que la naturaleza del ilícito lo permite, pero debido a la edad del sujeto activo se presenta la falta de capacidad en el menor, es decir, no le permite entender el alcance de su proceder, en virtud de que no tiene la capacidad de comprender el carácter ilícito de su acción o de conducirse de acuerdo con esa comprensión, ya que en la minoría de edad, se presenta la inmadurez mental, pues no alcanzan a comprender el alcance de su actuación.

La mayoría de las personas que realizan este acceso ilícito a los sistemas o programas de informática y en particular, del sistema financiero, son individuos mayores de edad que cuentan con la capacidad volitiva o intelectual, es decir, de comprender el carácter ilícito de su actuar o de conducirse de acuerdo a su comprensión para poder realizar la conducta típica.

4.3.9. Culpabilidad.

Una conducta será delictuosa no sólo cuando sea típica y antijurídica, sino además culpable. "La conducta se considera culpable, cuando a causa de las relaciones psíquicas entre ella y su autor, debe serle jurídicamente reprochada."[155]

En sentido amplio, la culpabilidad ha sido estimada como "el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica. La libertad de voluntad y la capacidad de imputación, constituyen un presupuesto de la culpabilidad, pues el reproche supone necesariamente libertad de decisión y capacidad de reprochabilidad."[156]

La culpabilidad, "es el reproche hecho a una persona por haber cometido un injusto, es decir, por haber realizado una conducta típica y antijurídica."[157]

Para Villalobos, "la culpabilidad, consiste en el desprecio del sujeto por el orden jurídico y por los mandatos y prohibiciones que tienden a constituirlo y conservarlo, desprecio que se manifiesta por franca oposición en el dolo o indirectamente, por indolencia o desatención nacidas del desinterés o subestimación del mal ajeno frente a los propios deseos, en la culpa."[158]

Se ha considerado que en la culpabilidad existe una relación de causalidad psicológica entre el agente y su conducta contraria a lo dispuesto por la ley, lo que origina como ya lo hemos mencionado, un juicio de reprobación por

[155] Cuello Calón, Eugenio, ***Op. cit.***, Pág. 290.
[156] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág. 362.
[157] Malo Camacho, Gustavo ***Op. cit.***, Pág. 521.
[158] Pavón Vasconcelos, Francisco, ***Op. cit.***, Pág. 283.

esta, la culpabilidad tiene un carácter subjetivo y está íntimamente ligada con la antijuricidad, ya que si una conducta no es antijurídica no habrá culpabilidad, esto en atención al principio de *nulla poena sine culpa*.

Formas de la culpabilidad.

La culpabilidad presenta dos vertientes, el dolo y la culpa. El dolo, es causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuricidad del hecho y la culpa, es cuando se realiza la conducta sin llevar la voluntad a la producción de un resultado típico, pero éste surge a pesar de ser previsible y evitable, por efectuarse la conducta por medio de la negligencia, imprudencia o bien por descuidar las precauciones indispensables por parte de sujeto activo y que le eral legalmente exigidas.

- **Dolo.**

Eugenio Cuelo Calón, dice que el dolo "consiste en la voluntad consciente dirigida a la ejecución de un hecho que la ley prevé como delito o simplemente en la intención de ejecutar un hecho delictuoso."[159]

El dolo consiste en el actuar, consciente y voluntario, dirigido a la producción de un resultado típico y antijurídico.

El artículo 18 del Nuevo Código Penal para el Distrito Federal, establece que las acciones o las omisiones delictivas solamente pueden realizarse dolosa o culposamente:

ARTÍCULO 18 (Dolo y Culpa). Las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente.

Obra dolosamente el que, conociendo los elementos objetivos del hecho típico de que se trate, o previendo como posible el resultado típico, quiere o acepta su realización.

[159] Cuello Calón Eugenio, citado pro Castellanos Tena, ***Op. cit.***, Pág. 239.

Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación de un deber de cuidado que objetivamente era necesario observar.

Clases de dolo.

- **Dolo directo**.- El dolo es directo cuando la voluntad es encaminada directamente al resultado previsto, existiendo identidad entre el acontecimiento real y el representado: si una persona apuñala a otra y la mata, obrando con animus occidendi o necandi, esto es, con voluntad de causar ese resultado típico, comete homicidio con dolo directo. Para Cuello Calón el dolo es directo "cuando el agente ha previsto como seguro y ha querido directamente el resultado de su acción u omisión, o los resultados ligados a ella de modo necesario; aquí el resultado corresponde a la intención del agente."[160]

- **Dolo indirecto.-** Conocido también como dolo de consecuencia necesaria, se presenta cuando el agente actúa o realiza el hecho delictuoso, no obstante la seguridad o certeza de que con su conducta causará otros resultados típicos y antijurídicos que no persigue de manera directa y a pesar de ello, no renuncia a la ejecución de su conducta, aceptando así sus consecuencias.

- **Dolo eventual.-** El agente desea un resultado, típico concreto, peor al mismo tiempo se presenta otro u otros posibles resultados delictuosos que no quiere directamente y a pesar de ello no renuncia a la ejecución del hecho, aceptando asimismo las consecuencias. Es cuando el agente, prevé la posible consecuencia de la propia acción. Se tiene entonces la hipótesis de la representación de varios eventos con voluntad limitada a uno de ellos, hipótesis que no puede ser referida al dolo directo, ni a la culpa con previsión.

- **Dolo indeterminado.-** La acción está orientada a producir varios posibles resultados y por ello se le denomina igualmente dolo alternativo. El

[160] ***Idem.***

agente tiene la intención genérica de delinquir, sin proponerse causar un delito en especial, existe la seguridad de causar daño sin saber cual será; en esta clase de dolo, la conducta está orientada a producir varios posibles resultados y por ello también se le denomina alternativo.

- **Dolo genérico y dolo específico**. En realidad, no existe consenso en la doctrina respecto a la noción del llamado dolo genérico, pues unos lo hacen consistir en la voluntad de dañar considerada en abstracto, en tanto otros lo identifican con el propósito de causar daño, sin que quede ahí la cuestión: también se le caracteriza por el *animus* o por el motivo particular del agente, etc., razón por la que muchos niegan su existencia al proclamar que sólo existen dolos específicos, que se identifican con las causas del delito.

- **Dolo de daño y dolo de peligro**. Consiste el primero en querer causar daño, ya lesionando o destruyendo el bien jurídico contra el que va encaminada la conducta delictiva del autor. El dolo de peligro es el dolo peculiar de los delitos de peligro, pues en él el autor quiere la simple amenaza del bien jurídico. El dolo de peligro ha sido negado por algunos, pues se piensa que en el querer dirigido a causar el daño o lesión a determinado bien, el peligro al mismo constituye un grado inferior, resultando evidente que a la lesión misma precede el peligro.

