UNIVERSIDAD CATÓLICA "ANDRÉS BELLO"
DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO
AREA DE DERECHO
ESPECIALIDAD EN CIENCIAS PENALES Y CRIMINOLÓGÍCAS

EL DELITO DE FRAUDE DE ACUERDO CON LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS

Trabajo Especial de Grado para optar al Grado de Especialista, en Ciencias Penales y Criminológicas

Autor: Abog. Erika M. Crespo A.

Asesor: Abog. Oscar Cambra

Caracas, Noviembre del 2005

UNIVERSIDAD CATÓLICA "ANDRÉS BELLO"
DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO
AREA DE DERECHO
ESPECIALIDAD EN CIENCIAS PENALES Y CRIMINOLÓGÍCAS

APROBACIÓN DEL ASESOR

En mi carácter de Asesor del Trabajo Especial de Grado, presentada por la ciudadana Abogada **Erika Michelle Crespo Alvarez**, para optar al Grado de Especialista en Ciencias Penales y Criminológicas, cuyo título es: **El Delito de Fraude de acuerdo con la Ley Especial contra los Delitos Informáticos**; Considero que dicho Trabajo reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte del jurado examinador que se designe.

En la Ciudad de Caracas, a los dos días del mes de Noviembre de 2005.

_____

Dr. Oscar Cambra Nunez

C.I.: 2.217.702

ÍNDICE GENERAL

UNIVERSIDAD CATÓLICA "ANDRÉS BELLO"
DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO
AREA DE DERECHO
ESPECIALIDAD EN CIENCIAS PENALES Y CRIMINOLÓGÍCAS

EL DELITO DE FRAUDE DE ACUERDO CON LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS

Autor: Abog. Erika M. Crespo A.
Tutor: Dr. Oscar Cambra
Año: Noviembre, 2005

RESUMEN

El presente estudio representa una investigación monográfica de tipo dogmática con carácter exegético, lo que significa que parte de una ley vigente, en este caso, la Ley Especial contra los Delitos Informáticos, la cual tipifica delitos que no recogía la legislación penal, pero ocurren con frecuencia mediante la utilización de tecnologías de información como la internet o sistemas de almacenamiento de datos, como el delito de fraude en donde está inmersa directamente el uso indebido de las tecnologías de información a través del cual se inserta instrucciones falsas o fraudulentas por medio de la manipulación de sistemas o cualquiera de sus componentes, o en la data o información en ellos contenidas, con el fin de producir un provecho injusto en perjuicio ajeno y aparece para llenar un vacío jurídico existente en el Código Penal por la diversidad de modus operandi en los cuales se puede presentar. Al abordar este estudio en particular, dentro de una investigación jurídica exploratoria; se realizó el análisis de los aspectos doctrinarios relacionadas con las tecnologías de información, los delitos informáticos, los delincuentes cibernéticos, la estafa y la mencionada Ley, se tomó en cuenta las referencias dogmáticas que sustentan esta investigación y el carácter exegético que la delimita en virtud de ampliar los conocimientos y alcance del delito de fraude tipificado en la Ley Especial contra los Delitos informáticos para así ayudar a la divulgación de una normativa que no había sido desarrollada en sus aspectos innovadores el cual se ha convertido en una dura lucha en el ámbito mundial para proteger los sistemas de tecnología de información.

Descriptores: tecnologías de información, internet, delitos informáticos, delincuentes cibernéticos, estafa, fraude informático.

INTRODUCCIÓN

Las tecnologías de la información se encuentran presentes en todos los sectores de la sociedad actual, tanto en lo científico como en lo político, en la educación, en el sector privado, en la vida cotidiana de todas las personas, así como en el desarrollo y crecimiento de las naciones. En otras palabras, la vida del hombre gira en torno a elementos que utilizan tecnología de información; y son capaces de adaptarse a este modo de vida, el cual permite realizar mas cosas en poco tiempo.

Las tecnologías de la información son el conjunto de conocimientos en materia informática utilizados para el manejo de toda clase de información, auxiliándose de los medios y avances en materia de comunicación y el desarrollo de la computación, en cuanto al procesamiento automático de la información. Así mismo, el medio idóneo para encontrar esa información es el internet, que es una gran red mundial de computadoras conectadas mediante diferentes tipos de enlaces, es decir, es una red de redes porque está hecha a base de unir muchas redes locales de computadoras.

En este sentido, las tecnologías de la información traen consigo numerosos beneficios para las sociedades, como también puede arrojar

consecuencias negativas cuando son utilizadas indebidamente, pueden ser el objeto del ataque o el medio para cometer otros delitos. Poseen características que la convierten en un medio idóneo para la comisión de muy distintas modalidades de delitos informáticos, que no son más que ilícitos penales llevados a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Las tecnologías de la información colocan al alcance de millones de personas la información y datos de forma fácil y rápida. Pero algunos individuos irresponsables alteran o modifican esa información, mejor conocidos como delincuentes cibernéticos. Estos delincuentes son muy diferentes a los delincuentes tradicionales, son personas con conocimiento en el área de la informática y que tienen acceso a la información; están dispuestos a dañar o sólo son personas que tienen un leve conocimiento en computadoras y agreden los sistemas de datos de otras personas.

La presente investigación tiene como fin el estudio del delito de fraude informático, en virtud que es un tipo penal especial que no recogía la legislación penal tradicional venezolana, siendo esta nueva regulación poco conocida por los abogados, que a pesar de concentrarse en dicho estudio

ignoran su especificidad; al igual que la población, quienes son las víctimas de los delitos informáticos. Este tipo de fraude es uno de los comportamientos delictivos que se presenta con mayor frecuencia afectando el comercio electrónico, las ventas a distancia o fuera del local comercial y principalmente las operaciones de banca electrónica como las transferencias electrónicas de fondos. Ante la situación planteada, el legislador venezolano reguló esta conducta a través de la promulgación de la Ley Especial contra los Delitos Informáticos, el cual fue publicado en Gaceta Oficial N° 37.313 el 30 de octubre del 2001.

En este mismo orden de ideas, es importante destacar que el fraude informático tiene como novedad el uso indebido de las tecnologías de información, insertando de manera fraudulenta instrucciones, en donde no existe el error a través de un engaño sobre la víctima de manera directa como en el delito de estafa, sino por el contrario, es una alteración de un sistema informático que arroja un resultado diferente o contrario o inexistente al esperado, con la consecuencia de un provecho injusto en perjuicio ajeno. Son estas las razones por la cual se considera necesario el estudio del delito de fraude tipificado en la Ley Especial contra los Delitos informáticos.

