UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANÍSTICAS

Carrera: Abogacía

TESIS DE GRADO

TEMA:

"El FRAUDE INFORMÁTICO: VALORACIONES TÉCNICO- JURÍDICAS"

Tesis Presentada Previo A La Obtención Del Titulo De Abogado De Los Tribunales Y Juzgados De La República

AUTORES:

PAMELA NATALLY GARZÓN TAPIA

MARCO FERNANDO VIZUETE GALLARDO

DIRECTORA DE TESIS:

ESP. LIYANIS SANTANA SANTANA

Latacunga – Ecuador

Noviembre - 2009

Declaración de autoría

Declaramos que somos los únicos autores de este trabajo y autorizo al Departamento de Derecho de la Facultad de Ciencias Sociales y Humanísticas de la Universidad Pinar del Río "Hermanos Saiz Montes de Oca" Cuba; y a la Carrera de Ciencias Administrativas, Humanísticas y del Hombre de la Universidad Técnica de Cotopaxi, Ecuador, para que hagan el uso que estimen pertinente del mismo.

Para que así conste firmo la presente a los _____ días del mes de _____ del año 2009.

_____	_____
Autor	**Autor**
Pamela Natally Garzón Tapia	**Marco Fernando Vizuete Gallardo**

AGRADECIMIENTOS

Nuestros agradecimientos van dirigidos a Dios por que nos ha permitido llegar al lugar donde nos encontramos, siendo nuestra guía y protector, el mismo quien con su infinito amor nos da sabiduría para cumplir con las metas que nos hemos trazado.

Agradecemos de manera muy especial a la Universidad Técnica de Cotopaxi prestigiosa Institución que nos acogió para formarnos como profesionales del derecho, así como a los docentes que conforman la misma, que con sus amplios conocimientos supieron encaminarnos en el desarrollo de nuestra profesión.

También agradecemos a la Universidad Pinar Del Rio "Hermanos Saiz Montes de Oca" de la República de Cuba digna institución que nos acogió para la realización de la Tesis de Diploma en la carrera de Abogacía, de manera especial a los docentes que en el transcurso de estos meses nos brindaron amistad, ayuda, conocimientos los mismos que nos apoyaron para la culminación de la misma.

Así mismo queremos extenderle nuestros más sinceros agradecimientos a la Esp. Liyanis Santana Santana en calidad de tutora quien con sus amplios conocimientos, carisma y amistad fue el pilar fundamental para el desarrollo de nuestra tesis.

DEDICATORIA

El presente trabajo de diploma que ha sido realizado con mucho esfuerzo, constancia, y dedicación queremos dedicarlo de manera especial:

A mis padres Elena y Rubén quien con su amor, sacrificio, me encaminaron para que pueda llegar a ser una profesional, enseñándome a ser perseverante para así alcanzar los objetivos que me he propuesto.

A mis hermanos Joel y Josué, quienes son mi apoyo incondicional.

A mi abuelita y a mi tía Elba quien es mi segunda madre quienes con su amor y apoyo me han ayudado para cumplir mis sueños.

A mi novio Marco la persona quien es mi apoyo, ayuda y esta siempre a mi lado dándome fuerzas.

A mi padre José Elías Vizuete, el mismo que con ejemplo, amor y rectitud supo guiar cada pasó que he dado en el transcurso de mi vida hasta llegar a ser un profesional, esforzándose por dar lo mejor de sí mismo.

A mis hermanos Telmo, Salomé, Sandra quienes de una u otra manera han contribuido para que pueda alcanzar el objetivo anhelado.

A mi novia y compañera de aula Pamela quien con su amor, ternura y paciencia me apoya desde el inicio de mi carrera.

ÍNDICE

Tabla De Contenidos **Página**

INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones están cambiando a la sociedad y al mundo, al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales y modificar la velocidad y el flujo de capitales. Este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática. La delincuencia informática es difícil de comprender o conceptualizar plenamente.

A menudo, se la considera una conducta condenada por la legislación que implica la utilización de tecnologías digitales en la comisión del delito; dirigiéndose a las propias tecnologías de la computación y las comunicaciones; al incluir la utilización incidental de computadoras en su comisión.

El delito informático tuvo su origen a finales de los años noventa, a medida que el Internet se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado “G8” con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por lo que migraron al Internet. El “Grupo de Lyón” utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones.

Con este avance vertiginoso de la computación, la informática y el uso de Internet, en la actualidad se cometen un sin número de delitos, llamados delitos informáticos, apareciendo el Fraude Informático como el más importante, ya que por medio de este se cometen desfalcos a entidades financieras en general, las cuales administran recursos propios y ajenos.

Tales conductas defraudatorias, abusos o interferencias en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención de obtener un provecho y causar un perjuicio económico, si no es debidamente controlado puede ocasionar serios problemas a la sociedad sin que se pueda sancionar a los responsables.

Este tema reviste de actualidad mundial y en el Ecuador su campo de acción es muy limitado debido a que es desconocido y su incursión en la legislación nacional es muy parca, y hasta desconocida, por casi la totalidad de las personas, cometiéndose en este sentido gran cantidad de agravios.

Estudiaremos, pues, en un primer momento, la delincuencia informática desde sus elementos técnico-doctrinales más generales, para comprender después la necesaria incorporación de la conducta típica conocida como fraude informático.

Para la presente investigación se han seguido las pautas metodológicas siguientes.

PROBLEMA DE INVESTIGACIÓN:

La inadecuada regulación del fraude informático dentro del ordenamiento jurídico ecuatoriano, que ocasiona daños patrimoniales a las personas naturales y jurídicas.

OBJETO DE INVESTIGACIÓN:

El fraude informático como expresión típica de la delincuencia informática.

OBJETIVOS:

OBJETIVO GENERAL

- Valorar la regulación del fraude informático en la legislación penal ecuatoriana.

OBJETIVOS ESPECÍFICOS

- Argumentar los presupuestos teóricos y doctrinales del delito informático.
- Argumentar la normativización idónea del fraude informático en Ecuador**.**

PREGUNTAS CIENTÍFICAS:

1. ¿Cuáles son los presupuestos teóricos y doctrinales del delito informático?
2. ¿Qué posición normativa asume Ecuador con relación a la regulación del fraude informático?

RESULTADOS ESPERADOS:

Lograr una material doctrinario y didáctico que sirva de soporte para el estudio del tema por parte de estudiantes, investigadores y operadores del Derecho.

A continuación analizaremos los métodos y procedimientos a utilizar.

MÉTODOS Y TÉCNICAS:

A continuación analizaremos los métodos y procedimientos a utilizar:

Método teórico jurídico: Con su utilización se explicó el tema propuesto soportando la estructura de la investigación, las categorías y conceptos que conforman el objeto de estudio seleccionado.

Método de análisis histórico: Este método se utilizó en la investigación para precisar cómo el Fraude Informático ha evolucionado desde su origen y cómo se va desarrollando e incrementado en proporcionalidad con el avance de la tecnología; así como para confrontar la legislación nacional y comparada con su evolución histórica.

Método jurídico comparado: Por medio de este método se pudo realizar un análisis comparativo de diferentes ordenamientos jurídicos en torno al fraude informático y así verificar el estado y la necesidad de modificar la regulación existente al respecto en Ecuador.

Técnicas: Para la realización del presente esfuerzo investigativo hemos utilizado la revisión de documentos como técnica fundamental, toda vez que hemos interactuado con materiales en diferentes soportes.

CAPÍTULO I: EL DELITO INFORMÁTICO: PRESUPUESTOS TEÓRICOS - DOCTRINALES

1.1 Concepto de delito informático.

La definición de delito ha estado determinada, en todas las fases del desarrollo de la sociedad, por el sistema de relaciones que en cada una de ellas ha predominado. En el devenir histórico de la humanidad, han sido disímiles las concepciones que sobre delito se han ofrecido, como la iusnaturalista en pleno siglo XX o la positivista en los finales del propio siglo.

En el presente, se ha sostenido la opinión desde un discurso materialista de aceptar al delito como fenómeno relacionado a la vida social, a las relaciones de los hombres y determinado por amenazar o atacar justamente esas relaciones sociales.

Sin dudas, son incontables las conductas que por su naturaleza constituyen delito, sin embargo nuestros esfuerzos investigativos se encaminan hacia la comprensión de la llamada delincuencia informática para la que son válidas las instituciones clásicas de la doctrina penal, pero en algunos casos es imprescindible revisar elementos o extremos de otros institutos.

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

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez, todas las ramas del saber humano se rinden ante los

progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios.

Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de

juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"

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

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

En la actualidad la informatización se ha implantado en casi todos los países: tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El delito informático cobra vida a partir del avance creciente de las Tecnologías de la Informática y las Comunicaciones (TIC) y el acceso e incorrecto uso de las mismas. Inicialmente, los países pretendieron encuadrar estas actividades

criminales dentro de figuras tradicionales reguladas convencionalmente en los ordenamientos penales, respectivo a cada uno de ellos. Sin embargo, la utilización de las TIC ha creado nuevas posibilidades de manejo indebido de las mismas, dando lugar a conductas delictivas que por sus particularidades no encuentran precedente dentro las regulaciones preexistentes y cuyas consecuencias llegan alcanzar altos niveles de nocividad que requieren una urgente regulación por parte del Derecho Penal.

Aunque no existe un consenso en la esfera internacional sobre la concepción de delito informático, el desarrollo doctrinal que sobre el mismo versa ha sido abundante. Las razones puede que sean diversas, mas a nuestro juicio, se concretan en que el tema brinda un estudio desde distintos ángulos y a partir de diferentes conductas ilícitas, cuyos modos de ejecución se perfeccionan a la par del desarrollo tecnológico.