- **Culpa.**

Se afirma la existencia de culpa "cuando la actitud del sujeto, enjuiciada a través del imperativo de los deberes impuestos por la ley, es reprochable a virtud de la inobservancia de la prudencia, atención, pericia, reglas, órdenes, disciplinas, etc., necesarias para evitar la producción de resultados previstos en la ley como delictuosos."[161]

[161] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág. 405.

La culpa es una de las formas de culpabilidad, por lo tanto habrá culpa, cuando se obra sin intención y sin diligencia debida, causando un resultado dañoso, previsible y penado por la ley, pues el sujeto realiza una conducta, sin que la voluntad se encamine precisamente a la producción de un resultado típico, pero éste surge a pesar de ser previsible y evitable, ya sea por negligencia o bien, por imprudencia, dejando a un lado las precauciones legalmente exigidas.

Elementos de la culpa.

Raúl Carrancá y Trujillo, señala el conjunto de elementos que considera constitutivos de la culpa, detallándolos de la siguiente manera:

a) Una conducta voluntaria, ya sea de acción u omisión, consciente y voluntaria, pero no intencional.
b) Un resultado típico y antijurídico.
c) Nexo causal entre la conducta y el resultado.
d) Naturaleza previsible y evitable del evento.
e) Ausencia de voluntad del resultado.
f) Violación de los deberes de cuidado.

Clases de culpa.

- **Culpa consciente, con previsión o con representación**.-Es cuando el sujeto ha previsto el resultado típico o delictivo como posible, es decir, representa como posible que de su conducta se originen consecuencias que no solamente no quiere, con la esperanza que no ocurrirán.

- **Culpa inconsciente, sin previsión o sin representación.**- Por lo contrario, en esta clase de culpa, se está en presencia de la culpa inconsciente (sin representación) cuando el sujeto no previó el resultado por falta de cuidado, teniendo obligación de preverlo por ser de naturaleza previsible y evitable.

En el delito establecido en el artículo 231 fracción XIV, no se presenta la culpa, es un delito de dolo, ya que conoce los elementos objetivos del hecho típico, prevé el resultado típico y sin embargo quiere y acepta su realización.

4.3.10. Inculpabilidad.

Con el nombre de inculpabilidad se conocen las causas que impiden la integración de la culpabilidad, evidente tautología, según expresión de Jiménez de Asúa.

"La inculpabilidad, es "la ausencia de culpabilidad, opera al hallarse ausentes los elementos esenciales de la culpabilidad: *conocimiento y voluntad*, tampoco será culpable una conducta si falta alguno de los otros elementos del delito o la imputabilidad del sujeto, porque si el delito integra un todo, sólo existirá mediante la conjugación de los caracteres constitutivos de su esencia."[162]

Son dos las causas genéricas de exclusión de la culpabilidad:

a) El error, y
b) La no exigibilidad de otra conducta

a) El error.

"El error es un vicio psicológico consistente en la falta de conformidad entre el sujeto cognoscente y el objeto conocido, tal y como éste es en la realidad, el error es un falso conocimiento de la verdad, un conocimiento incorrecto, se conoce, pero se conoce equivocadamente"[163]

"El error, consiste en una idea falsa o errónea respecto a un objeto, cosa o situación, constituyendo un estado positivo."[164]

---

[162] Castellanos Tena, ***Op. cit.***, Pág. 257.
[163] ***Cfr.*** Castellanos Tena, ***Op. cit.***, Págs. 257-258.
[164] Pavón Vasconcelos, Francisco, ***Op. cit.***, Pág. 433.

Al respecto, Carrancá y Trujillo nos explica el por qué el error puede constituirse como un excluyente de delito, toda vez que "para que exista dolo se requiere el conocimiento de los elementos componentes del resultado, si éste faltare aquél podrá estar ausente. Se estará entonces en presencia de una causa de inculpabilidad. Tal ocurre en los casos de error a diferencia de la ignorancia, que es carencia de conocimiento, entendido por él el falso o equivocado conocimiento acerca de algo. Su consecuencia en relación con el elemento intelectual del dolo es la falta de previsión del resultado, por lo que el error viene a ser como lo inverso al dolo."[165]

El error, se ha dividido en *error de hecho* y en *error de derecho*, el error de hecho o *facti* es le que recae sobre el resultado o las circunstancias determinadas de éste, en tanto que el error de derecho, es el que recae sobre la valoración o apreciación jurídica acerca de una conducta y su resultado.

Pavón Vasconcelos establece, que podemos determinar la existencia del error de derecho, "cuando un sujeto, no obstante conoce la conducta que realiza, está ignorante de la obligación que tiene de respetar una norma penal o extrapenal determinada, ya por desconocimiento de la propia norma, dispositiva o prohibitiva, o bien porque su conocimiento de ella es inequívoco y para que sea considerado como una causa de exclusión de la culpabilidad, debe ser invencible e insuperable, es decir, que el sujeto esté imposibilitado para conocer la ilicitud de su conducta, ya sea de acción u omisión."[166]

El error de hecho se subdivide a su vez en esencial y accidental, en el error esencial hay por parte del agente desconocimiento de la antijuricidad de su conducta y por ello, constituye el aspecto negativo del dolo.

Al respecto, Pavón Vasconcelos puntualiza:"el error esencial de hecho será invencible cuando recaiga sobre uno de los elementos necesarios para la integración del delito, o sea, respecto de los elementos objetivos del delito o sobre

[165] Carranca y Trujillo, Raúl, ***Op. cit.***, Pág. 405.
[166] Pavón Vasconcelos, Francisco, ***Op. cit.***, Pág. 470.

el resultado de la conducta o sobre alguna circunstancia agravante de la penalidad."[167]

Por otra parte el *error esencial vencible* se produce cuando un sujeto puso y debió prever el error, excluyendo sólo el dolo pero no la culpa, salvo que el delito no permita la forma de comisión culposa. El *error de hecho accidental*, no recae sobre ninguno de los elementos cuya concurrencia es necesaria para que se configure el delito, y abarca los siguientes aspectos: *aberratio ictus, aberratio in persona* y *aberratio delicti.*

El error en el golpe (*aberratio ictus*), se da cuando el resultado no es precisamente el querido o el deseado por el sujeto, pero si equivalente, hay por lo tanto una desviación en el golpe. El *aberratio in persona,* es cuando el error versa sobre la persona, objeto del delito. Y en el *aberratio delicti*, se produce un delito diferente al deseado.

Es necesario señalar que algunos especialistas utilizan los términos de error de tipo y error de prohibición, en lugar de error de hecho y de derecho, denominando igualmente al error de prohibición, error de licitud o de permisión.