Dentro de la perspectiva de la justificación, se considera necesario realizar un estudio de los delitos informáticos, principalmente el delito de fraude, y a comprender qué son las tecnologías de información, enfocando dicho análisis específicamente en la Ley Especial contra los Delitos Informáticos, todo con el fin de entender este nuevo tipo penal, así como sus aspectos innovadores.

Este estudio tiene un gran propósito, comprender las peculiaridades que presenta este tipo penal y conocer las razones por las cuales el legislador tipifica este delito en una ley especial. De igual forma, ayudar a la divulgación de la Ley Especial contra los Delitos Informáticos y entender el gran avance que se ha suscitado en el ámbito internacional para la regulación de estos delitos.

El objetivo general de la presente investigación, es analizar el delito de fraude tipificado en la Ley Especial contra los Delitos Informáticos. Así como desarrollar los objetivos específicos planteados, que son los siguientes:

- Establecer la importancia de las tecnologías de información.
- Describir el marco jurídico de los delitos informáticos.

- Identificar a los delincuentes cibernéticos.
- Determinar las características del delito de estafa contemplado en el Código Penal venezolano.
- Analizar las novedades que presenta el delito de fraude contemplado en la Ley Especial contra los Delitos Informáticos.

En lo que respecta al alcance, el investigador aborda aspectos referentes a la fundamentación teórica, conceptual y doctrinaria de la Ley Especial contra los Delitos Informáticos, para llegar a identificar los aspectos relevantes de la misma.

Es oportuno destacar, que para llevar a cabo la investigación, se estableció un análisis como única manera de obtener logros tanto a nivel del sujeto que la ejecuta, como en la exposición de motivos en cuestión, destacando la visualización del problema jurídico en cuestión desde una perceptiva legalista o dogmática, en donde el material de apoyo es legislativo y documental doctrinario.

Entra las limitaciones que interfirieron, en cierto grado, en el desarrollo de la investigación fue la ausencia de antecedentes disponibles relacionados

directamente con el tema propuesto, en virtud de la novedad que representa la Ley Especial contra los Delitos Informáticos

En relación a la metodología empleada para llevar a cabo el presente estudio bajo condiciones específicas de confiabilidad y veracidad, ésta se concibe como una investigación jurídica dogmática, el cual aborda el problema jurídico desde una perspectiva estrictamente formalista, descontando todo elemento fáctico o real que se relacione con la institución, norma jurídica o estructura legal en cuestión.

En lo que respecta a los aspectos planteados se fundamenta la visualización del problema jurídico bajo el prisma de las fuentes formales y, por ende, su horizonte se limitará a las normas legales vigentes referidas concretamente a los delitos informáticos, en especial al fraude, por lo que se ubica al presente estudio en la tipología jurídica dogmática.

La modalidad del presente estudio corresponde a la jurídica – exploratoria, la cual se trata de dar pasos preliminares frente a un problema jurídico, resaltando sus principales facetas, pero sin penetrar en las raíces explicativas del asunto. Generalmente, estas tesis abren el camino para otras investigaciones más profundas.

Es de importancia destacar que el carácter exploratorio del presente estudio obedece a una característica muy particular, representada por el hecho de que la Ley Especial contra los Delitos Informáticos, es un instrumento jurídico de reciente vigencia, de allí que la información y las disponibilidades de acceso son limitadas.

Se llevó a cabo una revisión bibliográfica dirigida a obtener información y datos de la Ley Especial contra los Delitos Informáticos, y en virtud de las características del estudio, la metodología incluyó el método o técnica del análisis tomando este aspecto como la descomposición de un todo en sus elementos. Así mismo, se incluye como Anexo “A” un glosario de términos técnicos relacionados con la informática, con el fin de obtener una mejor comprensión del estudio que se presenta.

La realización y el desarrollo de la investigación de carácter dogmática del delito de fraude de acuerdo con la Ley Especial contra los Delitos Informáticos, se estructuraron de una manera secuencial, en cinco (05) Capítulos, los cuales permiten el estudio del tema con el propósito de lograr los objetivos propuestos con apoyo de fuentes bibliográficas y documentales.

En referencia a la estructura del estudio, en el Capítulo Primero se refiriere a las tecnologías de información dividido en tres subcapítulos, el

primero se define las tecnologías de información; el segundo, la importancia de las tecnologías de información; y el tercero las tecnologías de información en Venezuela. Con las tecnologías de información o a través de ellas es el medio por cual se cometen los fraudes informáticos, de ahí radica la necesidad de establecer su concepto e importancia para la sociedad. La tecnología de la información es un conjunto de conocimientos en materia de informática, los cuales se utilizan para manejar toda clase de información, con la ayuda de los medios y avances de la comunicación y el desarrollo de la computación, en cuanto al procesamiento automático de la información.

Así mismo, el Capítulo Segundo se refiere a los delitos informáticos; el cual se divide en cuatro subcapítulos: el primero, donde se definen los delitos informáticos; el segundo, donde se realiza una clasificación de los delitos informáticos; el tercero, que se refiere a la regulación en el derecho comparado; y el último, los delitos informáticos en la Ley Especial contra los Delitos Informáticos. El describir el marco jurídico de los delitos informáticos conlleva a conocer mejor sus diferentes clases y ubicar al fraude dentro de su clasificación. Los delitos informáticos son conductas típicas donde el elemento principal es la tecnología de información a través de un medio como la computadora, este tipo de delitos contienen las mismas

características que los delitos comunes establecidos en el ordenamiento penal, pero son manipulados por elementos de información.

En cuanto el Capítulo Tercero se analiza el sujeto activo de los delitos informáticos, que lo denomina la presente investigación como delincuentes cibernéticos. Así como se divide en un subcapítulo que hace referencia a la descripción de comportamientos por parte del agente. Los delincuentes cibernéticos son personas con algún o mucho conocimiento en informática, el cual produce daños a los sistemas o a través de ella cometen algún delito, entre ellos el fraude informático.

En el Capítulo Cuarto se analiza el delito de estafa contemplado en el Código Penal venezolano, dividiendo en dos subcapítulos, el primero es una descripción de los antecedentes históricos de este tipo penal; y el segundo se realiza un análisis dogmático del delito de estafa. Tiene como finalidad el desarrollo de este Capítulo conocer el tipo penal de la estafa para luego, en el siguiente realizar una comparación con el fraude informático. El delito de estafa contemplado en el Código Penal venezolano es una conducta engañosa, que determinando un error a una o en varias personas con la finalidad de un lucro injusto para sí o para un tercero, les induce a realizar un acto de disposición con perjuicio ajeno.