Numerosos han sido los esfuerzos de estudiosos, que se han ocupado del tema, afanados por alcanzar una definición global de delito informático y aun cuando este objetivo no se ha materializado, se han formulado conceptos que van a responder a realidades nacionales concretas y que, en la generalidad de los casos, presenta un elemento común: la utilización de las técnicas informáticas en la obtención de un resultado. A pesar de los prolijos resultados con relación a la conceptualización, se siguen suscitando los más enconados debates.

El estudioso mexicano Julio Téllez Valdés**,** afirma que *"no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha*

sido objeto de tipificación aún" [1]. Para este autor se puede conceptualizar al delito informático en forma típica y atípica, la primera se integraría por "*las **conductas** típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y la segunda la conformarían las "***actitudes** ilícitas en que se tienen a las computadoras como instrumento o fin".*[2]

Nidia Callegari define al delito informático como "*aquel que se da con la ayuda de la informática* o de técnicas anexas"[3].

Para Carlos Sarzana, en su obra "*Criminalitá e tecnología*", los crímenes por computadora comprenden "*cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo"* [4]

María de la Luz Lima, denomina al delito informático como delito electrónico, plantea que el mismo "*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"*[5]*.*

---

[1] *Vid.* TELLEZ VALDÉS, JULIO, *Derecho Informático*, 2a. edición, Editorial Mc Graw Hill, México, 1996. P. 103

[2] *Ídem*

[3] *Vid.* CALLEGARI NIDIA, "Delitos informáticos y legislación" en *Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana*, No. 70 julio-agosto-septiembre. 1985, Medellín, Colombia, P.115.

[4] *Vid.* SARZANA, CARLOS, "Criminalità e tecnologia" en *Computers Crime. Rassagna Penitenziaria e Criminologia*. No. 1-2. Año 1. Enero-Febrero 1985, Roma, Italia. P.53.

[5] *Vid.* LIMA DE LA LUZ, MARÍA. "Delitos Electrónicos" en *Criminalista*, Academia Mexicana de Ciencias Penales, No. 1-6. Año L, Enero-Junio 1984, Ediciones Porrúa, México, P.100

De acuerdo con la definición elaborada por un grupo de expertos, el significado de delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

Rafael Fernández Calvo ve al delito informático como "*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la constitución española"*[6].

Otros autores tienden a hacer una distinción marcada entre delito computacional y delito informático viendo al primero como aquella conducta en que los medios informáticos, utilizados en su propia función, constituyen una nueva forma de atacar bienes jurídicos cuya protección ya ha sido reconocida por el Derecho Penal, el ejemplo más característico se puede ubicar en el delito de Hurto cometido mediante sistemas de transferencia electrónica de fondos, de la telemática en general o violación del empleo de claves secretas. Y al segundo, como aquel que afecta un nuevo interés social, un nuevo bien jurídico-penal que identifican como la información (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos).

[6] *Vid.* FERNÁNDEZ CALVO, RAFAEL, "El tratamiento de llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática)" en *Informática y Derecho*, P.1150, Disponible en: http://www.stj-sin.gob.mx/DelitosInformaticos2.htm,(mayo/ 2009)

Tomar partido con relación a la definición de delito informático, más que un mero afán técnico, significa en primer orden establecer si estos delitos son los que se cometen usando -o abusando- de las TIC, o los que atacan nuevos bienes muy específicos -u otros afines- o si por el contrario, comprenden ambos supuestos.

Ante estas tres posiciones, realmente consideramos que la que más análisis requiere, a la hora de definir qué entender por delito informático, es la que nos pone ante una disyuntiva: ¿son los delitos tradicionales cometidos mediante el uso de las tecnologías de la informática y la telemática verdaderos delitos informáticos o solo hay un cambio de instrumento en la comisión de los mismos?

El hecho de que acciones ilícitas tradicionales se realicen con el auxilio de medios informáticos, conlleva a reanalizar los elementos de la descripción legal del tipo penal, pues en mucho de los casos, la figura carecerá de aptitud suficiente para precisar, de forma total, todas las características que el uso de este nuevo instrumento le reporta al delito por ella previsto, dando lugar a la impunidad de algunos actos socialmente peligrosos. Además, tanto en los casos de delitos convencionales como en los que se ven lesionadas relevantes relaciones sociales, nacidas al calor de los avances tecnológicos, el hecho de estar, estrechamente ligados a los adelantos informáticos, va a dotarlos de un grupo de características comunes, distintivas del resto de los ilícitos. Por estas razones, somos partidarios del criterio de que un concepto adecuado de delito informático debe englobar ambas conductas.

Desde un principio, el concepto de delito se configura por medio de la sumatoria de los componentes de la estructura, obedeciendo a los particulares -y casi siempre no coincidentes- criterios que se sostienen en relación a los componentes de esta.

El método dialéctico reconoce al fenómeno delictivo como suceso de la vida social, compuesto por momentos subjetivos y objetivos de una conducta humana

específica que ataca o amenaza a relevantes relaciones sociales. En fin, se concibe al hecho delictuoso como un sistema de elementos relacionados entre sí, que cumplen una función y conforman una estructura compuesta por cuatro elementos que se complementan unos a otros: el sujeto del delito, el objeto del delito, la parte objetiva y la parte subjetiva.

El hecho de que acciones ilícitas tradicionales se realicen con el auxilio de medios informáticos, conlleva a reanalizar los elementos de la descripción legal del tipo penal, pues en mucho de los casos, la figura carecerá de aptitud suficiente para precisar, de forma total, todas las características que el uso de este nuevo instrumento le reporta al delito por ella previsto, dando lugar a la impunidad de algunos actos socialmente peligrosos.

Además, tanto en los casos de delitos convencionales como en los que se ven lesionadas relevantes relaciones sociales, nacidas al calor de los avances tecnológicos, el hecho de estar, estrechamente ligados a los adelantos informáticos, va a dotarlos de un grupo de características comunes, distintivas del resto de los ilícitos. Por estas razones, creemos que un concepto adecuado de delito informático debe englobar ambas conductas.

Definimos al delito informático como toda acción u omisión socialmente peligrosa y antijurídica directamente vinculada con el empleo de las Tecnología de la Informática y las Comunicaciones caracterizada por el uso indebido de sistemas informáticos, bien sea como medio o como objeto, para la comisión de un hecho delictivo, y susceptible de ser sancionada penalmente.

1.2 Características de los delitos informáticos

Los delitos informáticos pueden ser materializados de disímiles maneras, cada una de ellas con rasgos propios que permiten establecer parámetros de evaluación a la hora de ver su complejidad o nivel de peligrosidad.

Si variadas y encontradas son las posiciones con relación a la conceptualización, la sistematización de sus características no es menos debatida. Sin embargo, generalmente se presentan un grupo de características que distinguen a los mismos en su totalidad:

- Los sujetos activos de este tipo de delito se distinguen por tener ciertos conocimientos técnicos de informática, los que permiten su desenvolvimiento dentro de este campo y la dan la capacidad requerida para materializarlos.

- Se les reconoce como acciones ocupacionales, pues por lo general se realizan cuando el sujeto activo se haya laborando o de alguna manera tiende a vincularse con su ocupación.

- Frecuentemente son acciones de oportunidad donde el sujeto aprovecha ocasiones creadas o altamente intensificadas en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Brindan posibilidades de tiempo y espacio, pues en milésimas de segundo y sin una necesaria presencia física pueden llegar a ejecutarse.

- Son cuantiosos los casos y escasas las denuncias, y todo esto producto a la propia falta de regulación por parte del Derecho, además del desconocimiento de las víctimas de que han sido objeto de tales acciones.

- Muestran grandes dificultades a la hora de su comprobación, debido a su mismo carácter técnico, lo que atenta contra su punición.

- Tienden a proliferar cada vez más, a la par del avance de las tecnologías de la informática y las comunicaciones, por lo que requieren una urgente regulación ya que en la mayoría de los casos son ilícitos impunes.

1.3 Clasificación de los delitos informáticos

Podemos encontrar en la doctrina, legislaciones y pautas de organismos internacionales, diversos criterios clasificatorios de los delitos informáticos. Esta diversidad está dada por el hecho, anteriormente planteado, de que este naciente fenómeno abarca desde las figuras típicas, reconocidas tradicionalmente por las legislaciones, hasta nuevas posibilidades de conductas dañosas que no encuentran precedente en los ordenamientos ya existentes; es decir, no son recogidas convencionalmente. Revisar estos criterios es imprescindible si se desea una visión general de lo que muchos van adoptando como conductas antijurídicas en la esfera de la informática y las comunicaciones.

1.3.1 Tipos de delitos informáticos reconocidos por la Organización de Naciones Unidas (ONU)

La ONU distingue tres tipologías de delito informático, las que han sido aceptadas por la mayoría de la doctrina especializada, estas son:

- *Fraudes*: conductas que consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas. Pueden ser realizados mediante manipulación de computadoras, la cual se subdivide en:

  - ✓ Fraudes cometidos mediante manipulación de datos de entrada
  - ✓ Manipulación de programas
  - ✓ Manipulación de datos de salida
  - ✓ Fraude efectuado por la manipulación de la información.

- *Falsificación:* La falsificación por medio de la informática se subclasifica en:

- ✓ Falsificaciones como medio
- ✓ Como instrumento.