El denominado error de tipo lo encontraremos previsto en la fracción VIII inciso del articulo 29 del Nuevo Código Penal, que dispone también como excluyente del delito cuando se realice la acción o la omisión bajo un error invencible, sobre alguno de los elementos objetivos que integran la descripción legal del delito del que se trate, es decir, que el error recaiga sobre un elemento o requisito constitutivo del tipo penal.

El inciso b) establece a su vez el error de prohibición o de derecho, que se da cuando la acción o la omisión se realice bajo un error invencible respecto de la ilicitud de la conducta, ya sea por que el sujeto desconozca la existencia de la ley o el alcance de la misma o porque cree que esta justificada su conducta, denominada esta ultima parte por error de permisión error de prohibición indirecto,

[167] ***Ibidem***, Pág.471.

originándose con ello el tema de las eximentes putativas, que son causas de inculpabilidad que aunque no están expresamente reglamentadas en la ley, se desprenden dogmáticamente.

En el artículo 29, fracción VIII, de nuestro Nuevo Código Penal, establece lo siguiente:

Error de tipo y error de prohibición. Se realice la acción o la omisión bajo un error invencible, respecto de:

a) Alguno de los elementos objetivos que integran la descripción legal del delito de que se trate; o

b) La ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma o porque crea que está justificada su conducta.

Si los errores a que se refieren los incisos anteriores son vencibles, se estará a lo dispuesto en el artículo 83 de este Código.

Estos eximentes putativas, son situaciones en las que el agente, por un error esencial de hecho insuperable cree fundadamente, al realizar un hecho típico del derecho penal, hallarse amparado por una justificante, o ejecutar una conducta atípica permitida, licita, sin serlo.

Dentro de las eximentes putativas tenemos las siguientes:

a) Legítima defensa putativa
b) Estado necesario putativo
c) Cumplimiento de un deber o ejercicio de un derecho putativos sujeto en el juicio de reproche.

La no exigibilidad de otra conducta.

Se afirma que la no exigibilidad de otra conducta es también una causa eliminatoria de la culpabilidad, pues no es posible exigir al autor un actuar de manera distinta a como lo hizo, o sea, que no se le puede exigir que hubiera actuado conforme a derecho, aun cuando en el momento de la ejecución del hecho delictivo existía la comprensión de la antijuridicidad del acto.

Así pues, nuestra ley sustantiva penal contempla de igual modo como excluyente del delito en el artículo 29 fracción IX, cuando ante las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente una conducta diversa a la que realizo, en virtud de no haberse podido determinar a actuar conforme a derecho.

Estado de necesidad tratándose de bienes de la misma entidad.

La conducta de quien sacrifica un bien para salvar a otro del mismo valor, no es delictuosa, ya que según alguno autor, debe operar a favor del agente una causa de inculpabilidad por la no exigibilidad de otra conducta.

Vis compulsiva.- Que es una fuerza moral, por la que el sujeto pasivo puede elegir entre la realización o no de la conducta, es decir, es resistible, pudiendo ser una causa de inculpabilidad por la no exigibilidad de otra conducta.

El tipo penal previsto en el artículo 231 fracción XIV, como hemos dicho es doloso, el sujeto activo requiere tener la voluntad y el conocimiento para llevar a cabo la conducta y así aceptar el resultado producido por la misma por lo que consideramos que difícilmente pudiera presentarse un error invencible de tipo, la conducta de acción desplegada por el agente, no puede realizarse bajo un error invencible sobre algunos de los elementos del tipo penal que contempla el delito que se analiza.

No puede presentarse un error invencible de prohibición en este tipo penal, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la

misma o porque crea que esta justificada su conducta, toda vez que el agente al acceder, entrar o introducirse por cualquier medio a un sistema o programa informático del sistema financiero e indebidamente realizar operación, transferencias o movimientos de dinero o valores, al obtener un beneficio para si o para un tercero, sabe que su conducta no esta siendo licita y que por lo tanto es prohibida.

Tampoco es posible que se produzca el resultado típico en este delito, si el sujeto activo hubiera actuado de manera licita, cuidadosa y precavida y este se produjeran debido a una causa ajena e incontrolable (caso fortuito), pues el delincuente en este tipo de delitos, conduce su actuar precisamente a obtener un beneficio para sí o para un tercero sin que intervenga ninguna causa ajena más que su propia voluntad y conocimiento.

Es inaceptable, que se presente en este delito como causa de inculpabilidad, el estado de necesidad, ya que en ningún momento podemos decir que el agente sacrifique un bien para salvar a otro del mismo valor, pues su objetivo primordial es obtener un beneficio para sí o para un tercero, no importando a quien a quienes afecte en su patrimonio.

4.3.11. Punibilidad.

"La punibilidad consiste en el merecimiento de una pena, en función de la realización de cierta conducta. Un comportamiento es punible cuando se hace acreedor a una pena, tal merecimiento acarrea la conminación legal de aplicación de esa sanción."[168]

La punibilidad consiste en el merecimiento de una pena en función de la realización de cierta conducta. Por punibilidad entendemos, la amenaza de pena que el Estado asocia a la violación de los deberes consignados en las normas jurídicas, dictadas para garantizar la permanencia del orden social.

[168] Castellanos Tena, ***Op. cit.***, Pág. 275.

En resumen, punibilidad es:

a) Merecimiento de penas;
b) Conminación estatal de imposiciones si se llenan los presuntos legales y
c) Aplicación fáctica de las penas señaladas en la ley.

De lo anterior, concluimos que la punibilidad consiste en el merecimiento de una pena, en función de la realización de cierta conducta que la ley considera delito o la conminación estatal de imposición de sancione, siempre y cuando se satisfagan los presupuestos legales.

La punibilidad del tipo penal descrito en el artículo 231 fracción XIV, esta contemplada en el artículo 230 de nuestra legislación penal:

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

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

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

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

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

Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores.

Sin embargo, es importante volver a destacar que este tipo penal se encuentra ubicado erróneamente, inmediatamente después del fraude, como ya lo hemos dicho, la conducta no se realiza por medio del engaño ni se aprovecha del error de nadie, se da un apoderamiento, con ánimo de dominio y sin el consentimiento de quien legalmente pueda otorgarlo, por lo que la punibilidad debe ser la que establece el artículo 220 del Nuevo Código Penal para el Distrito Federal, por ello consideramos conveniente llevar a cabo la reforma a este artículo, para los efecto de ubicarlo dentro del robo y que establece:

ARTÍCULO 220. Al que con ánimo de dominio y sin consentimiento de quien legalmente pueda otorgarlo, se apodere de una cosa mueble ajena, se le impondrán:

I. Se deroga (Publicado en la Gaceta Oficial del Distrito Federal el 15 de mayo del 2003).

II. Prisión de seis meses a dos años y sesenta a ciento cincuenta días multa, cuando el valor de lo robado no exceda de trescientas veces el salario mínimo o cuando no sea posible determinar el valor de lo robado;

III. Prisión de dos a cuatro años y de ciento cincuenta a cuatrocientos días multa, cuando el valor de lo robado exceda de trescientas pero no de setecientas cincuenta veces el salario mínimo, y

IV. Prisión de cuatro a diez años y de cuatrocientos a seiscientos días multa, cuando el valor de lo robado exceda de setecientos cincuenta veces el salario mínimo.