El Capítulo Quinto se refiere al fraude informático. Consta de tres subcapítulos, el primero es el desarrollo de las causas que imposibilita la adecuación del tipo penal de estafa al fraude informático; el segundo, es el análisis del delito fraude en La Ley Especial contra los Delitos Informáticos; y por último se mencionan los tipos de fraudes informáticos. El fraude informático no es más que la indebida utilización de las tecnologías de información, manipulando sistemas o cualquiera de sus componentes o en información en ellas contenidas, inserte instrucciones falsas o fraudulentas con la finalidad de obtener un provecho injusto con perjuicio ajeno.

CAPÍTULO I

LAS TECNOLOGÍAS DE INFORMACIÓN

El delito de fraude de acuerdo con la Ley Especial contra los Delitos Informáticos es perpetrado a través del uso indebido de las tecnologías de información, motivo por el cual es necesario conocer su definición, así como establecer su importancia, relevancia e influencia en la sociedad moderna, para luego determinar el alcance de las tecnologías de información en Venezuela. Todo con el fin de comprender las formas por medio del cual se comete el delito de fraude informático.

Definición de las Tecnologías de Información

Desde los tiempos remotos el hombre ha considerado la comunicación como una de sus armas más preciadas, así ha utilizado diferentes mensajes simbólicos humanos como diversos medios de comunicación o tecnologías para transmitirlos. Luego de mucho evolucionar genera sus tecnologías más universales: la invención de la escritura y la imprenta, las cuales hasta hoy constituyen los fundamentos básicos de la comunicación. (Fernández y Dahnke, 1996, 54).

Las tecnologías se pueden definir usualmente como “el conjunto de herramientas hechas por el hombre, como los medios eficientes para un fin, o como el conjunto de artefactos materiales”. Pero la tecnología también contiene “prácticas instrumentales, como la creación, fabricación, uso de los medios y las máquinas; incluye el conjunto material y no material de hechos técnicos; está íntimamente conectada con las necesidades institucionalizadas y los fines previstos a los cuales las tecnologías sirven” (García, 2005, 8).

Con respecto a la información, Barrios (2001, 4), la define como el “conjunto de datos numéricos y alfanuméricos que representan la expresión de un conocimiento, que puede utilizarse para la toma de decisiones”.

Por otra parte, la comunicación constituye el proceso social por excelencia, porque “permite al hombre desarrollar sus capacidades y mantener viva la comunidad, la cultura y el progreso” (Rodríguez, 1998, 1).

En este sentido, la tecnología de la información se puede entender como un “conjunto de dispositivos y procesos lógicos y prácticos, que basados en soportes físicos permiten agregar valor a los datos, comunicarlos y transformarlos en productos y servicios, a fin de promocionar una ventaja competitiva a sus usuarios” (Grandinetti, 2000, 17).

Desde la segunda guerra mundial, el desarrollo de la tecnología de la información y de la comunicación ha sido vertiginoso, con el mayor crecimiento en la revolución social del computador donde los datos pudieran ser almacenados y transformados rápidamente en información, este vuelco que se presenta en la forma de producir y compartir información genera lo se conoce como la era de la información. Esta era se caracteriza por el amplio espectro que la información alcanza, puesto que es producida socialmente para crear conocimiento. (Andrades, 2000, 18).

La Ley Especial contra los Delitos Informáticos en el artículo 2 literal a, define lo que se entiende por tecnología de información como:

> La rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

Así mismo, a las tecnologías de la información y comunicación las define el Centro Nacional de las Tecnologías de la Información como "aquellas tecnologías que permiten transmitir, procesar y difundir la información de manera instantánea y constituyen, por lo tanto, la base sobre la cual se construye la sociedad de la información" (2004, 1).

En tal sentido, para la presente investigación, la tecnología de la información puede ser definida como el conjunto de conocimientos en materia informática utilizados para el manejo de toda clase de información, auxiliándose de los medios y avances en materia de comunicación y el desarrollo de la computación, en cuanto al procesamiento automático de la información.

Es evidente entonces, que las tecnologías de información cumplen un papel determinante en esta nueva sociedad, por lo que los ciudadanos en general y los gobiernos en particular, especialmente en aquellas naciones que van a la vanguardia del desarrollo, han comprendido la convergencia de elementos que comienzan a desplegarse tratando por ende de organizar el contexto tecnológico para aumentar su productividad y riqueza. Los enfoques concuerdan en crear a las tecnologías de información como instrumentos que pueden ayudar al logro de amplios objetivos nacionales, tanto sociales como económicos, en la medida en que los Estados las concentren en las principales políticas y programas de desarrollo de sus naciones.

Importancia de las Tecnologías de Información

Las tecnologías de la información son principalmente la “informática y afines, debido a su facilidad para adoptar soluciones, cuando se implanta el

sistema de información y se almacenan datos, se obtiene un proceso rápido y con pocos errores, así mismo comunicaciones automáticas entre los procesos que se utilizan, en ello radica la importancia que tiene su progreso para el desarrollo de un país" (Cruz, 2005, 2). Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad y otros, son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

En efecto, se observa que la tecnología ha cambiado el estilo de vida, las costumbres y forma de pensar de las personas en todos los ámbitos. Los beneficios que trae consigo la tecnología moderna son muy numerosos y ampliamente conocidos. Una mayor productividad proporciona a la sociedad excedentes que permiten disponer de tiempo libre, dispensar la educación; y de hecho, proseguir la propia labor científica. Cuando quedan satisfechas esas necesidades básicas y la tecnología empieza a proporcionar beneficios cada vez más triviales.

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" (Manson, 1999, 1), y las ubica el mismo autor, como un nuevo medio de comunicación, condicionado su desarrollo en la informática. Tecnología cuya esencia se

resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Además, esta tecnología de la información pretende poner al alcance del hombre la información que va desde lo científico, cultural, económico, y otros, sin ninguna limitación, y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al entregar una cantidad de datos que hasta hace poco exigían una larga búsqueda, donde las personas desempeñaban un papel importante y ahora se cuenta con el sólo manejo de las máquinas que entregan todo ese conocimiento de la manera mas fácil y rápida. Afirmando de esta manera, que la informática ha llegado a obtener el puesto de poder social, por todos los elementos que pone a disposición de los gobiernos de cualquier estado y de los particulares, economizando tiempo y energía en la mejora para el desarrollo de cualquiera que lo necesite.

Cabe agregar, que 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.

Por su parte, según Tablante (2001, 18), en los últimos años, “la rápida evolución de las tecnologías de la información, la unión entre el desarrollo informático y las telecomunicaciones, entre computadoras y redes de comunicación, bautizada como teleinformática ha abierto paso a lo que algunos llaman la sociedad informatizada o sociedad de la información”.