- *Daños a Datos:* conductas consistentes en generar daños por medio de virus, gusanos, accesos no autorizados por hacker o cracker

A) Fraude informático

a) Fraudes cometidos mediante manipulación de computadoras:

- *Manipulación de los datos de entrada:* conocido también como sustracción de datos o manipulación del *input*, es el más común de los delitos informáticos ya que es fácil de cometer y difícil de descubrir. Este tipo de fraude no requiere de conocimientos técnicos de informática y es realizable por cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. Consiste en alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador.

- *La manipulación de programas*: es el denominado Caballo de Troya, consiste en interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales existentes en el sistema de computadoras, como al adicionar al sistema programas especiales que introduce el autor, es decir, 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.

A diferencia del anterior, este fraude es muy difícil de descubrir y a menudo pasa inadvertido debido a que esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

- *Manipulación de los datos de salida:* modalidad denominada también manipulación del *output,* es efectuada fijando un objetivo al funcionamiento del sistema informático. Una característica general de este tipo de fraude, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo, producto a que una vez que el autor descubre o crea una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces pretenda, la comisión del hecho. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito

b) Fraude efectuado por manipulación informática:

El autor lo ejecuta valiéndose de las repeticiones automáticas de los procesos del cómputo. Esta es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas apreciables, de transacciones financieras, se van sacando reiteradamente de una cuenta y se transfieren a otra.

B) Falsificaciones informáticas

Partiendo del uso de las nuevas tecnologías informáticas se logra alcanzar desde la ejecución del tradicional delito de falsificación de monedas, hasta la alteración de los propios datos contenidos en un ordenador, es por ello que la Organización

de Naciones Unida subdivide las falsificaciones por medio de la informática en falsificaciones informáticas:

- *Como objeto*: Cuando se alteran datos de los documentos almacenados en forma computarizada; y
- *Como instrumento:* Cuando se efectúan falsificaciones de documentos de uso comercial haciendo uso de las computadoras. Un ejemplo claro lo constituye la falsificación de documentos a través de fotocopiadoras computarizadas en color, basándose en rayos láser pues de ese modo se pueden hacer copias de alta resolución, modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos obtenidos a través de ellas poseen tanta calidad que sólo pueden ser diferenciados de los documentos auténticos por un experto. Con el surgimiento de estas fotocopiadoras se dio paso a una nueva generación de falsificaciones o alteraciones fraudulentas.

C) Daños o modificaciones de programas o datos computarizados

a) Sabotaje informático

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

- *Conductas dirigidas a causar daños físicos*

Este primer grupo comprende todo tipo de conductas consignadas a la destrucción «física» del *hardware* y el *software* de un sistema (por ejemplo: causar incendios o

explosiones, introducir piezas de aluminio dentro de la computadora para originar cortocircuitos, arrojar café o agentes cáusticos en los equipos, etc.).

En general, estas conductas pueden ser examinadas, desde el enfoque jurídico, en forma análoga a los comportamientos similares de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

- *Conductas dirigidas a causar daños lógicos*

Este segundo grupo, más propiamente relacionado con la técnica informática, se refiere a las conductas que motivan destrozos «lógicos», o sea, todas aquellas conductas que provocan, como resultado, la destrucción, ocultación, o alteración de datos comprendidos en un sistema informático.

Este tipo de daño a un sistema se puede agenciar de diversas formas. Desde la más simple que podemos suponer, como desconectar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complicados programas lógicos destructivos (*crash programs*), supremamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructores, emplean disímiles técnicas de sabotaje, muchas veces, en forma combinada, dentro de ellos podemos distinguir:

- *Virus:* son una serie de claves programáticas que se adhieren a los programas legítimos. Los virus pueden entrar a un sistema a través de una pieza legítima de soporte lógico que ha quedado infectada o utilizando el método del Caballo de Troya. Es un programa capaz de reproducirse por sí mismo e infectar los otros programas que se encuentran en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión. Constituye una variante

perfeccionada del cáncer de rutinas, técnica en la que los programas destructivos tienen la peculiaridad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos. Pueden ser insertados o propagados por otros programas malignos como los llamados *malware* y los *bots*.

- *Gusanos:* su producción ocurre de forma equivalente al virus con el objetivo de infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, se diferencia del virus en su incapacidad para regenerarse. Las consecuencias del ataque de un gusano pueden ser tan letales como las del ataque de un virus: por ejemplo, un programa gusano que inmediatamente se destruirá puede dar disposiciones a un sistema informático de un banco para que transfiera consecutivamente dinero a una cuenta ilícita.
- Bomba lógica o cronológica: En esta modalidad, la actividad destructiva del programa inicia tras un plazo, sea por el mero transcurso del tiempo, o por la aparición de determinada señal, que puede o no aparecer, como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar. Demanda conocimientos especializados. Al contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por lo que se considera que de todos los dispositivos informáticos criminales son las que ocasionan el superior daño. Puede ser programada para originar las mayores pérdidas posibles y su detonación puede ocurrir tiempo después de que se haya marchado el delincuente. También constituye un medio de extorsión puesto que a cambio de dar a conocer el lugar en donde se halla la bomba se piden valiosos rescates.

b) *El* acceso no autorizado a servicios y sistemas informáticos

Se da por múltiples motivos que van desde la simple curiosidad, como en el caso de muchos piratas informáticos (*hackers*) hasta el sabotaje o espionaje informático.

- *Piratería informática o hacking:* constituye fundamentalmente un acceso indebido o no autorizado a sistemas automatizados, puede hablarse de *hacking* propiamente dicho, cuando nos referimos a la acción de acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o *passwords,* esta contraseña se establece como medio de seguridad a un sistema o programa informático, limita su uso o acceso y su conocimiento es necesario para acceder de forma correcta al mismo, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

Y puede hablarse de *hacking* como medio de comisión de otros delitos o *hacking* indirecto cuando el acceso indebido, se efectúe como medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje. El comisor del delito de *hacking* es el *hacker*.

El *Hacker* en general utiliza reglas gramaticales particulares, juega y crea un lenguaje propio con la intención de confundir y diferenciarse, y con ello obtener cierto poder. Ese leguaje puede ser universal en el *hackerdown*, o ser de su propia autoría en un programa en particular.

Utiliza frases que literalmente significan una cosa y quieren decir otra, de este modo el operador creerá que está ejecutando una acción o programa, cuando en realidad ejecutará otra cosa; la esperada y programada por el *Hacker*.

Los *hackers*, son la última vanguardia de la delincuencia informática. Hacker es un término en inglés con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad: El delincuente silencioso o tecnológico.

Casi siempre el *hacker* o pirata informático accede desde un lugar exterior, situado dentro de la red de telecomunicaciones, haciendo uso de medios como:

- ✓ Aprovechamiento de la falta de rigidez de las medidas de seguridad para obtener acceso.
- ✓ Descubrimiento de deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

Con frecuencia, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c) Reproducción no autorizada de programas informáticos de protección legal:

Este daño puede llegar a inducir una pérdida económica sustancial para los propietarios legítimos.

En algunas jurisdicciones se ha tipificado como delito esta clase de actividad y se han impuesto sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

1.3.2 Clasificación de los delitos informático según el instrumento o fin

Dentro de las múltiples clasificaciones que se han hecho de delitos informáticos, las más claras son las que lo hacen sobre la base de dos criterios:

- Como instrumento o medio
- Como fin u objetivo

a) Como instrumento o medio: Se tienen a las conductas criminógenas que se valen de las computadoras como medio, o símbolo en la comisión del ilícito, por ejemplo:

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

b) *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 con el fin de provocar un daño, como por ejemplo:

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

- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

1.3.3 Otra clasificación de los delitos informáticos

Algunos especialistas de la materia han estimado clasificar los delitos de forma más desglosada, subdividiéndolos de esta manera:

- Clasificación según la actividad informática
- Clasificación según el instrumento, medio o fin u objetivo
- Clasificación según actividades delictivas graves

A) Clasificación según la actividad informática

Dentro de esta tipología encontramos algunas conductas como el sabotaje y el fraude informático explicados anteriormente y otras como la copia ilegal de *software* y espionaje informático, el uso ilegítimo de sistemas informáticos ajenos y los delitos informáticos contra la privacidad, a los cuales haremos breve referencia.

a) Copia ilegal de software y espionaje informático

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común la toma de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (*software*) que suele tener un importante valor económico.

- Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. Por tanto, las conductas que van a constituir infracciones de los derechos de autor a través de los sistemas computacionales van a estar determinadas por las posiciones que asuma cada país en relación a este tema.

- *Infracción del Copyright de bases de datos:* No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más frecuente es el contractual: el propietario del sistema consiente que los usuarios hagan copias de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información

b) Uso ilegítimo de sistemas informáticos ajenos

Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas son propias en empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades adicionales a su trabajo. En estos supuestos, sólo se ocasiona un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

- *Acceso no autorizado:* La corriente reguladora sostiene que el uso ilegítimo de *passwords* y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

c) Delitos informáticos contra la privacidad

Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

Esta tipificación se refiere a quién, sin estar acreditado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

Existen circunstancias agravantes de la divulgación de ficheros, los cuales se dan en función de:

- El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.
- Las circunstancias de la víctima: menor de edad o incapaz.

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

Interceptación de *e-mail*: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

B) *Clasificación según actividades delictivas graves*

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos como:

a) *Terrorismo:* La existencia de *hosts* que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.
b) *Narcotráfico:* Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
c) *espionaje informático:* Se incluyen las formas de acceso no autorizado a un sistema de tratamiento de la información. En él podemos encontrar el espionaje industrial: Se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y *know how* estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.
d) Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

De todos los criterios clasificatorios el más acertado es el de hacerlo según el instrumento o fin del delito informático.