Para determinar la cuantía del robo, se atenderá únicamente al valor de mercado que tenga la cosa en el momento del apoderamiento.

4.3.12. Excusas absolutorias.

En función de las excusas absolutorias no es posible la aplicación de la pena, en presencia de una excusa absolutoria, los elementos del delito permanecen, sólo se excluye la posibilidad de punición.

En cambio existen las causas de impunidad de la conducta o del hecho típico, antijurídico y culpable, las cuales, constituyen el aspecto negativo de la punibilidad y originan la inexistencia del delito, se caracterizan porque dejan subsistir el carácter delictivo de una conducta, excluyendo la posibilidad de punición, es decir, de imposición de una pena, que no es más que el medio represivo o castigo del que se vale la sociedad para sancionar una conducta delictuosa, impuesta desde luego, por la autoridad legitimada para ello.

El delito que establece el artículo 231 fracción XIV, no se pueden darse excusas absolutorias, por la importancia que tiene la conducta no puede excluirse de una punición.

4.3.13. Aspectos colaterales.

- Iter criminis. El Iter criminis o camino del delito comprende el estudio de las fases recorridas por el delito, desde su ideación hasta su agotamiento, aun cuando se trate de aquellos que se realizan en forma casi instantánea. El iter criminis consta de dos fases, una interna, cuando no se ha exteriorizado todavía y, la otra externa, cuando la resolución de delinquir se ha manifestado.

- Fase interna. Se dan tres momentos: a) ideación que le corresponde al ámbito del psique; b) deliberación, que consiste en la lucha interna de hacer o no; y c) Resolución, que es en sí la decisión.

La ideación es la representación subjetiva del hacer o no que conlleva una consecuencia objetiva, es decir, este es el primer momento en el que surge en el sujeto la idea determinada por caracteres volitivos delictuosos.

Durante la llamada deliberación, se produce el proceso psíquico de la lucha entre la idea criminosa y aquellos factores de carácter moral o utilitario que pugna contra ella.

Si persiste la concepción criminosa, después de haber concluido el proceso psíquico, se ha tomado la resolución, última etapa de la fase interna o

subjetiva, sin embargo, hasta entonces no hay una trascendencia penal, pues de igual modo no hay materialización de la idea criminal. El derecho regula, principalmente, relaciones entre personas, es por ello que se aplica el principio consagrado en la fórmula "*Cogitationes poenam nemo patitur*", el pensamiento no delinque.

La fase interna, se presentará en la mente del agente cuando surja la idea de cometer el tipo penal que se analiza, después delibera respecto de los obstáculos que pudieran presentarse en la comisión y resuelve cometer el delito, lo que originará que se exteriorice esta voluntad.

- Fase externa. Es aquella en la que el sujeto exterioriza su idea criminal, ello implica una acción que se materializa a través de dos fases que son: a) la realización de actos preparatorios que son aquellos que sirven para realización de los actos, y pueden ser equívocos y unívocos; y b) actos de ejecución, que son los que ponen en movimiento el verbo núcleo del tipo delictivo.

Inicia cuando el sujeto activo exterioriza su conducta, preparando los elementos necesarios para la realización como lo es el equipo informático, número de cuentas bancarias, passwords, para que los ejecute hasta obtener un beneficio para sí o para un tercero.

4.4. Tentativa.

La ejecución puede ser subjetivamente completa y objetivamente incompleta o imperfecta, en cuyo caso se habla de delito frustrado, o bien subjetiva y objetivamente incompleta o imperfecta, en el que se habla de delito tentado, tentativa o conato.

Carrara, citado por Pavón Vasconcelos, distinguió brillantemente, entre delito perfecto y delito imperfecto. “En el primero la violación al derecho tutelado se consuma, mientras en el segundo no llega a realizarse a pesar de la voluntad proyectada a ese fin a través de actos apropiados. El delito queda imperfecto, explica Carrara, cuando imperfecta ha quedado la acción al interrumpir el curso de

sus momentos físicos, o porque éste ha sido insuficientemente promovido, o cuando aun siendo perfecta la acción, en todo lo necesario a alcanzar el fin propuesto y por ello suficientes los momentos precisos para la finalidad, el efecto no ha sido logrado debido a un impedimento imprevisto; en el primer caso surge el conato, en tanto en el segundo puede tenerse, en ciertas condiciones, el delito frustrado."[169]

La mayoría de los tratadistas siguen la clasificación bipartita que se compone de tentativa-delito y consumado, distinguiéndose la tentativa entre acabada o inacabada, esto es, la tentativa punible.

La tentativa acabada, es aquella en la que el sujeto realiza todos los últimos pasos que consumarían el delito.

La tentativa inacabada, es aquella en la que el sujeto deja de realizar el último o los últimos pasos que consumarían el delito, pero por causas ajenas a su voluntad.

La tentativa se encuentra estipulada en el artículo 20 y 21 del Nuevo Código Penal para el Distrito Federal:

ARTÍCULO 20 (Tentativa punible). Existe tentativa punible, cuando la resolución de cometer un delito se exterioriza realizando, en parte o totalmente, los actos ejecutivos que deberían producir el resultado, u omitiendo los que deberían evitarlo, si por causas ajenas a la voluntad del sujeto activo no se llega a la consumación, pero se pone en peligro el bien jurídico tutelado.

ARTÍCULO 21 (Desistimiento y arrepentimiento). Si el sujeto desiste espontáneamente de la ejecución o impide la consumación del delito, no se le impondrá pena o medida de seguridad alguna por lo que a éste se refiere, a no ser que los actos ejecutados constituyan por sí mismos algún delito diferente, en cuyo caso se le impondrá la pena o medida señalada para éste.

[169] Carrara, citado por Pavón Vasconcelos, ***Op. cit.***, Pág. 503.

En los casos de tentativa en que no fuere posible determinar el daño que se pretendió causar, cuando éste fuera determinante para la correcta adecuación típica, se aplicará hasta la mitad de la sanción señalada en el párrafo anterior. Las formas negativas de la tentativa son el arrepentimiento y el desistimiento.

a) El desistimiento.