En efecto, nadie pensaría que la evolución de la tecnología pudiera llegar a opacar la mano de obra por parte del hombre, o que cualquier información se podía encontrar en un solo lugar, además de la gran comunicación existente entre las personas. La tecnología informática está alterando la naturaleza y el curso futuro de la vida de las personas de un modo positivo. El trabajo del hombre es cada día más fácil y de forma intelectual, donde el campo laboral está más exigente porque las personas deben tener un mayor conocimiento de la informática, así mismo la tecnología informática cambiará enormemente la forma en que la gente aprende y concibe al mundo.

De hecho, cuando el volumen de información fue superior a la capacidad humana, se necesitó de medios para poder almacenarla,

procesarla y proporcionarla, así como brindar resultados, siempre tomando en cuenta las necesidades del hombre y obtener buenos resultados para lograr así un buen trabajo en cualquiera de las áreas donde se desenvuelva. (Barrios, 2001, 3).

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aún están en la memoria los métodos antiguos de comunicación, y más recientemente los mensajes transmitidos a través de cables utilizando el código morse, o la propia voz por medio del teléfono. La humanidad no ha terminado con la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estos elementos y métodos, y además con la idea de ayudar al hombre en aquellos trabajos habituales y monótonos, generalmente de procesamiento de datos.

Así mismo, en toda la historia de la humanidad, el hombre ha procurado garantizar y mejorar su nivel de vida mediante un mejor conocimiento del mundo que le rodea y un dominio más eficaz del mismo, es decir, mediante un desarrollo constante de la ciencia.

Es muy acertado afirmar, que una de las características del momento actual es la conexión rápida y eficaz que se puede encontrar, y la muy

estrecha interacción y el acondicionamiento mutuo de la sociedad con la ciencia. La ciencia es uno de los factores esenciales del desarrollo social y está adquiriendo un carácter cada vez más masivo.

En consecuencia, nace el internet “en 1962, en pleno auge de la guerra fría entre los bloques comunista y capitalista, la instalación de una batería de misiles nucleares en Cuba por parte de Unión Soviética generó pánico colectivo en los Estados Unidos” (Tablante, 2001, 18). Ante este ataque el “gobierno norteamericano ordenó al pentágono el desarrollo de un sistema de comunicación, de una red, entre las principales bases militares alrededor del mundo” (Tablante, 2001, 18). A partir de entonces la antigua red militar empieza a ser enriquecida por los aportes del mundo civil, particularmente del mundo académico, y posteriormente del mundo empresarial, dando origen a un conjunto de innovaciones que van a explotar quince años después, cuando la red es abierta al publico masivo.

Cabe destacar, según Barrios (2001, 2), que el término internet es una contracción de internetwork System (sistema de intercomunicación de redes). Algunos técnicos identifican el término internet como una contracción de INTERnacional NET (red internacional de computadoras).

Por su parte, el Doctor Rojas Amandi (citado por Barrios, 2001, 2), indica que “internet es un sistema maestro de diversas redes de computación que cumple dos funciones básicas: medio de comunicación y medio de información”.

A los efectos de este trabajo, el internet es el conjunto de computadoras, redes y dispositivos de telecomunicaciones, conectados por medio de enlaces, tanto nacional como internacionalmente, y que permiten la comunicación y el intercambio de información y servicios, lo que se realiza a través de un protocolo común.

Cabe agregar, que el internet es una red mundial de un sistema de ordenadores interconectados, cuyos usuarios pueden comunicarse entre sí, siempre que tengan permiso de acceso, mediante un protocolo común. Este protocolo es de control de transmisión/protocolo de internet (TCP/IP) y utiliza un soporte físico de telecomunicaciones que pone a disposición de los usuarios gran cantidad de información y de servicios. (Barrios, 2001, 2)

En efecto, el internet es el medio idóneo para encontrar información, donde las personas tienen a su alcance más oportunidades de localizar distintos tipos de resultados, es por ello que se afirma que el internet es la transformación rápida de la naturaleza misma de los hechos sociales, los

conceptos tradicionales adquieren otras dimensiones, es actividad continua a velocidad superior a la capacidad de reacción, es intercambio de información desde cualquier parte del mundo, y el más notorio fenómeno de crecimiento que se ha vivido donde la ciencia siempre implementa elementos que facilitan el desarrollo de la vida de las personas, su tráfico se duplica cada día y considerando que millones de personas interactúan en la línea o en la red en solo milésimas de segundo haciendo que la comunicación sea mas rápida y eficiente.

Si bien en Venezuela hay un camino recorrido en esta materia, teniendo el Estado en ello un papel determinante, es posible decir que tales elementos como son las computadoras, redes y procesamiento electrónico de datos, telefonía móvil, satélite, anchura de banda para transmisión de voz y datos, y la utilización de nuevos materiales como la fibra óptica, tendrán el fin de estimular la conexión en todos los lugares de la sociedad y que esto se restituya en beneficios sociales y económicos extensivos.

Así mismo, cada día las personas deben interactuar más con las tecnologías de información, ya sea por conocimiento o transmisión de ideas, obtención de datos o difusión de información por cualquiera de sus medios. Como hay personas que fomentan la evolución de las tecnologías, existen otras que se aprovechan y se apoderan de ellas, realizan actos contrarios a

su fin o intentan expresar la información de manera errada obteniendo beneficios ajenos, cometiendo actos que van en contra del ordenamiento jurídico.

En tal sentido, junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos.

Igualmente se considera al derecho como un “instrumento regulador de las relaciones humanas que procura mantener el orden social, además juega un papel importante para la regulación de los medios informáticos y la nueva forma de vida que las personas”, tratando de adecuarse en las normas el mundo actual que evoluciona rápidamente (Barrios, 2001, 4).

Por esta razón, es necesario buscar fórmulas o mecanismos efectivos para solucionar los problemas que acarrean el uso de las tecnologías, y en muchos casos con cierta complejidad y sin solución. En estos casos es necesario la regulación de estos actos y el cumplimiento de las normas para el buen funcionamiento del estado de derecho.

El desarrollo y la evolución del derecho informático nace porque la mayoría de la población mundial tiene contacto permanente con la computadora; y ésta evolución no tiene mucha trayectoria como las demás legislaciones que estudian otras ramas del derecho, pero sí existe en el ámbito del derecho informático legislación basada en normas, tratados y convenios internacionales, además de los distintos proyectos y leyes especiales que promueven los entes legislativos con la finalidad de proveer seguridad a los usuarios y un encuadre legal de los instrumentos o medios informáticos.

Así mismo, la información que se obtiene de las tecnologías ha adquirido un valor superior desde el punto de vista económico, constituyéndose en un bien esencial del mundo jurídico, adquiriendo importante relevancia jurídico-penal por ser posible objeto de conductas delictivas y por ser instrumento de facilitación, aseguramiento y calificación de los ilícitos tradicionales.