1.4 SUJETOS DE DELITOS INFORMÁTICOS

1.4.1 Sujeto Activo.

Los sujetos activos en los delitos informáticos tienen como características:

a) Poseen importantes conocimientos de informática.

b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible; se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.

c) A pesar de las características anteriores se deben tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

e) Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico.

La "**cifra negra**" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes lo cometen y también es importante destacar que los daños económicos son altísimos. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los U$S 100 millones (Cámara de Comercio de los Estados Unidos) hasta la suma de U$S 5.000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora.

Pacheco Klein señala en un estudio realizado, se estimó que sólo el 1% de los robos de computadora son detectados, y quizá sólo un 15 % de ellos sean denunciados. Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; sólo alrededor del 24 % van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente.

Un punto muy importante es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario el autor de estos delitos distingue entre el daño a las personas (que es inmoral) y el daño a las organizaciones, porque en este último caso sienten que "hacen justicia", se le ha llamado a este punto de vista el síndrome de Robin Hood.

1.4.2 Sujeto Pasivo.

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

Al respecto no solamente por los motivos antes señalados los sujetos pasivos no denuncian estos delitos, sino también porque además de la falta de leyes que los protejan, la falta de preparación por parte de las autoridades (policiales y jurídicas) para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática, ha faltado mucha difusión, hay quienes a pesar de encontrarse muy relacionados con todo lo referente a los sistemas informáticos, no saben qué hacer cuando sufren algún menoscabo por algunas de estas conductas, no saben ante quien acudir y si realmente pueden ser resarcidos de los daños que sufrieron, es por ello que es importante darle una difusión por todos los medios pertinentes a la existencia de este tipo de delitos y alertar de esta manera a quienes son y han sido víctimas de éstos delitos. La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que, la difusión de la existencia de estos delitos puede ser un factor minimizante de los mismos.

1.5 BIEN JURÍDICO PROTEGIDO.

El bien jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás tiene que dejar de existir, ya que constituye la razón de ser del delito, y no suele estar señalado en los tipos penales.

1.5.1. Elementos que integran el concepto.

Objeto de protección.- Son aquellos bienes considerados esenciales para la convivencia pacífica en una comunidad dada. De esta manera, una acción es antijurídica cuando afecta a estos bienes jurídicos protegidos. De su parte el bien jurídico no es un bien del derecho, si no uno de los hombres, un interés vital, reconocido y protegido por el derecho.

El objeto jurídico de un delito está constituido por aquellos bienes públicos o intereses colectivos privados asumidos por el estado que, por ser precisamente tales, el derecho debe proteger. Concebido o entendido en virtud de una abstracción estamos pensando en "….el bien jurídico que al hecho punible pone en peligro o lesiona y que la ley penal ampara mediante la amenaza de una pena para quienes lo ataquen"[7].

Los ejemplos son clásicos: La vida, la integridad personal, la libertad, el honor, patrimonio, etc.

Sujeto en quién radica la protección jurídico-penal.- En principio se acuñó el concepto refiriéndolo concretamente a personas o cosas, lo que llevó a reconocer como bien jurídico sujeto a protección, a las representaciones morales de la sociedad.

[7] NOVOA MONREAL, Eduardo, "Curso de Derecho Penal", 1966, Universidad de Chile.

En tal sentido Hanssner, desarrolla el concepto de bien jurídico personal atendiendo al campo de tensión entre individuo, sociedad y estado; los bienes jurídicos son intereses humanos que requieren resguardo penal, por tanto la protección de las instituciones solo puede llegar hasta el punto en que es condición de la posibilidad de protección de la persona, límite en la elección de los objetos de protección penal. No obstante a lo anterior el concepto debe permitir la decisión discrecional del legislador penal. Una concepción personal no rechaza la posibilidad de bienes jurídicos generales o estatales, pero los funcionaliza, desde la persona: solo puede aceptarlos cuando brinden la posibilidad de servir a los intereses del hombre. Así en los delitos insertos en el derecho ambiental, el bien jurídico no es en sí el medio ambiente, si no en tanto para la salud y la vida del hombre.

Protección jurídico penal.- Es Binding, quien lo integra al arsenal conceptual del positivismo jurídico; lo concibe como voluntad legal que el legislador tuvo en vista al dictar la norma; y dice en forma concreta que cada norma tiene un bien jurídico protegido que se identifica con los motivos que se tuvo en vista al generarlos; sin embargo Hessener sostiene que una conducta que amenaza un bien jurídico es condición necesaria, más no suficiente para criminalizarla, pues han de considerarse además los principios de subsidiaridad, dañosidad social, tolerancia, humanidad, protección de la dignidad del hombre, los fundamentos del derecho penal del hecho y las leyes penales determinadas, que imponen al legislador penal unos límites estrechos y medios específicos.

1.5.2.- Los bienes jurídicos protegidos del Delito Informático.

Dentro de los delitos informáticos la tendencia es que la protección a los bines jurídicos, se lo haga desde el punto de vista de los delitos tradicionales, para subsanar las lagunas originadas de las novedosas formas de delinquir. Esto quiere decir que a los delitos se les ha agregado un nuevo elemento para de esta manera realizar su persecución y sanción por parte del órgano jurisdiccional competente.

Los bienes jurídicos protegidos en general son los siguientes:

- **El Patrimonio,** en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da lugar.
- **La Reserva, la Intimidad y Confidencialidad de los Datos,** en caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- **La Seguridad y Fiabilidad del Tráfico Jurídico y Probatorio,** en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- **El Derecho de Propiedad,** en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el denominado terrorismo informático.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan por que simultáneamente protegen varios intereses jurídicos, sin perjuicio de que tales están independientemente tutelados por otro tipo"[8]. En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

1.6 PENALIZACIÓN DE LA DELINCUENCIA INFORMÁTICA.

Elemento indispensable en la norma penal, es la pena que se le impone al responsable o responsables de la conducta ilícita, una vez que se haya verificado la existencia de ciertos elementos: La Tipicidad, antijuricidad, y culpabilidad, lo que da una conducta punible, merecedora de una pena.

[8] REYES ECHEANDÍA, Alfonso, "La Tipicidad", Universidad de Externado de Colombia, 1981.

En relación a los delitos Informáticos, aquellas legislaciones que cuentan con una protección penal frente a estos ilícitos, han previsto penas privativas de la libertad o penas pecuniarias o ambos simultáneamente.

Un aspecto importante que debe tomar en cuenta el legislador, al momento de incriminar un acto que pueda ser considerado como delito Informático, es el principio de la última alternativa del ordenamiento punitivo, es decir que la protección penal debe ser la última opción utilizada para el mantenimiento de la paz social.

Existen otros mecanismos y medidas de protección extra penal que pueden cumplir la misma finalidad, sin necesidad de restringir, ni vulnerar los derechos fundamentales, garantizados a la persona humana, como es el caso de las sanciones administrativas cuando establecen multas o revocatorias de permisos de funcionamiento o cesación para la explotación de ciertos bienes y servicios.

Así se ha procedido en algunos países que han incorporado normas destinadas a proteger la información, la propiedad intelectual, la intimidad, etc., en cuerpos legales no punitivos, como la ley de comercio electrónico, la ley de propiedad intelectual, entre otros, únicamente han establecido normas jurídicas de carácter penal para aquellas infracciones que vulneran gravemente los bines jurídicos antes referidos. Sin embargo; como se ha expresado anteriormente, las normas de carácter penal solo deben constar en el código de la materia y no en cuerpos legales paralelos que solo producen la dispersión de las normas punitivas en el ordenamiento jurídico de un estado.

Para determinar si una conducta ilícita será sancionada con la aplicación de una pena de mayor o menor gravedad, se debe considerar el grado de peligro del acto, las consecuencias que ha ocasionado o que puede haber ocasionado, las circunstancias que rodean al cometimiento del hecho ilícito, etc., este último con el objeto de establecer circunstancias agravantes o atenuantes de la infracción.

Así para precisar circunstancias agravantes se deberá considerar aspectos como:

- La índole o naturaleza de la información. Ej. Información privada que podría atentar contra la seguridad nacional de un estado.
- La presencia de engaño, abuso de confianza, perjuicio patrimonial al obtener la información.
- El uso de medios electrónicos para cometer el delito.

1.7 Consideraciones finales del capítulo

El fenómeno de la informatización, al igual que una moneda, nos ofrece dos caras. Una de ellas proporciona ventajas y beneficios a la humanidad, le ofrece un mundo de tecnología donde el almacenamiento, transmisión y acceso a la información es cada día más viable.

Sin embargo; la otra, lejos de ser favorable nos resulta peligrosa, pues nos brinda esa misma tecnología como progenitora de un engendro criminal que se ha dado a conocer como criminalidad informática. Ante este acontecimiento se hace inminente reflexionar sobre si las medidas jurídicas con las que consta el Estado en representación de la sociedad, son válidas para lograr que los delitos informáticos no constituyan un quebranto de los derechos y libertades de los ciudadanos o una “reestructuración contraproducente” del sistema político al que sirven de soporte.

Es esencial visualizar este fenómeno desde su esencia nociva y buscar, en soluciones globales, el antídoto al mal, cada vez más notorio y creciente, que la intrusión y mal uso de las nuevas tecnologías de la información han provocado en la sociedad.

En fin, se hace condición básica para la protección de variados derechos y libertades ciudadanas la pronta regulación del tráfico de la información en una estructura social en la que la posesión de información implica posesión de poder.