El desistimiento es la interrupción de la actividad ejecutiva realizada por el autor, como expresión de su libre voluntad el designio criminal propuesto e iniciado.

La tentativa punible requiere, como requisito *sine qua non*, la inconsumación del delito por causas ajenas a la voluntad del autor. No serán punibles, dentro de la redacción del precepto, aquellas tentativas en las cuales el resultado no se produce en virtud del propio desistimiento, o cuando por la actividad voluntaria del autor, a tal fin, se impide la consumación del delito a pesar de haberse realizado todos los actos de ejecución. Así, el desistimiento voluntario se constituye como una causa de atipicidad de la tentativa.

b) El arrepentimiento.

El arrepentimiento eficaz es la actividad voluntaria, realizada por el autor, para impedir la consumación del delito, una vez agotado el proceso ejecutivo capaz, por sí mismo, de lograr dicho resultado.

El arrepentimiento supone, la realización previa de todos los actos de ejecución necesarios para producir el resultado, elemento al cual viene a sumarse la actividad de carácter voluntario practicada por el sujeto para interrumpir el proceso causal puesto en movimiento e impedir así la consumación del delito. El arrepentimiento puede ser diseccionado en cuatro elementos esenciales que lo integran:

a) Una voluntad inicial de causación del resultado
b) Realización de todos los actos de ejecución

c) Una actividad eficaz voluntaria para impedir el resultado

d) No verificación de dicho resultado

En nuestro caso, consideramos que pudiera presentarse un caso de tentativa acabada en el tipo penal que se analiza, cuando el sujeto activo, tiene un equipo informático, accesa al sistema o programa informático de un banco, por ejemplo, en el que logra accesar, sin embargo, al teclear “enter” para completar la transferencia, no consuma el delito debido a que se cae el sistema en ese momento o existen fallas en el sistema informático del banco.

En cuanto a la tentativa inacabada, si bien es cierto que pudiera darse el caso de que el agente realizara en parte los actos necesarios para el resultado previsto, y no consumarse la conducta establecida en el tipo penal que se analiza, por una causa ajena a su voluntad, sin embargo, es más difícil detectar este tipo de conductas, porque no se dejan rastro, convirtiéndose en una tentativa no punible.

4.5. Concurso de delitos.

Este se da cuando concurren dos o más delitos. El concurso puede ser real o ideal.

a) El concurso real.- También llamado material, se presenta cuando, con diversos actos se producen diversos delitos. Para este caso se impondrá la suma de las penas de los delitos cometidos, si tales son de diversa especie. Si son de la misma especie, se aplicarán la pena correspondiente al delito que se merezca la mayor, la cual podrá aumentarse hasta en una mitad más, sin que exceda de los máximos señalados en el Código Penal.

El concurso real o material se presenta cuando una persona con varios comportamientos realiza diversidad de delitos. Sobre el particular el artículo 18 del Código Penal dice existe concurso real, cuando con pluralidad de conductas se cometen varios delitos.

b) Concurso Ideal.- Denominado formal, ocurre cuando con una sola conducta (acción u omisión) se producen varios resultados. En tal situación se aplicará la pena correspondiente al delito que merezca la mayor, la cual se podrá aumentar hasta en una mitad más del máximo de duración, sin que pueda exceder en la actualidad de cincuenta años.

El concurso ideal, se presenta cuando con un comportamiento se realizan varios ilícitos de índole penal. El artículo 20 del Código Penal establece lo siguiente:

ARTÍCULO 28 (Concurso ideal y real de delito). Hay concurso ideal, cuando con una sola acción o una sola omisión se cometen varios delitos.

Hay concurso real, cuando con pluralidad de acciones u omisiones se cometen varios delitos. No hay concurso cuando las conductas constituyan un delito continuado.

En caso de concurso de delitos se estará a lo dispuesto en el artículo 79 de este Código.

El concurso ideal sólo puede tener cabida respecto a delitos de resultado material en donde con una misma acción o una misma omisión ocasiona diversos resultados materiales delictivos.

En el delito que se analiza, puede presentarse el concurso real, ya que con una pluralidad de conductas, se cometen varios delitos de la misma índole, se da ese apoderamiento del dinero o de los valores, cuando el sujeto accesa a los sistemas o programas de cómputo del sistema financiero, para obtener un beneficio para si o para un tercero, y al otro día realice lo mismo, pero en diferentes programas de informática del sistema financiero.

A lo largo del presente trabajo, hemos mencionado que la aparición de los delitos informáticos circula a una velocidad mayor que la de las legislaciones en el campo preventivo y sobre todo punitivo. El avance de esta ciencia informática, ha

creado una red de computadoras donde individuos y empresas publican información, venden productos y servicios y realizan un sin número de actividades, pero debido al libre acceso y la apertura de la red puede conducir a situaciones donde se intente delinquir.

Las computadoras o los sistemas informáticos no actúan por su cuenta, sino que siguen las órdenes con las que fueron programadas, por lo tanto resulta equívoco pensar que puede engañársele o aprovecharse del error de una computadora, para introducirse ilícitamente a un sistema o programa informático del sistema financiero, para realizar indebidamente operaciones, transferencias o movimientos de dinero o valores, como lo han establecido nuestros legisladores en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal.

De lo antes señalado y de acuerdo a la definición de delito de fraude, nos queda claro que el supuesto que marca la fracción XIV del artículo 231, es un delito de robo que se da por un medio electrónico, siendo su conducta típica el acceso ilícito a los sistemas o programas informáticos del sistema financiero para realizar operaciones, transferencias o movimientos de dinero o valores, por lo tanto nuestra propuesta es el de ubicarlo en el capítulo correspondiente a robo, que se encuentra en el mismo Título Décimo Quinto de los Delitos contra el Patrimonio.

Lo cierto es que los sistemas informáticos están reemplazando al hombre y lo suplantan en ese control de seguridad que antes realizaban los humanos. Las intromisiones informáticas son cada vez más frecuentes, siendo esto una violación a la privacidad.

PROPUESTA

Considerando que a lo largo del presente trabajo, hemos tratado el tema de los delitos informáticos, en los que la computadora es el medio para cometer este tipo de ilícitos, sin embargo, hemos visto que nuestro país cuenta con muy poca legislación al respecto; pero principalmente, abordamos la problemática que presenta el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal.

De lo establecido en este artículo, considero que no se trata de un delito de fraude, en primer lugar porque no se da un engaño ni mucho menos se induce al error a un sistema o programa informático, para tener acceso a él, se deben de introducir claves o contraseñas válidas para que el sistema permita el acceso. En segundo lugar, al accesar de manera ilícita a los sistemas o programas de informática del sistema financiero e indebidamente se realicen operaciones, transferencias o movimientos de dinero independientemente de que los recursos no salgan de la institución, es suficiente para considerar que surte el delito de robo, por el hecho de que se realiza un apoderamiento mediante una transferencia de fondos a favor de persona distinta a la institución bancaria afectada, utilizando el sistema de cómputo sin el consentimiento de la persona autorizada.