La informática está en todos los sectores, es una realidad indiscutible. La vida del hombre gira en torno a elementos que utilizan tecnología de información; y son capaces de adaptarse a este modo de vida que permite realizar más cosas en poco tiempo, es decir, desde lo más trivial hasta lo mas sofisticado. Todo ésta relacionado con la informática, sin la tecnología el

mundo colapsaría por que se depende cada vez más de las computadoras y es a la vez una forma de tener al alcance tanta información y poder manejarla.

De igual manera, nadie escapa de la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y así como la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, y otros, son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

El mundo de las tecnologías de información traspasa fronteras territoriales, uniendo a todas las personas del mundo en un solo pensar, transportándolos a un mundo virtual. Logrando la difusión inmediata de información de un lugar a otro, conociendo las noticias, operaciones comerciales, bancarias, cadenas de información, que revolucionan y seguramente continuarán revolucionando al mundo.

Por consiguiente, la tecnología de información tiene su importancia en su capacidad para colocar en la red conocimientos e ideas tecnológicas, facilitar su interconexión y reforzamiento mutuo, y transformarlos en procesos

de información que multiplican el impacto específico de cada tecnología. Todo ello debido a la evolución que ha tenido la informática en el mundo para tener al alcance de la mano toda la información con la rapidez y facilidad que se puede obtener por medio de la red. Actualmente estas tecnologías ayudan a entender que el ser humano gusta de estar informado con cualquier lenguaje.

Las Tecnologías de Información en Venezuela

La importancia que el Estado le otorga a la tecnología de información se puede ver reseñada en el artículo 110 de la Constitución de la República Bolivariana de Venezuela que establece:

> El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

A partir de la promulgación de la Constitución de 1999, Venezuela ha experimentado un desarrollo legislativo marcado por un acentuado propósito

de lograr la actualización de normas y la integración del país en el marco de una economía globalizada, dentro de estos cambios, la tecnología ha ocupado un lugar de destacada importancia. En el propio texto constitucional se puede apreciar la influencia de la tecnología en el ámbito jurídico, al consagrarse el acceso a la tecnología como un derecho fundamental de los ciudadanos, reconociéndose dentro de los derechos culturales, el carácter de interés público de la ciencia, la tecnología, el conocimiento y la innovación, tal como lo establece el artículo 110.

Igualmente, en el artículo 108 la Constitución de la República Bolivariana de Venezuela, impone al Estado la obligación de garantizar los servicios de radio, televisión, redes de biblioteca y de procesamiento de datos, con el fin de permitir el acceso universal a la información, estableciendo como deber de los centros educativos, la necesidad de incorporar el conocimiento y la aplicación de las nuevas tecnologías en los procesos de enseñanza, como nueva forma de seguridad para la sociedad de estar comunicado.

En desarrollo de este derecho constitucional, la Comisión Nacional de Telecomunicaciones (CONATEL), organismo rector de las telecomunicaciones en Venezuela, adoptó en el año 2000 el Plan Nacional de Telecomunicaciones, donde se menciona por primera vez la necesidad

de incorporar a la nación dentro de la sociedad de la información. En el marco de este plan, se establecen como objetivos primordiales para el desarrollo del país, el fomento del uso de internet a todos los niveles y la divulgación del conocimiento y el uso de las tecnologías de la información y las comunicaciones. Siguiendo estos principios, a finales del 2001 el Ministerio de Ciencia y Tecnología dicta el Plan Nacional de Tecnologías de la Información, destacando entre sus principales lineamientos:

> La promoción a la investigación y el desarrollo de la transferencia de tecnología en el ámbito de la Tecnología de la información y las Comunicaciones (TIC); desarrollo y la capacitación del talento humano; la modernización del Estado a objeto de potenciar la calidad de los servicios públicos y la promoción en el uso de las TIC en el sector productivo y su democratización a fin de establecer una sociedad en línea. (2, 2001).

Cabe decir que la importancia de la consagración del acceso a la tecnología como un derecho fundamental, se ha visto reflejada en la adopción de distintos textos legales que obligan a la administración a facilitar el empleo de medios tecnológicos en sus relaciones con los administrados.

En este sentido, en el Plan Nacional de Tecnologías de Información se establecen los aportes de las tecnologías de la información y la comunicación en todos los ámbitos de la sociedad; la actuación del Estado se manifiesta de manera concreta en:

a. Los procesos educativos a todos los niveles y modalidades, y de bienestar social.
b. En el desarrollo rural y en la programación de la distribución de la riqueza.
c. En los esfuerzos de conservación de los recursos naturales y del medio ambiente.
d. En los procesos de dirección y gobierno para construir una economía fuerte con armonía social. (p. 3).

De igual manera, este plan revertirá el proceso de desequilibrio existente en los servicios básicos con el proceso de apertura del sector. La creación de un Fondo de Investigación y Desarrollo de las Telecomunicaciones servirá para crear mecanismos institucionales que incentiven la participación del sector privado. Así mismo, la creación del Fondo de Servicio Universal que permitirá democratizar el acceso a las nuevas tecnologías. Por consiguiente, su ejecución en forma coordinada con los demás planes nacionales y regionales en este ámbito, apoyarán el desarrollo y la consolidación de una Plataforma Nacional de Tecnología de Información (PNTI), sustentada con mecanismos de financiamiento de diversas fuentes, con lo cual se incrementarán los recursos de capital necesarios para desarrollar el sector de las tecnologías de la información y comunicación en el país.

Es importante destacar que el punto de referencia para el diseño de las políticas orientadas a lograr la Plataforma Nacional de Tecnología de Información, partirá de las necesidades globales de la nación y la sociedad,

con mayor enfoque hacia la atención de los sectores sociales de menores ingresos, de la demanda de las pequeñas empresas y del desarrollo armónico de las regiones y localidades.

Por lo tanto, teniendo como norte estos aspectos antes señalados, este Plan de Tecnologías de Información no se establece como una forma científica o impulsadora en la informática, sino que se refiere a la capacidad y repercusión de estas tecnologías en el desarrollo del país como un todo. En atención a ello, busca proporcionar un marco estratégico y de políticas para aprovechar en la medida de lo posible esa capacidad y repercusión hacia el desarrollo de sectores esenciales como la enseñanza, la salud, el ambiente, la gestión pública y el comercio electrónico.

Adicionalmente el 10 de mayo de 2000, se promulgó el decreto presidencial 825 mediante el cual se declara el uso de internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela. Siguiendo los principios constitucionales establecidos en el artículo 110, el decreto 825 reconoce como de interés público la ciencia, la tecnología, el conocimiento y los servicios de las tecnologías de la información, imponiendo a los órganos de la administración pública nacional, la obligación de incluir en el desarrollo de sus actividades, metas relacionadas con el uso de internet a todos los

niveles, a objeto de facilitar la tramitación de los asuntos de su competencia y el intercambio de información.