Frente a un eminente fenómeno nuevo el ordenamiento jurídico puede preferir entre una de estas dos actitudes: o bien regular jurídicamente antes de que los peligros que de tal fenómeno se derivan se materialicen, con el consiguiente riesgo de que dicha regulación peque de insuficiencia, precipitación o excesiva legislación de la materia; o bien, puede dar tiempo a que se produzca un desarrollo del fenómeno, para de esta forma evaluar y acrisolar mucho mejor la respuesta jurídica y evitar, por tanto, cualquier innecesaria y precipitada intervención legislativa que pudiera entorpecer el desarrollo social.

Primariamente, los peligros que el nuevo medio conlleva son identificables desde hace tiempo y algunos ya se han materializado en las sociedades que han alcanzado un cierto grado de desarrollo en relación con esta materia y en las que el acceso a las tecnologías se ha generalizado de manera sobresaliente.

No obstante, el hecho de que estas sociedades sean las más amenazadas no supone que sean las únicas pues las que ostentan niveles bajos de desarrollo tecnológico y reducido acceso de la población a él, también se ven amenazadas, aunque en menor escala, en las esferas de la economía donde la informática juega un papel primordial.

No faltan quienes toman como válido el referente del delito ecológico y han sido comparadas las consecuencias de esta evolución tecnológica con las consecuencias que para el medio ambiente ha tenido la evolución industrial, concluyendo que cuando el legislador ha pretendido controlar un proceso indiscutiblemente dañoso para la sociedad muchos de sus efectos ya eran definitivos. Es pues, ineludible la existencia de una regulación del tema que permita que este desarrollo se mueva dentro de unos límites claros y la propia

investigación en materia fundamentalmente de *software*, atienda no sólo a la obtención de los mayores beneficios posibles, sino que desde ya, sea consciente de que en dicha investigación han de tomarse en cuenta otros parámetros de importancia tan trascendente para la sociedad como el ya citado.

El avance tecnológico de la información debe examinar siempre más efectividad pero sin obviar el límite constituido por el respeto a los derechos y libertades de los ciudadanos y, en caso de disyuntiva, optar claramente por la preferencia de estos últimos: al encauzamiento en este sentido del proceso contribuirá decisivamente la existencia de una normativa legal.

El arsenal de medios de que en la actualidad disponen los diferentes ordenamientos jurídicos es axiomáticamente exiguo en relación con la problemática de la información en la sociedad, pues están encaminados a estructuras peculiarmente distintas frente a la que cabían reacciones individuales del tipo de las indemnizaciones de daños y perjuicios, insuficientes en la actualidad.

Es imperioso, pues, articular toda una serie de medidas jurídicas que coloquen nuevamente al ciudadano en el papel activo que le pertenece en el Estado de Derecho, medidas que han de dirigirse especialmente a esa nueva realidad que abarca todos los sectores de la estructura social para que los individuos no se vean convertidos en meros objetos de información, sino que sean sujetos que intervienen en los procesos que les afectan.

Los peligros que de una mala utilización de las nuevas tecnologías se derivan no son monopolio exclusivo del Estado, pues no debe olvidarse, que la fuerza de penetración de la informática en el sector privado es, en la mayoría de los subsectores igual, e incluso superior, a la que se da en el sector estatal. Por todo ello parece evidente la necesidad de una regulación global, lo que, por supuesto, no implica una regulación uniforme. Esta regulación ha de tener en cuenta

necesariamente las peculiaridades de los distintos sectores para, de esta forma, hacer frente a los específicos problemas que, de cada uno de ellos, se derivan.

El recurso al Derecho Penal y, por tanto, el carácter grave de las sanciones de que debe hacer uso el legislador, se halla justificado tanto por la clase de los bienes en juego en esta materia, ya que se trata de garantizar las condiciones necesarias para el ejercicio de la mayor parte de los derechos fundamentales y libertades públicas; como por el carácter, también especialmente grave, de estas formas de ataque a dichos bienes, ya que colocan al individuo en una situación de absoluta indefensión, pues la mayoría de las veces no llegará ni siquiera a conocer que ha sido lesionado en sus derechos, ni quien ocasionó los daños.

CAPITULO II EL FRAUDE INFORMÁTICO COMO FIGURA TÍPICA DEL DELITO INFORMÁTICO: CARACTERÍSTICAS Y ENTIDAD DE SU TIPOLOGÍA

"Con el avance de la tecnología, la informática se ha convertido en un instrumento que proporciona infinitas posibilidades de desarrollo y progreso. Sin embargo, se ha dado lugar a una nueva forma de delincuencia, la delincuencia informática; ya que esta tecnología pone a disposición del delincuente un abanico de nuevas técnicas y métodos para alcanzar sus propósitos criminales"[9]. Los autores chilenos Magliona y López, mencionan que el fraude informático es uno de los fenómenos más importantes dentro de la delincuencia informática, dado el creciente aumento de las manipulaciones fraudulentas, y es por tanto la zona más inexplorada y la que mayores problemas enfrente en cuanto a su prevención, detección y represión.

Con la incursión de la informática en el sistema financiero, se ha remplazado muchos de los documentos tradicionales en soporte papel en los que constan las operaciones y saldos de cada uno de los clientes, por anotaciones en cuenta, o registros lógicos realizados en los sistemas informáticos, sin un soporte en papel o con reflejos en papel meramente informativos o secundarios. De ahí que, la doctrina haya centrado el estudio del problema desde el enfoque de las manipulaciones de datos informativos.

Se ha sostenido que estas manipulaciones constituyen la forma más frecuente de comisión de delitos por medios informáticos: cuando se tuvo conocimiento de los primeros casos de fraude informático, estos fueron vinculados al delito de estafa. Así se trató de encajar esta nueva figura dentro de los moldes estrechos de dicho tipo clásico, lo que a la postre supuso una dificultad para su encuadre, ya que los mismos elementos que configuraban a la estafa no lo permitían. Es así como nacieron en la doctrina extranjera las discusiones a cerca de la imposibilidad de

[9] MAGLIONA H, Claudio Paúl, LÓPEZ MENDEL, Macarena, "Delincuencia y Fraude Informático, Editorial Jurídica de Chile, 1999.

engañar a una máquina, o de la existencia de un error psicológico por parte del computador que lo lleva a la disposición patrimonial lesiva.

Por tales razones y al verse el tipo penal de la estafa desbordado por los nuevos avances tecnológicos aplicados por los delincuentes, para efectuar sus defraudaciones, llevaron a que naciera un nuevo tipo delictivo, el fraude informático, que vendrá a absorber todas aquellas conductas defraudatorias que, por tener incorporada la informática como herramienta de comisión, no podían ser subsumidas en el tipo clásico de la estafa.

En nuestro país la vocación de tipo clásico de estafa, para incluir en su estructura constitutiva, los supuestos y conductas que entrañan al fraude informático, es prácticamente insuficiente, dado que su propia estructura constitutiva sería el obstáculo para que dichos supuestos y conductas pudieran ser subsumidos en dicho tipo clásico.

Esta vinculación con la estafa desde sus inicios determinó además que el concepto, estructura y contenido del fraude informático fueran construidos a partir de los elementos del delito de estafa.

2.1. Conceptualización Técnico - Jurídica del Fraude Informático.

Es la manipulación indebida de datos, tomando como medio un sistema de tratamiento de información, lo que da como resultado una adulteración o alteración de los datos contenidos en ese sistema, en cualquiera de las fases de su tratamiento, con o sin ánimo de lucro.

El fraude informático delito informático realizado con intención de engañar o perjudicar a una persona u organización y proporcionar un beneficio ilegítimo a quien lo realiza.

La mayor parte de la doctrina, especialmente europea, entiende que son precisamente estas manipulaciones al computador las que representan los mayores índices de delincuencia informática.

Es usual observar que los juristas extranjeros tratan como sinónimos a los términos manipulación y fraude informático. Queriendo decir con eso que se trata de ilícitos de carácter patrimonial, lo cual también se deriva de su creencia en los bienes jurídicos múltiples en los que se ampararían los Delitos Informáticos.

La mayoría de los Delitos Informáticos se cometen a través de alguna forma de manipulación. Tal vez el único tipo de Delito Informático que se puede salvar es el de espionaje, realizado por medio de la captación a distancia de ondas electromagnéticas producidas por el campo eléctrico de un monitor.

Desde este punto de vista decimos que la manipulación de datos es un ilícito generalmente envolvente en donde se pueden agrupar las distintas clases de delitos que se mencionaron en la clasificación.

2.1.2 Noción de Fraude y Defraudación.

Gutiérrez Francés, señala que el vocablo fraude y sus derivados, en lenguaje común, con frecuencia suelen identificarse con la idea de engaño, aunque percibe que no es fraude cualquier engaño. Por otro lado para el tratadista ecuatoriano Jorge Zavala Baquerizo el fraude es "*un modo de actuar dentro de la vida, una conducta que se manifiesta, unas veces mediante el engaño y, en otras mediante el abuso de confianza*"[10].

Por tanto se puede afirmar que, cuando se habla de fraude se está aludiendo al "modus operandi, a la dinámica intelectiva ideal, que caracteriza un determinado

[10] ZAVALA BAQUERIZO, Jorge, "Delitos Contra la Propiedad", Tomo 2, editorial edina, Guayaquil, Ecuador- 1998.

comportamiento. Implica la presencia dominante de un montaje o artimaña ideal que desencadena determinada modalidad de acción"[11].

De lo dicho se deduce que, si bien el fraude encuentra en el engaño su máxima expresión, éste no se agota con él, ya que el fraude solo supone como medios para su comisión, el engaño o el abuso de confianza, como señala Zavala Baquerizo, sino que también supone el uso o el empleo de otros artificios o medios intelectuales para elaborar ciertas maquinaciones que, como bien señala el tratadista ecuatoriano deben ir encaminadas a perjudicar el patrimonio ajeno.