Por lo que considero que hay una errónea ubicación del tipo penal que contempla el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal y en ese tenor de ideas se propone en el presente trabajo, que el legislador integre debidamente este delito, al Código Penal Federal en el capítulo referente a Robo, por tratarse de una conducta que afecta al sistema financiero y por lo tanto, es incompetente la Asamblea Legislativa del Distrito Federal para crear leyes que se refieran al sistema financiero mexicano, además por las razones antes expuestas.

Por lo tanto, cometerá delito de robo electrónico, aquél que por cualquier medio accese, a los sistemas o programas de informática del sistema financiero e

indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

Y toda vez que los delitos relacionados con los sistemas informáticos representan una amenaza para la economía y seguridad del país, aunado a ello la falta de una legislación acorde a esta problemática, se propone que el legislador integre o elabore un título especial dentro del Código Penal, en el que considere a los delitos informáticos, en el que las medidas de seguridad que se implanten, deban ser acordes a las necesidades del sistema informático de que se trate, sea empresas, gobierno, etcétera.

Por ello, puede señalarse que los delitos informáticos, constituyen un reto considerable tanto para los legisladores como para las autoridades encargadas de la procuración y administración de justicia.

Por lo tanto se propone lo siguiente:

1. Derogación de la fracción XIV del artículo 231, del Nuevo Código Penal para el Distrito Federal.

2. Establecimiento del tipo penal dentro del Código Penal Federal, en el que establezca:

   Comete delito de robo electrónico: aquél que por cualquier medio accese, a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

3. La sanción se aplicará en proporción al daño causado al bien jurídico tutelado.

CONCLUSIONES

Primera.- Las nuevas tecnologías de la informática, nunca hubiesen existido de no ser posible por el desarrollo de las computadoras. Los equipos de informática, han abierto una nueva era y han permitido mejorar los sistemas de comunicación, convirtiéndose la computadora.

Segunda.- El Derecho, no escapa a la influencia de las nuevas tecnologías, ya que la informática resalta como uno de los campos que encuentra mayor aplicación en el quehacer cotidiano del hombre, jugando un papel preponderante ya sea porque se utiliza como medio para delinquir o porque ella es el objeto del delito, por lo tanto, el Derecho debe reaccionar intentando respuestas normativas que atienden a las causas de estas situaciones previniendo y reprimiendo las conductas delictivas que involucra el empleo de la computadora.

Tercera.- Es indudable que así como la computadora se presenta como una herramienta muy favorable a la sociedad, también se puede constituir en un instrumento u objeto en la comisión de actos ilícitos. Este tipo de actitudes concebidas por el hombre y no por las máquinas como algunos pudieran suponer, encuadra sus orígenes desde el surgimiento de la tecnología informática. La facilitación las labores que se realizan a través de ella, traen consigo que en un momento dado, el usuario se encuentre ante una situación de ocio, cometiendo una serie de ilícitos y debido a la magnitud de los valores e intereses en juego, se exige la necesidad de definir los nuevos delitos informáticos, para evitar una desprotección de la sociedad frente a los avances tecnológicos

Cuarta.- Los delitos informáticos son aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, valiéndose para su realización de las computadoras como medio para la comisión de éstas conductas. Este tipo de ilícitos, han pasado de ser formas tradicionales a formas no tradicionales por el uso indebido de la computadora, lo que ha propiciado la necesidad de regulación por parte del derecho.

Quinta.- Los delitos informáticos, han alcanzado un alto índice delictivo, toda vez que la falta de tipificación de los mismos permite a los delincuentes realizarlos con toda impunidad, que van más allá de una violación a los derechos patrimoniales de las víctimas, debido a las diferentes formas de comisión de estos.

Sexta.- La falta de preparación de nuestras autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de los sujetos pasivos de denunciar este tipo de ilícitos y las consecuentes pérdidas económicas entre otros aspectos más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada cifra negra.

Séptima.- Los ataques informáticos son transnacionales por su propia naturaleza y requieren de una cooperación internacional. La uniformidad de las legislaciones mejorará esta cooperación y garantizará que se cumpla la exigencia de doble incriminación. Por ello, que surge la necesidad de adoptar medidas legislativas a nivel nacional e internacional, acorde al avance tecnológico para enfrentar la problemática de los delitos informáticos.

Octava.- En el contexto nacional se han dado algunos avances legislativos en materia de delitos informáticos; sin embargo, el tratamiento de estos delitos es muy precario en México, en los Estado de Aguascalientes, Baja California, Chiapas, Colima, Distrito Federal, Morelos, Oaxaca, Puebla, Sinaloa, Querétaro, Tabasco, Tamaulipas, Zacatecas y en el Código Penal Federal, se tipifican las conductas ilícitas derivadas del uso de los sistemas informáticos. Es por ello, que cada vez más existe la necesidad de legislar en materia de delitos informáticos en México, la expansión y la considerable demanda entre la población mundial de las computadoras, dan como resultado un constante incremento de delincuentes con habilidad en materia informática.

Novena.- El artículo 231 fracción XIV del nuevo Código Penal para el Distrito Federal es una conducta equiparable a fraude, al ubicarla el legislador inmediatamente después del tipo penal de fraude, lo que consideramos un primer

yerro legislativo, la conducta consiste en accesar ilícitamente a los sistemas o programas de informática del sistema financiero e indebidamente realizar operaciones, transferencias o movimientos de dinero.

Décima.- El delito contemplado en el artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal, es un delito de acción, de resultado material que causa un daño al bien jurídicamente tutelado, instantáneo, doloso y se persigue de querella.

Décima Primera.- En el artículo 231 fracción XIV, no se realiza por medio del engaño ni por el aprovechamiento del error de alguien, las computadoras por su propia naturaleza no son susceptibles de caer en errores o falsas concepciones de la realidad, como sucede con las personas físicas.

Décima Segunda.- Para engañar a alguien se requiere la posibilidad de caer o no en ese engaño, tener la capacidad para reconocer el error, lo que de ninguna manera acontece con los sistemas computacionales, de tal modo que es imposible que los elementos que conforman la estructura del fraude: error, falsa representación, engaño, motivación, voluntad, decisión, disposición, puedan actualizarse en un sistema carente de las condiciones psicológicas correspondientes, como lo es la de la computadora.