Así mismo, el nombrado decreto, contempla entre otras cosas “el incentivo al uso del internet a todos los niveles y la mejora de la calidad de vida de la población a través del uso de los servicios de telecomunicaciones” (2000, 1). La visión es insertar a los ciudadanos en una sociedad del conocimiento, permitiendo la oportunidad de capacitación a través de internet.

En Venezuela existe una infraestructura de telecomunicaciones que provee servicios básicos, tanto en el sector público como en el privado. El Estado ha invertido recursos en el ámbito de la educación superior para formar una generación de profesionales calificados que atienda este sector. Desde el punto de vista legislativo, se promulgó la nueva Ley Orgánica de Telecomunicaciones en Gaceta Oficial No. 36.970 de fecha 12 de junio de 2000, con la finalidad de generar un marco adecuado para la modernización y apertura de las telecomunicaciones en el país.

Adicionalmente esta Ley Orgánica, tiene la finalidad de adaptar la legislación a las nuevas tendencias del sector, cambiando la noción tradicional de servicio público por la de “actividad de interés general”,

correspondiéndole a los particulares prestar el servicio en régimen de libre competencia. Dentro de los objetivos de esta ley en materia de tecnológica, se destacan: la promoción a la investigación, el desarrollo y la transferencia tecnológica en materia de telecomunicaciones y la utilización de nuevos servicios, redes y tecnologías con el propósito de asegurar el acceso a éstos en condiciones de igualdad a todas las personas. Para garantizar el cumplimento de sus objetivos, la ley exige a los distintos operadores la homologación y certificación de equipos, así como el uso de la tecnología adecuada, a fin de lograr el acceso universal a la comunicación.

Es conveniente destacar el decreto Ley de Mensajes de Datos y Firmas Electrónicas No 1.204, promulgado el de 10 de febrero de 2001, el cual está orientado a reconocer valor y eficacia jurídica a los documentos electrónicos, equiparándolos a los documentos tradicionales. Este instrumento constituye el punto de partida para la tramitación de los procedimientos electrónicos en el campo de la administración pública y la administración de justicia. Cabe destacar, que los diversos textos jurídicos promulgados luego de la adopción de esta ley, contemplan de una u otra manera la posibilidad de tramitación de los procedimientos tradicionales en forma electrónica.

En el ámbito tributario, el actual Código Orgánico Tributario, promulgado en el año 2001, contempla la posibilidad de tramitar sus procedimientos a través de medios electrónicos, a tal efecto, el artículo 125 establece la potestad a la "Administración Tributaria de utilizar medios electrónicos o magnéticos para recibir e intercambiar documentos, declaraciones, pagos o actos administrativos, así como cualquier información en general". En atención a esta norma, el Servicio Nacional Integrado de la Administración Aduanera y Tributaria (SENIAT) ha puesto a disposición de los contribuyentes una vía alternativa que permite realizar la declaración de impuestos a través de Internet.

En el decreto con fuerza de Ley de Reforma Parcial de la Ley de Licitaciones No. 1.555 publicado el 13 de noviembre del 2001, también se contempla el uso de los medios electrónicos, específicamente en el artículo 136, que faculta al "Ejecutivo Nacional para reglamentar el uso y la aplicación de estos medios en los procesos de licitación". De la misma manera, el decreto con Fuerza de Ley de Registro Público y Notariado No. 1.290 del 30 de agosto del 2001 y publicado el 13 de noviembre del 2001, implementa los medios electrónicos en la gestión y automatización de los registros y las notarías, otorgando validez a la firma electrónica de los Registradores y Notarios (artículos 2, 4 y 5).

En el campo de la investigación y el desarrollo tecnológico, cabe mencionar la Ley Orgánica de Ciencia, Tecnología e Innovación, promulgada en septiembre del 2001, con la finalidad de desarrollar los principios que establece el artículo 110 de la Constitución en materia de ciencia, tecnología e innovación, mediante el estímulo y fomento de la investigación científica, definiendo los lineamientos que sirven de base para el desarrollo de estas actividades.

Así mismo, dentro de sus objetivos se destacan: la promoción y el fomento de los planes nacionales en materia de ciencia, tecnología e innovación; el estímulo a los programas de formación en estas áreas, a través del establecimiento de incentivos a la investigación; el fortalecimiento de las infraestructuras y servicios adecuados en las instituciones de investigación, desarrollo e innovación tecnológica y el impulso al establecimiento de redes de comunicación para la cooperación científica y tecnológica.

Para asegurar el cumplimento de estos objetivos, la ley propone la creación del Sistema Nacional de Ciencia, Tecnología e Innovación, integrado por instituciones públicas o privadas, entre éstas el Ministerio de Ciencia y Tecnología, dando cabida a todas aquellas personas que se dedican o tienen participación en actividades científicas vinculadas a la

investigación y desarrollo de la innovación tecnológica y a la formación y el perfeccionamiento del talento humano necesario para el desarrollo de estas actividades.

Finalmente es de destacar la repercusión de la tecnología en el ámbito del Derecho Penal. A objeto de salvaguardar el acceso a la tecnología, en octubre del 2001 tuvo lugar la publicación de la Ley especial contra Delitos Informáticos, adoptada con la finalidad de lograr la protección integral de los sistemas que utilicen tecnologías de la información, previniendo y sancionando los delitos cometidos contra tales sistemas o mediante el empleo de medios tecnológicos.

En efecto, para el país avanzar hacia la sociedad del conocimiento y de la información exige capacidad de dirección y gobierno. Se hace necesario el entendimiento de amplia base entre los dirigentes nacionales, los encargados de tomar las decisiones y la población en general. La posición de este conjunto de actores ante los cambios que se avecinan, así como las implicaciones que estas decisiones tienen en la transformación del modelo económico, social y político existente, permitirá situar a Venezuela dentro de las nuevas corrientes de una economía mundial basada en el conocimiento, aprovechando por ende, las mejores oportunidades que brinda un contexto marcado por la globalización.

Por lo tanto, el Estado debe dar el primer paso hacia su propia modernización mediante la introducción y uso masivo de las tecnologías de la información y comunicación, para la automatización de sus procesos, prestar sus servicios en línea, implantar la comunicación entre los miembros del mismo estado, y con la sociedad (gobierno electrónico). Esta modernización va acorde con el nuevo papel que debe cumplir el Estado en la sociedad del conocimiento y la información, a saber: vigilante y proveedor de soluciones para que exista igualdad de información, integridad y privacidad, y protección a la propiedad intelectual; promotor y coordinador de la infraestructura institucional, industrial y de recursos humanos; removedor de obstáculos críticos del proceso; y sobre todo, difundir la utilidad de las tecnologías de la información y comunicación como colaboradores al asentamiento de un nuevo modelo de sociedad y como impulsoras de procesos complejos como son la descentralización y desconcentración del poder público.