Otro elemento necesario para que se configure el fraude, es la existencia, de una lesión o la puesta en peligro de un bien jurídico, protegido. Doctrinariamente el bien jurídico protegido por las defraudaciones es el patrimonio, considerando este como "*el conjunto de relaciones jurídicas activas o pasivas que pertenecen a una persona y que son estimables económicamente*"[12] . Por tanto cuando se utiliza, la fórmula fraude se hace con relación con específicos bienes jurídicos lesionados o puestos en peligro.

Siguiendo a la tratadista española Gutiérrez Francés, la defraudación es el perjuicio económico ocasionado mediante fraude, el cual comprende no solo el engaño y el abuso de confianza si no también el uso de otros medios fraudulentos, que no solo afectan el patrimonio individual de una persona, sino que también lesionan otros intereses económicos de carácter macro social.

Esta definición es muy acertada para saber lo que es la defraudación, porque es de carácter funcional, es una definición amplia, que reúne a una multiplicidad de conductas defraudatorias realizadas por medio de comportamientos astutos, engañosos y arteros lesivos de intereses económicos diversos y realizados con el ánimo de obtener una ventaja económica.

[11] GUTIÉRREZ FRANCÉS, María Luz, "Fraude Informático y estafa".
[12] CASTAN TOBEÑAS , "Derecho Civil", España, 1978.

2.1.3 Carácter informático del fraude.

Lo informático del fraude está en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera; o sea, el carácter informático del fraude alude al instrumento con cuyo auxilio se efectúa la defraudación.

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

Para los autores Magliona y López, esto es muy importante ya que "*ayuda a distinguir el fraude informático de otros hechos delictivos, que no obstante ser realizados por medios informáticos, no constituye defraudaciones, por ejemplo, atentados contra la intimidad cometidos por medio de manipulaciones informática"*[13]. A este respecto Marcelo Huerta y Claudio Líbano señalan que "*la finalidad perseguida por el sujeto activo, es la que condiciona el tipo de delito que se produce"*[14], ya que para ellos las manipulaciones informáticas se aplican a todos los delitos informáticos.

2.1.4 Principales sujetos pasivos de los fraudes informáticos.

Los sujetos pasivos que pueden ser afectados por los fraudes informáticos son todas las empresas o instituciones del sector público o privado, que tengan información en computadoras los principales blancos de este tipo de delito son:

[13] MAGLIONA MARKCOVICH Claudio Paúl, LÓPEZ MENDEL Macarena, "Delincuencia y Fraude Informático", Editorial Jurídica de Chile, 1999.
[14] HUERTA MIRANDA Marcelo, LÍBANO MANZUR Claudio, "Los Delitos Informáticos", Editorial Jurídica Cono Sur.

- Las empresas.
- Los bancos o instituciones financieras.
- Los servicios públicos.
- Las compañías de seguros.

Varios autores coinciden en que las modificaciones de los datos, vía manipulaciones se cometen principalmente por los propios trabajadores de las empresas perjudicadas, tomando en consideración que son los que tienen mayor acceso a sus sistemas, pero con el desarrollo de las técnicas telemáticas, como el Internet y servicios como cajeros automáticos, se ha abierto un nuevo campo para las manipulaciones de datos realizados por terceros extraños.

2.1.5 Características.

Las características intrínsecas de todo tipo de fraude son las siguientes

- El fraude es una acción deliberada de manipulación de datos: en la entrada, en el programa o en la salida de datos.
- El fraude puede producirse en cualquiera de las fases de de tratamiento o procesamiento o procesamiento informático de los datos.
- El objeto es obtener un beneficio económico.
- El fraude se realiza contra una organización o persona.
- El medio informático está involucrado directa o indirectamente.

2.2 Vocación del tipo clásico de estafa.

El artículo número 563, del Código Penal Ecuatoriano, recoge el tipo de la estafa el cual dice:

Art. 563.- El que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya

haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norte América.

La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en casos de migraciones legales.

Jorge Zavala Baquerizo señala que la estafa es "*un delito por la cual una persona mediante fraude (engaño, o abuso de confianza), y con ánimo de apropiación induce a otra a entregarle una cosa de su propiedad o de un tercero*"[15]. De esta lectura se deducen los elementos que constituyen al delito de estafa, con el fin de examinar si dichos elementos pueden subsumir en su estructura al fraude informático.

En primer lugar se deben señalar que el profesor Zavala Baquerizo, trata con este concepto de abarcar todas las características tanto objetivas (como el fraude y la entrega de la cosa), como subjetivas (dolo y ánimo de apropiación), contenidas en el artículo 563 del Código Penal Ecuatoriano.

Animo de Apropiación.- El artículo mencionado comienza diciendo que "el que, con propósito de apropiarse", ejecuta las maniobras fraudulentas tendientes a hacerse entregar una cosa ajena, consuma el delito de estafa. Para Zavala Baquerizo, lo que interesa aquí es que con dicha frase, el ordenamiento jurídico penal quiere resaltar "*que no solo la acción ejecutiva del agente tiende a lesionar la propiedad ajena, si no que, además, si el ánimo especial de dicha acción*

[15] ZAVALA BAQUERIZO Jorge, "Delitos Contra la Propiedad", Tomo 2 Editorial Edino, Guayaquil Ecuador, 1988.

ejecutiva no tiene por finalidad apropiarse de la cosa, es decir, hacerla ingresar en el patrimonio del autor, el delito de estafa no se consuma aunque se reúnan los demás elementos del tipo"[16].

Este elemento subjetivo tanto en la estafa como en el fraude informático está presente, ya que en ambos casos el ánimo del sujeto activo quiere apropiarse de algo que le es ajeno, que no le pertenece, por lo tanto con la acción ejecutiva lo que se persigue es lesionar el patrimonio ajeno.

Cosa Ajena.- En el derecho penal, se entiende por cosa aquello que tiene corporeidad, tangibilidad y es susceptible de apropiación. Por otro lado el término ajeno, engloba aquello que pertenece a otra persona, es decir, que se encuentra fuera del poder de disposición de una persona y que en cambio se encuentra dentro de la esfera de disposición de otra persona.

En el derecho positivo ecuatoriano, no existe la definición del término **cosa**, en este sentido por ejemplo, para el derecho civil a decir del Dr. Juan Larrea Holguín, *"se usa como sinónimos los términos bien y cosa, tal como sucede en el lenguaje popular"*[17]. Así también el Diccionario de la Real Academia de la Lengua Española, define a la palabra cosa diciendo que "viene del latín causa, y es todo lo que tiene entidad, ya sea física o espiritual, natural o artificial, real abstracta o imaginaria"[18]. El diccionario de Derecho Usual de Guillermo Cabanellas, define la cosa como *"El objeto de las relaciones jurídicas, en contraposición a persona o sujeto. Es también el objeto material en oposición a los derechos creados sobre él y a las prestaciones personales"*[19]. En un sentido jurídico más restringido, expresa lo material (una casa, dinero,) frente a lo inmaterial o derechos (un crédito, una obligación).

[16] Ob. Cita. Anterior.
[17] LARREA HOLGUÍN, Juan, "Derecho Civil del Ecuador, los Bienes y la Posesión", Tercera edición, Corporación de estudios y publicaciones.
[18] Diccionario de la Real Academia de la Lengua, 1999.
[19] CABANELLAS Guillermo, Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta, 1990.

En sentido jurídico "*se llama cosas a los objetos corporales susceptibles de tener un valor*"[20]; es decir, que para que el objeto pueda ser considerado como cosa en derecho se necesitan dos condiciones.

- Que sean objetos corporales.
- Que se trate de objetos susceptibles de tener valor, cualquiera que sea su importancia.

El derecho civil ecuatoriano usa como sinónimos las palabras bien y cosa, y así por ejemplo, el Art. 602, del Código Civil dice que, "Los bienes consisten en cosas corporales e incorporales". Lo que lleva a afirmar que existen dos clases de cosas dentro del derecho civil ecuatoriano, en primer lugar están las, cosas corporales o que tienen materia física, como un auto o una cámara y en segundo lugar las cosas incorporales o aquellas que consisten en meros derechos como los créditos.

A su vez, las cosas materiales se dividen en bienes muebles e inmuebles, y las cosas incorporales se dividen en derechos reales y personales

A decir del Dr. Juan Larrea Holguín, "Nuestro Derecho civil usa las palabras dominio y propiedad como perfectamente sinónimas"[21]. Pero la doctrina generalmente distingue entre dominio y propiedad, a pesar de la similitud de los conceptos; por ejemplo, el tratadista español Puig Brutao, señala que "*El término propiedad tiene un sentido más amplio que la palabra dominio. El primero indica toda relación de pertenencia o titularidad, y así resulta posibles hablar, por ejemplo de propiedad intelectual industrial, etc., en cambio, el dominio hace referencia a la titularidad sobre el dominio corporal"*[22].

[20] Enciclopedia Jurídica OMEBA, Tomo IV, Editorial Driskill S.A.
[21] LARREA HOLGUÍN, Juan, "Derecho Civil del Ecuador, El Dominio y los Modos de Adquirir", Primera edición, Corporación de estudios y publicaciones.
[22] PUIG BRUTAU, Juan "Derecho de cosas" Barcelona, España. Citado por Juan Larrea Holguín en la cita anterior.

En este sentido, el Art. 618 del Código Civil Ecuatoriano define al dominio (también llamado propiedad) y dice que "*es el derecho real que recae en una cosa corporal para gozar y disponer de ella, conforme a las disposiciones de las leyes y respetando el derecho ajeno, sea individual o social*"[23].