Décima Tercera.- A una computadora no se le puede engañar, ésta funciona bajo instrucciones o comandos que le son dadas por una persona, y con las que fueron programadas, por lo tanto una computadora depende en su totalidad de las instrucciones que le son dadas, mismas que no pueden ser erróneas o falsas, sólo deben introducirse datos que son válidos para el sistema, por lo tanto resulta equívoco el ubicamiento que el legislador ha dado al artículo 231 fracción XIV del Nuevo Código Penal, ya que no se puede engañar ni aprovecharse del error de una máquina para introducirse ilícitamente a un sistema o programa informático del sistema financiero y realizar indebidamente operaciones, transferencias o movimientos de dinero o valores.

Décima Cuarta.- El acceso ilícito a un sistema informático para realizar indebidamente operaciones, transferencias o movimientos de dinero o valores (acto de disposición) del sistema financiero, no es un delito equiparable a fraude, se trata de un delito de robo electrónico, en el que se utiliza a la computadora como herramienta o medio de comisión, para llevar a cabo esa conducta ilícita.

Décima Quinta.- Se propone en el presente trabajo, la reforma al artículo 231 fracción XIV del Nuevo Código Penal para el Distrito Federal de la siguiente manera: la derogación de la fracción XIV del artículo 231 del Nuevo Código Penal para el Distrito Federal, establecimiento del tipo penal dentro del Código Penal Federal en el capítulo referente a Robo, por tratarse de una conducta que afecta al sistema financiero, por lo tanto, cometerá delito de robo electrónico: aquél que por cualquier medio accese, a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución. La sanción se aplicará en proporción al daño causado al bien jurídico tutelado.

Y toda vez que los delitos relacionados con los sistemas informáticos representan una amenaza para la economía y seguridad del país, aunado a ello la falta de una legislación acorde a esta problemática, se propone que el legislador integre o elabore un título especial dentro del Código Penal, en el que considere a los delitos informáticos y en ese tenor las medidas de seguridad que se implanten, deban ser acordes a las necesidades del sistema informático de que se trate, sea empresa, gobierno, etcétera.

BIBLIOGRAFÍA

1.-Arechiga Gallegos, Jorge, y otros, ***Fundamentos de la Computación***, 2ª Edición, Editorial Limusa, México, 1978, pp.391.

2.-Breekman, George, ***Computación e Informática hoy*****,** Una mirada a la tecnología de mañana**,** (Traducción de Ernesto Morales Peake), Editorial Addison-Wesley Iberoamericana S.A., México 1995, pp.372.

3.-Cámpoli Andrés, Gabriel, ***Derecho Penal Informático en México***, Instituto Nacional de Ciencias Penales, México, 2004, pp. 116.

4.-Carrancá y Trujillo, Raúl, ***Derecho Penal Mexicano***, *Parte General*, 21ª Edición, Porrúa, México, 1988, pp.986.

5.-Castellanos Tena, Fernando, ***Lineamientos elementales del Derecho Penal,*** 45ª Edición, Porrúa, México, 2004, pp. 363.

6.-Coello Coello, Carlos A., ***Breve historia de la computación y sus pioneros,*** Editorial, Fondo de Cultura Económica, México, 2003, pp.358.

7.-Colín Sánchez, Guillermo, ***Derecho Mexicano de Procedimientos Penales***, 18ª Edición, Porrúa, México, 2001, pp. 787.

8.-Correa, Carlos, ***Derecho Informático***, Ediciones Depalma, Buenos Aires, Argentina, 1987, pp. 341.

9.-Couffgal, Louis, ***La Cibernética,*** 4ª Edición, Industrias Gráficas, Barcelona, 1989, pp.149.

10.-Cuello Calón, Eugenio, ***Derecho Penal***, Tomo I, Parte General, Volumen II, 18ª Edición, Editorial Bosch, Casa Editorial, S.A. Barcelona, 1981, pp. 958.

11.-Davara Rodríguez, Miguel Ángel, ***Derecho Informático***, 2ª Edición, Editorial Aranzadi, Pamplona, España, 1993, pp. 413.

12.-Fix Fierro, Héctor, ***Informática y Documentación Jurídica,*** 2ª Edición, Instituto de Investigaciones Jurídicas, UNAM, México, 1996, pp. 116.

13.-Freedman, Alan, ***Glosario de Computación*****,** 3ª Edición, Editorial, Mc Graw Hill, (Traducción de María de Lourdes Fournier García) México, 1985, pp. 396.

14.-Jiménez de Asúa Luis, ***Lecciones de Derecho Penal,*** Editorial Pedagógica Iberoamericana, México 1995, pp. 367.

15.- ----------***Teoría del Delito,*** Editorial Iure Editores, México 2003, pp. 711.

16.-Jiménez Huerta, Mariano, ***Derecho Penal Mexicano***, Tomo I, 6ª Edición, Porrúa, México, 2000, pp.514.

17.-June Jamrich Parsons y Dan Oja, ***Conceptos de Computación*****,** 6ª Edición, Editorial Thomson, (Traducción Eloy Pineda), México, 2004, pp. 728.

18.-Leal Güemez Regina y otros, ***Fundamentos de computación,*** Editorial Trillas, México, 2000, pp. 291.

19.-Levine Gutiérrez, Guillermo, ***Introducción a la Computación***, 2ª Edición, Editorial, Mc. Graw Hill, México, 1997, pp. 424.

20.-Long Larry, ***Introducción a las computadoras y al procesamiento de información***, 2ª Edición, Editorial Hispanoamericana, México, 1990.

21.-Luño, Antonio-Enrique, ***Ensayos de Informática Jurídica***, Fontamara. México, 1996, pp.159.

22.-Maggiore, Giuseppe, ***Derecho Penal,*** Vol. I, 2ª reimpresión de la 2ª Edición, Editorial Temis, Bogotá, Colombia, 2000.

23.-Malo Camacho, Gustavo, ***Derecho Penal Mexicano,*** 2ª Edición, Porrúa, México, 1998, pp.714.

24.-Mezger, Edmund, ***Derecho Penal***, *Parte General*, 2ª Edición, Cárdenas Editor y Distribuidor, México, 1990, pp.461.

25.-Mir Puig, Santiago, ***El Nuevo Derecho Penal Informático en Alemania***, ***Delincuencia Informática,*** Editorial Promociones y Publicaciones Universitarias, Barcelona, 1992.

26.-Molina Salgado, Jesús Antonio, ***Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial,*** Colección: Breviarios Jurídicos, Porrúa, México, 2003, pp.107.

27.-Nava Garcés, Alberto Enrique, ***Análisis de los Delitos Informáticos,*** Tesis para obtener el grado de Maestro en Derecho en la Universidad Nacional Autónoma de México, Ciudad Universitaria, 2004, pp. 335.

28.- ----------, ***Análisis de los Delitos Informáticos,*** Porrúa, México, 2005, pp. 119.