De todo esto se desprende que el mundo actual se caracteriza por un creciente acceso a la tecnología y a una globalización social de la información y de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas como internet, en los próximos años proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos. La infraestructura de la información se ha convertido en una parte vital del eje de

las economías. Los usuarios deberían confiar en la disponibilidad de los servicios informativos y tener la seguridad de que sus comunicaciones y sus datos están protegidos frente al acceso o la modificación no autorizados.

Sin embargo, esto no siempre sucede y se cometen una infinidad de actos que atentan contra la seguridad de las tecnologías de información, así como de la información o bienes patrimoniales de las personas. Por las consideraciones anteriores el siguiente Capítulo define los delitos informáticos, analiza la regulación de estos delitos en el ordenamiento jurídico venezolano, así como sus clasificaciones.

CAPÍTULO II

DELITOS INFORMÁTICOS

En el presente Capítulo se describe el marco jurídico de los delitos informáticos a través de su definición, así como los planteamientos de los diferentes criterios acerca de la validez de clasificarlos de esta forma. De igual manera, se presentan las diferentes clasificaciones de esta clase de delitos y la regulación que se le ha dado en el Derecho comparado, para finalmente describir los delitos informáticos que contempla la Ley Especial contra los Delitos Informáticos, entre los cuales se ubica el fraude informático.

El marco Jurídico Venezolano se enriquece con la entrada en vigencia de la Ley Especial contra los Delitos Informáticos, el cual fue publicado en Gaceta Oficial N° 37.313 el 30 de octubre del 2001 y tiene como propósito regular y dar respuesta sancionatoria a las conductas que vulneran bienes jurídicos a través del uso indebido de las tecnologías de información, las cuales necesitaban ser reguladas, por cuanto no estaban contempladas en el ordenamiento penal.

Esta ley especial, busca ir mas allá de la tipificación de los delitos y de atender de manera integral los aspectos y necesidades de las personas afectadas, así como comprender en un mismo texto, alternativas punitivas y la tipificación como conducta delictiva del mayor número de posibles manifestaciones de los delitos informáticos, sean de índole contra la propiedad, la privacidad de las personas y de las comunicaciones, los niños y adolescentes, y otros.

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 en la informática" (Lorenzo, s/f, 1). Tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. Así mismo, las aplicaciones de la informática no sólo tienen un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los bienes jurídicos de las personas.

Como puede observarse, este es el panorama de este nuevo fenómeno científico y tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que las tecnologías de la información y comunicación constituyen una forma de poder social. Las ventajas de este fenómeno ponen

a disposición de gobiernos y de particulares, la rapidez y el ahorro consiguiente de tiempo y energía, como también configuran un cuadro de realidades de aplicación y de posibilidades de actos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Hoy las tecnologías de información se han implantado en casi todos los países. Como advierte la autora Lorenzo, “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” (s/f, 1). Sin embargo, junto a estas incuestionables ventajas de la informática, comienzan a surgir algunas facetas negativas relacionadas con su uso, como por ejemplo, lo que se conoce como delitos informáticos.

Así mismo, se observan las grandes posibilidades de la informática como instrumento de desarrollo económico, social y cultural, y se ha advertido acerca de algunas de sus consecuencias negativas, como la errónea utilización de las nuevas tecnologías de información o si se quiere, en aquellas nuevas conductas delictivas que requieren la intervención del derecho penal.

Sin embargo, la tecnología no se ha utilizado solamente para el beneficio del hombre, sino que también algunos individuos han traspasado sus límites de seguridad y han realizado actividades fraudulentas, lo cual genera alerta y preocupación por parte de los usuarios de este medio informático.

Naturalmente frente a este fenómeno es imposible que la criminalidad quedara fuera del impacto de la tecnología de la información. Donde se aprecia que la informática abre nuevos horizontes al delincuente, incita su imaginación, favorece su impunidad y potencia los efectos del delito convencional; a lo cual contribuye por la facilidad para su comisión y encubrimiento y la dificultad para su descubrimiento, prueba y persecución.

Así mismo, si se toma en cuenta que los sistemas informáticos pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas; se comprenderá que están en juego valores

colectivos y los consiguientes bienes protegidos que el ordenamiento jurídico institucional debe asegurar.

Cabe destacar, que el abuso de los sistemas de información puede generar consecuencias nefastas, debido a la mala utilización de la información de los ciudadanos, la cual está protegida por las garantías constitucionales propias de un Estado de Derecho, y donde la información implica poder y este aumenta la capacidad de control sobre los individuos.

Por lo tanto, la informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, el hurto, y otros). La capacidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente sencilla manipulación de esos datos, como en esta área existe gran cantidad de información y toda se puede encontrar en un solo lugar, todo va a depender de la agilidad que tiene el usuario para su aplicación.

El desarrollo de las tecnologías de la información y comunicación promueve nuevas posibilidades de delincuencia. Así afirma la autora Lorenzo, (s/f) cuando advierte:

> La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. (p. 2).

Definición de los Delitos Informáticos

Para definir lo que se entiende por delito informático es necesario desglosar cada uno de sus términos, y analizarlos teniendo en cuenta de donde se origina el término jurídico que el derecho penal lo ajusta al marco jurídico.

En este sentido, la palabra delito proviene del verbo latino delinquere, que significa “abandonar, apartarse del buen camino, apartarse del sendero señalado por la ley” (Capitánt, 1930, 89).

Por su parte, para González (citado por Ramírez, 2003, 3) el delito "es un comportamiento típico, antijurídico y culpable". Es por eso que para Villalobos (citado por Ramírez, 2003, 3), el delito "es un acto humano típicamente antijurídico y culpable". Así mismo, según Pina Vara (citado por Ramírez, 2003, 3), el delito "es un acto u omisión constitutivo de una infracción de la ley penal".

De igual forma, el Dr. Grisanti (2000, 78), define al delito como “un acto típicamente antijurídico, culpable e imputable a un hombre y castigado con una pena, más ampliamente castigado con una sanción penal”.

Según el penalista Cuello (1983), los elementos integrantes del delito son:

> El delito es un acto humano, es una acción (acción u omisión). Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido. Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.
> El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
> La ejecución u omisión del acto debe estar sancionada por una pena.
> Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena. (p. 66).