Se concluye que para el ordenamiento jurídico positivo la propiedad recae necesariamente sobre una cosa corporal es decir un objeto material, un objeto con sustancia, y que ocupa un lugar en el espacio.

Por lo tanto, la primera dificultad que surge para tratar de subsumir el fraude informático en el delito tradicional de estafa es la consideración de cosa corporal mueble como el objeto de dicho delito. Ya que de la lectura del Art. 563 determina las cosas que pueden ser objeto de delito de estafa, se deduce que, en efecto solo las cosas corporales muebles pueden constituir el indicado objeto. Por tanto, si mediante la manipulación fraudulenta de datos lo que se afecta es al dinero escritural o contable (cosa incorporal), mediante la alteración de los registros de crédito y débito no se afecta a ninguna cosa corporal mueble, sólo se adquiere un derecho de crédito contra la entidad que fuere; o bien se salda un débito que le era atribuido; si bien en ambos casos se efectúa una disposición patrimonial.

Consideramos, al igual que el profesor Zavala Baquerizo, que dentro del derecho penal no podría hablarse de cosas incorporales para los efectos de los delitos contra la propiedad, pues ni siquiera podríamos pensar que el despojo de un derecho de crédito, como en el caso señalado por ejemplo, pueda ser considerado en función de cosa corporal inmueble, si no de protección a un derecho concreto pues no se puede despojar del derecho, que está en la persona, si no que se puede despojar del ejercicio del derecho o de la cosa sobre la cual recae ese derecho. "*Nadie nos puede despojar del derecho a la libertad, el derecho lo tenemos, es el ejercicio del mismo el que nos puede ser coartado*"[24]. Nadie por

[23] Código Civil Ecuatoriano, Corporación de Estudios y Publicaciones.
[24] ZAVALA BAQUERIZO Jorge, "Delitos Contra la Propiedad", Tomo 2 Editorial Edino, Guayaquil Ecuador, 1988.

tanto, nos puede defraudar nuestro derecho a la propiedad, es el ejercicio del mismo el que nos puede ser impedido.

Ante lo anterior se aduce que en este caso el sujeto activo sustrae el ámbito de disposición del legítimo poseedor los efectos del delito, privándolo del crédito de que era titular, con lo cual se produce el mismo efecto que en la aprensión física de la cosa, consumándose el delito en el momento en que se practica la anotación de crédito en la cuenta del sujeto activo, sin necesidad que éste retire en metálico, entendiéndose que desde ese momento el sujeto activo puede disponer del dinero fraudulento conseguido.

En conclusión, la dificultad que presenta este elemento objetivo de la estafa para encasillar al fraude informático, es la de extender el concepto de cosa corporal mueble, al dinero contable que en efecto es una cosa pero incorporal, mediante una interpretación extensiva que se estima contraria al principio de legalidad, dado que la corporeidad es una característica intrínseca de las cosas corporales muebles.

El Dolo y el Medio Fraudulento.- Para el profesor Zavala Baquerizo el fraude se presenta únicamente de dos formas el engaño y el abuso de confianza. En cuanto al dolo, Zavala Baquerizo señala que *"la esencia de la estafa radica en que el agente actúa con la intención de engañar o abusar de la confianza de la víctima para lograr que ésta disponga del bien del cual se desea apropiar el agente"*[25].

Si bien es cierto que el engaño y el abuso de confianza son los medios fraudulentos por excelencia para cometer el delito de estafa, no son los únicos medios fraudulentos, también existen otros medios fraudulentos que son por ejemplo, las manipulaciones informáticas fraudulentas.

[25] ZAVALA BAQUERIZO Jorge, "Delitos Contra la Propiedad", Tomo 2 Editorial Edino, Guayaquil Ecuador, 1988.

En el Art. 563 del Código Penal se deja abierta la posibilidad de la comisión de otros fraudes que no estuvieron provistos en dicho texto legal, esa posibilidad queda coartada en el sentido de que el empleo de otros manejos fraudulentos siempre irán dirigidos o al engaño o al abuso de confianza de la víctima, lo que hace imposible la adecuación del tipo penal de estafa al fraude informático dado que, no es factible engañar o hacer caer en el error psicológico, o abusar de la confianza de una máquina.

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

En Argentina el profesor Marcos G. Salt, manifiesta que "*en el ordenamiento penal argentino la discreción sobre la posibilidad de adecuación del fraude informático a los delitos tradicionales gira alrededor de dos problema.- por un lado, la adecuación de esta modalidad de conductas en el tipo penal del hurto, requiere que el autor se apropie de una cosa mueble ajena. Esto genera algunos inconvenientes para el encuadramiento típico de las conductas que comportan el fraude informático, teniendo en cuenta que, el dinero contable, no es una cosa mueble en el sentido de la ley si no, antes bien, un crédito. Además no se produce la acción de apoderamiento si no que el objeto es recibido por el autor*"[26].

En cuanto al tipo penal de estafa, Salt, menciona "*que este requiere del engaño, de un ardid que determine el error de la víctima. Por este motivo, sostiene que, en los casos en los que el autor manipula el sistema causando un perjuicio pero sin inducir error a una persona, su conducta no será típica de los delitos de defraudación*"[27].

[26] SALT G. Marcos, "Informática y Delito", Publicación en Internet, URL: http: //.www. Derecho. Org.ar.
[27] Ob. Cita. Anterior

Podemos concluir que la vocación del delito de estafa en el Ecuador para asumir las diferentes modalidades del fraude informático deriva en una atipicidad relativa si cabe el término, ya que tanto sus elementos objetivos como subjetivos no encontrarían fundamento dentro del llamado fraude informático, ya que serían tipos completamente diferentes, así que en aplicación del principio de legalidad antes estudiado, el tipo penal de estafa no podría ser aplicado al fraude informático en razón de que sus elementos subjetivos y objetivos tienen connotaciones diferentes, lo que torna en inaplicable a dicho tipo penal clásico.

2.3 TRATAMIENTO DEL FRAUDE INFORMÁTICO EN EL DERECHO COMPARADO

ARGENTINA

En Argentina existe la Ley 26.388 de delitos informáticos que fue sancionada el 4 de junio del 2008 y promulgado el 24 de junio del mismo año, incorporándose así a la lista de países que cuentan con regulación legal sobre esta importante cuestión.

La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código Penal.

La sanción de la Ley 26.388 constituye un gran avance en la materia; tal vez sea el acontecimiento del año para el derecho informático en Argentina. Sólo basta recordar, que en materia penal rigen los principios de legalidad (una acción no es delictiva si no está expresamente tipificada como tal por una ley, por más aberrante y dañosa que pueda llegar a ser) y, como consecuencia, la prohibición

de la analogía (no se puede castigar una conducta no tipificada por su analogía con otra tipificada).

La figura del fraude informático fue incorporada en el artículo 173 del código penal inciso 16 de la siguiente manera:

Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

La pena será de tres (3) meses a cuatro (4) años de prisión.

En Argentina el delito de fraude informático como un tipo autónomo y no como una figura especial de las previstas en los arts. 172 y 173 del Código Penal. Se entiende que en el fraude informático, la conducta del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude previstos en Código: 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.

El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o Provincial, o entidad financiera.

CHILE

En Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993 la Ley n°19.223, sobre delitos informáticos, un cuerpo legal que consta de 4 artículos.

Tal es la situación que las pérdidas medias por empresa resultado del fraude ha aumentado un 22% desde el año pasado, de acuerdo con las cifras recogidas en este estudio. La cantidad media en los últimos años ha sido de 8,2 millones de dólares, frente a los 7,6 millones de dólares correspondientes al trienio precedente.

Los datos justifican tales preocupaciones: los tipos de fraude de mayor crecimiento son el robo de información, que aumentó un 27%, frente al 22% de incremento que experimentó el año pasado; y las brechas de conformidad y regulativas, cuyo crecimiento aumentó 25%, frente al 19% correspondiente a 2007.

Según la ley chilena, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

Por reforma del año 1993 se redactó una ley especial que contempla las figuras del delito informático, entre las cuales se encuentran:

1. La destrucción maliciosa de un sistema de tratamiento de información, o de alguno de sus componentes, así como impedir u obstaculizar su funcionamiento.
2. La interceptación, interferencia o acceso a un sistema con el ánimo de apoderarse o usar la información.
3. La alteración, o daño de datos contenidos en un sistema de tratamiento de la información.
4. Revelar o difundir datos contenidos en un sistema de información.

ESPAÑA

El ordenamiento jurídico español, en los últimos años, ha avanzado considerablemente en la incorporación de nuevas normas que contemplan el fenómeno informático, pero queda mucho camino por recorrer. La integración de la telemática, fusión de la informática y las comunicaciones, en la vida cotidiana ha hecho esto necesario.

La protección de los datos de carácter personal ya se encontraba prevista en el artículo 18.4 de la Constitución. Con harto retraso, cerca de 14 años, la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de carácter personal así como una serie de normas posteriores y concordantes, regulan esta protección.

En España, a partir de la reforma del Código Penal, el nuevo artículo 264.2 reprime a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

España cuenta con determinadas normas que tipifican los delitos informáticos, así como algunos órganos especiales dedicados a la persecución de los mismos.

España posee organismo para el control de los delitos informáticos, además de la ya mencionada Brigada de Investigación Tecnológica del CNP. Se trata del Grupo de Delitos Telemáticos, de la Guardia Civil.

Hasta ahora, el principal esfuerzo europeo por regular el tema de los delitos informáticos dio como resultado el "Convenio sobre la Ciberdelincuencia", de 21 de noviembre de 2001. Este documento fue firmado por los representantes de cada país miembro del Consejo de Europa, aunque su eficacia depende de su posterior refrendo por los órganos nacionales de cada país firmante.