29.-Orts Berenguer, Enrique y Margarita Roig Torres, ***Delitos informáticos y delitos comunes cometidos a través de la informática,*** Tirant lo Blanch, "Colección los Delitos," Valencia, España, 2001, pp. 195.

30.-Palazzi Pablo Andrés, ***Delitos Informáticos,*** Editorial Ad Hoc, Buenos Aires, Argentina, 2000, pp.272.

31.-Pavón Vasconcelos, Francisco, ***Imputabilidad e Inimputabilidad***, 4ª Edición, Porrúa, México, 2000, pp.137.

32.- ----------, ***Derecho Penal Mexicano,*** 13ª Edición, Porrúa, México, 1994, pp. 652.

33.-Pérez Luño, Antonio-Enrique, ***Ensayos de Informática Jurídica***, Fontamara. México, 1996, pp.159.

34.-Porte Petit Candaudap, Celestino, ***Apuntamientos de la parte general del Derecho Penal,*** 18ª Edición, Porrúa, México, 1999, pp.508.

35.-Prieto Espinosa Alberto y otros, ***Introducción a la informática***, 3ª Edición, Editorial Mc. Graw Hill, España, 2002, pp.676.

36.-Ríos Estavillo, Juan José, ***Derecho e Informática en México,"*** Instituto de Investigaciones Jurídicas UNAM, México, 1997, pp.175.

27.-Rovira del Canto, Enrique, ***Delincuencia informática y fraudes informáticos***, Editorial, Comares, Granada, España, 2002, pp.693.

38.-Téllez Valdés, Julio, ***Derecho Informático*****,** 3ª Edición, Editorial Mc Graw Hill, México, 2004, pp.514.

39.-Vasconcelos Santillán, Jorge, y otros, ***Estampas de la Ciencia***, Editorial Fondo de Cultura Económica, México, 1999, pp.245.

40.- ----------, ***Introducción a la Computación***, 2ª Edición, Editorial Grupo Patria Cultural, México, 2002, pp.338.

41.- ----------, ***Introducción a la Computación, Parte II***, Editorial Grupo Patria Cultural, México, 1999, pp. 330.

42.- ----------, ***Informática I***, ***Computación Básica***, Editorial Grupo Patria Cultural, S.A. de C.V., México, 2002, pp.138.

43.- ----------, ***Informática II, Sistemas de información,*** Editorial Publicaciones Cultural, México, 2002, pp.151.

44.-Villalobos, Ignacio, ***Derecho Penal Mexicano***, *Parte General*, 5ª Edición, Porrúa, México, 1990, pp. 654.

45.-Zaffaroni, Eugenio Raúl, ***Manual de Derecho Penal***, Parte General, 4ª reimpresión de la 4ª Edición, Cárdenas Editor y Distribuidor, México, 1998, pp.857.

HEMEROGRAFÍA

1.-Fernández, Maricel, ***Delitos Informáticos***, La Revista La Ley, Año LXVI, Número 23, Buenos Aires Argentina, Febrero 2002.

2.-Fuentes, Víctor, ***"Revocan reforma sobre fraude cibernético,"*** en el Diario Reforma, México, 17 de junio de 2003.

3.-Herrera Bravo, Rodolfo, ***Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley Chilena 19.223***, ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998.

4.-Lima Malvado, María de la Luz, ***Delitos Electrónicos***, en Criminalia, México, Academia Mexicana de Ciencias Penales, Porrúa, No. 1-6. Año L, Enero-Junio 1984.

5.-Palazuelos, Silvia Guadalupe, ***Delitos informáticos, Propuesta para el Tratamiento de la Problemática en México,*** Aequitas, Revista Jurídica del Poder Judicial del estado de Sinaloa, Segunda Época, Número 32, México, 1999.

6.-Ramírez Acosta, Carlos, ***Delitos informáticos***, La Revista de la Seguridad, Año 5, Volumen 4, Número 42, Sistema Ópalo, México, 2002.

7.-Sánchez Franco, Alfredo, ***Delitos informáticos***, Derecho Penal, Constitución y Derechos por la Universidad Autónoma de Barcelona, España (U.A.B.), México, 2002-2003.

8.-Toniatti, Roberto, ***Libertad Informática y derecho a la protección de datos personales: principios de legislación comparada,*** Revista Vasca de administración Pública, Número29, Enero-Abril, 1991, España.

DICCIONARIOS Y ENCICLOPEDIAS.

1.- Diccionario Enciclopédico Salvat, 4ª. Edición, Salvat Editores, España, 1995.
Enciclopedia Científica, Editorial Larousse, México, 1997.

Gran Diccionario Enciclopédico Ilustrado, Selecciones del Reader's Digest, México, 1988.

LEGISLACIÓN

1.- Constitución Política de los Estados Unidos Mexicanos, Sista, México, 2004.

2.- Código de Procedimientos Penales para el Distrito Federal, Sista, México, 2004.

3.- Código Penal Federal, Sista, México, 2004.

4.- Constitución Española, Tercera edición, Editorial Aranzadi, S.A., España 2004.

5.- Nuevo Código Penal para el Distrito Federal, Sista, México, 2005.

FUENTES ELECTRÓNICAS

1.- Biblioteca de Consulta Microsoft Encarta, CD Rom, Microsoft Corporation, 2002.

2.- Código Penal para el Estado Libre y soberano de Sinaloa, CD Rom, Suprema Corte de Justicia de la Nación, México 2004.

3.- Diccionario de la Lengua Española, Real Academia Española, CD Rom, 2001.

4.- Jurisprudencia y Tesis aisladas IUS 2002, CD Rom, Suprema Corte de Justicia de la Nación, México 2002.

5.- Legislación Federal y del Distrito Federal, Compila X, CD Rom, Suprema Corte de Justicia de la Nación, México 2005.

6.- Legislación Penal, CD Rom, Suprema Corte de Justicia de la Nación, México 2004.

7.- Ley para el Tratamiento de Menores Infractores, para el Distrito Federal en Materia Común y para toda la República en Materia Federal, CD Rom, Suprema Corte de Justicia de la Nación, México 2004.

a) http://www.geocities.com

b) http://es.wikipedia.org

c) http://www.segu-info.com.argentina/

d)) http://www.ciencia-ficcion.com/glosario/c/ciberesp.htm

e) http://webworld.unesco.org/infoethics2000/forum.html

f) http://www.informaticamilenium.com.mx/sitioweb.htm/dinternet

g) http://www.iespana.es/iabot/ciencia/ definicion_virus.htm

h) http:/www.delitosinformaticos.com

i) http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm

j) http://www.portaley.com/delitos-informáticos/codigo-penal-esp-shtml

k) http://www.delitosinformaticos/legislación/argentina.htm

l) http://www.ssp.gob.mx