El "Convenio sobre la Ciberdelincuencia" permitió la definición de los delitos informáticos y algunos elementos relacionados con éstos, tales como "sistemas informáticos", "datos informáticos", o "proveedor de servicios". Estos delitos informáticos fueron clasificados en cuatro grupos:

- ✓ Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- ✓ Acceso ilícito a sistemas informáticos.
- ✓ Interceptación ilícita de datos informáticos.
- ✓ Interferencia en el sistema mediante la introducción, transmisión, provocación de daños, borrado, alteración o supresión de estos.
- ✓ Abuso de dispositivos que faciliten la comisión de delitos.
- ✓ Delitos informáticos.
- ✓ Falsificación informática que produzca la alteración, borrado o supresión de datos informático que ocasionen datos no auténticos.
- ✓ **Fraudes informáticos.**

CUBA

En la legislación penal cubana no se cuenta aún con las figuras que tipifiquen de modo particular las conductas conocidas como delitos informáticos por lo que a la hora de juzgar estos hechos como delictivos, los Tribunales se ven obligados a

adecuar estas acciones a aquellas similares que aparecen tipificadas en el Código Penal.

Hasta el momento, en Cuba se han venido promulgando algunos textos legales que sin ser penales, establecen determinadas regulaciones dirigidas a garantizar la Seguridad Informática. En Noviembre de 1996, entró en vigor el Reglamento de Seguridad Informática emitido por Ministerio del Interior el cual establece la obligación por parte de todos los Organismos de la Administración Central del Estado de analizar, elaborar y poner en práctica el "Plan de Seguridad Informática y Contingencia". Por esa misma fecha el entonces Ministerio de la Industria Sideromecánica y la Electrónica, actual Ministerio de la Industria Sideromecánica, dictó el Reglamento sobre la Protección y Seguridad Técnica de los sistemas informáticos.

Por el desarrollo y vulnerabilidad que actualmente han alcanzado las TIC, la auditoría informática se ha convertido en una herramienta vital para garantizar el cumplimiento de los controles internos en todas las entidades del país que utilicen sistemas informáticos y su ciclo de revisión comprende: la administración de la seguridad de la red, la seguridad de las comunicaciones, la seguridad de las aplicaciones y la seguridad física.

La existencia de normas legalmente establecidas que regulen el funcionamiento y control del Ciberespacio y su seguridad requieren de manera ineludible de normas penales que complementen el ordenamiento jurídico y establezcan sanciones que permitan enfrentar la comisión de conductas que violen la Seguridad Informática.

En Cuba la incidencia comenzó en el año 1995, detectándose algunos casos aislados y observándose por primera vez la ocurrencia, en los delitos tradicionales, de la utilización de la tecnología para la comisión de los hechos delictivos. Esta forma de conducta delictiva se comenzó a trabajar de forma especializada y hasta la fecha se han trabajado un número reservado de hechos en los que ha estado presente las TIC.

El incremento en pocos años es significativo, de menos de 50 casos identificados entre los años 1995 al 2000 en Ciudad de la Habana, vemos que del 2001 al mes de Julio del 2004 se han incrementado de 5 a 6 veces su incidencia, igualmente vemos que en el año 2006 se ha elevado varias veces la incidencia comparada con el 2005.

2.4 Consideraciones finales del capítulo.

El principio penal universal de *nullum crimen, nulla poena, sine lege*, estima que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico protegido específico, ni que se haya determinado una pena para tales conductas, no existe delito ni pena por las acciones criminales o delictuosas.

Podemos aseverar que el fraude informático es una conducta típica y antijurídica que cobra hoy matices alarmantes en la realidad socio-jurídica ecuatoriana, toda vez que mediante esta pueden producirse defraudaciones monetarias gigantes sin que pueda imputarse delito alguno.

Las previsiones normativas con que cuenta la legislación nacional son insuficientes, desbordando el fraude informático cualquiera de estas figuras legales.

Con relación a la informática y la regulación penal solo contamos con las tipificaciones siguientes:

Art.415.1 C.P.- Daños informáticos.- el que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, base de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica cuando se trate de programas, datos, base de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.415.2 C.P.- sanción por delito mayor.- si no se tratare de un delito mayor, la destrucción, alteración, o inutilización, de la infraestructura o instalaciones físicas necesarias para la trasmisión, recepción o procesamiento de datos será reprimido con prisión de ocho mese a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art.553.1 C.P.- Apropiación ilícita.- serán reprimidos con prisión se seis meses a cinco años y multa de quinientos a mil dólares de los estados unidos de Norteamérica los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensaje de datos.

Art.353.1 C.P.- Falsificación electrónica.- son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos o la información incluida en estos, que se encuentran contenidas en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2. Simulando un mensaje de datos en todo o en parte de manera que induzca a error sobre su autenticidad;

3. Suponiendo en un acto la intervención de personas que no lo han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.

Art.563.C.P.- Estafa.- el que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsa empresas, de un poder, o de un crédito imaginario para infundir la esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento, quimérico o para abusar de otro modo de la confianza o de la credulidad será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norteamérica.

Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica el que cometiere el delito utilizando medios electrónicos o telemáticos.

La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en caso de migraciones ilegales.

CONCLUSIONES

1. La aplicación de la informática se ha extendido hasta alcanzar niveles no imaginados. La experiencia a escala internacional y nacional demuestra que este fenómeno conduce a una serie de cambios que generarán un nuevo tipo de sociedad y de conductas.

2. La delincuencia informática se considera un fenómeno transnacional que obliga la revisión de los elementos técnico-doctrinales más ortodoxos del fenómeno delictivo en su acepción más general.

3. En nuestro país la falta de leyes que controlen estos ilícitos, causan pérdidas inmensas a empresas, creadoras de sistemas de operación, es decir software, a los artistas que trabajan en el mundo de la música, y a las entidades bancarias, entre otros agentes y sujetos.

4. En los últimos años, el fraude ha aumentado aceleradamente y suele presentarse de muchas formas aún no previstas legalmente ya que se utilizan, en provecho propio, los servicios de la empresa para la cual se labora, hasta las bandas internacionales conocidas como “delincuentes tecnológicos” y quienes hacen de las estafas su profesión.

5. La previsión normativa de otras figuras resulta insuficiente a los efectos de la represión legal del fraude informático, pues este desborda los elementos de tipicidad de las primeras, resultando imprescindible la creación de un tipo penal propio para esta modalidad defraudatoria.

RECOMENDACIONES

1. Continuar el estudio del fenómeno delincuencial informático, pues este demanda la revisión de elementos, categorías e instituciones jurídicas ortodoxas para la comprensión de tales conductas delictivas.

2. Para la realidad socio-jurídico ecuatoriana, el fraude informático es una figura penal que precisa una regulación normativa propia, al desbordar los límites sancionadores y dogmáticos de tipos ancestralmente reconocidos como defraudaciones y entre las que figura la estafa.

BIBLIOGRAFÍA

1. ALESSANDRE RODRÍGUEZ, Arturo, y SOMARREVI UDAGARRA Manuel, “Los Bienes y los Derechos Rales I y II”, Imprente Universal santiago 1987.

2. ALEYTUEY DBON, María del Carmen, “Apuntes sobre la perspectiva, criminológica de los Delítos Informáticos, Informática y Derecho Nº4, UNED”, Centro regional de Extremadura, III Congreso Iberoamericano de informática, Mérida, 1994, editorial Aranzadi.

3. ALVARES DE LOS RÍOS, José Luís, “Delitos Informáticos”, Ponencia en las jornadas sobre marco legal y deontológico de la informática, Mérida 17 de septiembre de 1997.

4. BAÓN RAMÍREZ, Rogelio, “Visión general de la informática en el nuevo código penal, en ámbito jurídico de las tecnologías de la información cuadernos de derecho judicial”, escuela judicial, Consejo General del poder judicial Madrid, 1996.

5. BETTSIOL GIUSSEPPE, “Derecho Penal”, Editorial Temis, Bogotá, Colombia, 1990.

6. BRIAT MARTIN, La fraude Informatique, une approche de druit, comprar, revue de droit penal et de criminologie, año 1985.

7. BUENO ARÚS, Francisco, “El delito informático”, Actualidad Informática Aranzadi Nº 11 de abril 1994.

8. CABANELLAS DE LAS CUEVAS, Guillermo, “Régimen Jurídico de los conocimientos técnicos”, Editorial heliosta, buenos aires 1985.

9. CASTILLO JIMÉNEZ, María, ROMILLO ROMERO, Miguel, “El Delito Informático”, Facultad de Derecho de Zaragoza, congreso sobre derecho informático 22-24 de junio de 1984.

10. CHOCLAN MONTALVO, José Antonio, “Estafa por computación y criminalidad económica vinculada a la informática”; Actualidad Penal Nº 47, 22-28 de diciembre de 1997.

11. CORREA Carlos María, “El derecho informático en América latina”, Publicado en derecho y tecnología informática. Editorial Temis, Bogotá, Mayo de 1990.

12. Enciclopedia Jurídica, Omeba Editorial Bibliográfica Argentina, Buenos aires.

13 .FALCÓN PEREZ, Miguel, “Protección Jurídica de los Programas de computación”, Guayaquil Ecuador.

14. MUÑOS NAVARRO, Patricio, “Derecho e Informática”, actos y congreso Iberoamericano de Informática Jurídica, 1989.

15. RODRÍGUEZ CARAMELO, Luis Miguel, “Informática y Ordenadores, Conceptos Básicos y aplicaciones jurídicas”. Facultad de Derecho de la Universidad Complutense. 1986.