En efecto, el delito representa generalmente un ataque directo a los derechos del individuo, donde la ruptura de las normas trae consigo la sanción de la misma. Toda persona que vulnere un bien estará propensa a una amonestación ya que se han realizado normas para seguridad de las personas y protección de sus bienes, tomando en cuenta que la conducta del agresor, dependiendo de los actos que cometa, deberá estar tipificado en el ordenamiento jurídico.

Con respecto a la informática, según Mora y Molino (citado por Ramírez, 2003, 12), la define como un “estudio que delimita las relaciones entre los medios, es decir, equipo, datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado”.

En este sentido, para la presente investigación, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.

En la Ley Especial contra los Delitos Informáticos no se establece claramente la definición de los delitos informáticos, es decir un concepto universal, por tal razón se hace una breve reseña de algunos autores que estudian el tema y han enunciado un concepto práctico atendiendo las necesidades de la época.

Según el autor mexicano Téllez (1996, 104), los delitos informáticos se pueden conceptualizar de forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Para Sarzana, en su obra “Criminalista y Tecnología” (citado por Morales, s/f, 2), 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".

Así mismo, la autora Callegari, (citado por Morales, s/f, 2) define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

En cuanto a la definición Davara Rodríguez (citado por Palazzi, 2000, 272), entiende a los delitos informáticos como “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada acabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”.

Debe señalarse el concepto de Calvo (citado por Morales, s/f, 2), quien considera 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".

Para García de la Cruz (2005), el delito informático es:

> Toda acción culpable realizada por un ser humano que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que por el contrario produzca un beneficio ilícito a su autor aunque no perjudique en forma directa o indirecta a la víctima. (p. 2).

En efecto, los delitos informáticos son conductas típicas por que están reguladas en un ordenamiento jurídico donde el elemento principal es la tecnología de información a través de un medio como es la computadora, que es un instrumento muy utilizado por el ser humano, y se refiere a las atípicas como la actitud que toman las personas frente a esté, donde el manejo de la computadora viene a ser su arma principal y el conocimiento que adquieren frente a ésta, a lo largo del desempeño de las personas dentro del área electrónica.

Por su parte, para García (citado por Cruz y Salvador, s/f, 13), el delito informático es "todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes".

Significa entonces, que este hecho ilícito es realizado a través de tecnología de información, siempre relacionado con el alcance que tiene la

persona para la obtención de información; de esta forma, existe una ruptura entre el ordenamiento y la protección de los bienes jurídicos de las personas.

Dentro de esta perspectiva, para la presente investigación, los delitos informáticos se pueden definir como todas las acciones u omisiones realizadas, típicas, antijurídicas y culpables; trátese de hechos aislados o como una serie de ellos, que van en contra de las personas naturales o jurídicas, realizadas con el uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima. Lo cual generalmente producirá de manera colateral lesiones a distintos valores jurídicos, otorgando así un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

En efecto, el agente a través del uso indebido de la tecnología de información obtiene un beneficio para sí o para otro. Cabe considerar por otra parte, que el medio a utilizar para la realización de este acto es a través de la computadora, por medio del cual obtiene un beneficio en perjuicio de la víctima.

En este sentido, se señala el concepto de los autores Beltramone, Herrera y Zabale (1999, 33), quienes consideran al delito informático como “toda conducta que revista características delictivas, es decir, sea típica,

antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".

Significa entonces, que el delito informático contiene las mismas características que los delitos comunes establecidos en el ordenamiento penal, pero que están siendo manipulados por elementos de información como es la computadora, que es el arma más común en este tipo de delito. Así mismo, este delito es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando elementos informáticos contra los derechos y libertades de los ciudadanos.

De igual manera, el delito informático se caracteriza por las dificultades que concierne descubrirlo, probarlo, perseguirlo, y en la mayoría de los casos no se denuncian para evitar la alarma social o la deshonra por la falta de seguridad. Las víctimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta enormemente el conocimiento preciso del número de delitos cometidos y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por La Organización para la Cooperación Económica y el Desarrollo (OCDE) a París en mayo de 1983 (citado por Pinarello, s/f, 1), el término delito relacionado con las computadoras lo definen como “cualquier conducta, no ético, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos”.

El departamento de investigación de la Universidad de México (citado por Pinarello, s/f, 1), señala como delitos informáticos que son “todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático”.

Así mismo, para Quiñones (citado por Viega, 1999, 2), los delitos informáticos son “cualquier acto violatorio de la ley penal para cuya comisión exitosa es esencial el conocimiento y utilización de la tecnología de las computadoras”. Para Parker (citado por Viega, 1999, 2) el delito informático es “todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha, o habría podido sufrir una pérdida; y cuyo autor ha, o habría podido obtener un beneficio”.

Además, para la autora Lima (citado por Cruz y Salvador, s/f), los delitos informáticos los nombra como “delitos electrónicos” y en un sentido amplio los define como:

> 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 sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin. (p. 13).

En consecuencia, se puede definir a los delitos informáticos como aquellas conductas típicas, antijurídicas y culpables que lesionan la seguridad informática de los sistemas tecnológicos, dirigidas contra bienes tangibles o intangibles como datos, programas, imágenes y voces almacenados electrónicamente o cualquier otro tipo de bien.

Téllez (1996), establece que los delitos informáticos, presentan algunas características fundamentales que revisten este tipo de acciones:

a. Son conductas criminales de cuello blanco, se pude decir que un determinado número de personas con ciertos conocimientos en la parte informática o con cierto manejo de la computadora y con conocimiento de alguna información en este caso técnicos puede llegar a cometerlas puede ser que se desenvuelva en un campo donde tenga cerca cualquier información que lo beneficie.
b. Son acciones ocupacionales, muchas veces se realizan cuando el sujeto se encuentre trabajando y tiene la facilidad de penetrar en todo tipo de investigación referente a esa actividad que quiere realizar.
c. Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo

de funciones y organizaciones del sistema tecnológico y económico.

d. Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que los realizan.
e. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, todo ello debido a la misma falta de regulación por parte del Derecho.
g. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico. (p. 105).

Por su parte, para los autores Cruz y Salvador (s/f), algunas de las características de los delitos informáticos que a su juicio son las más importantes son:

- Son "delitos de cuello blanco", pues solo un limitado número de personas con conocimientos informáticos puede cometerlos.
- Generan grandes pérdidas de dinero, ya que se realizan en contra de personas o a instituciones pudientes.
- Se realizan en poco tiempo y no es necesaria la presencia física para que pueda llegar a consumarse el delito.
- Son pocas las denuncias debido a la falta de reglamentación por parte del derecho sobre esta materia.
- Su comprobación es muy difícil.
- No siempre se cometen con la intención de perjudicar a otro.
- Últimamente se ha incrementado, por lo que creemos que es necesario que se regule para poder sancionarlo penalmente. (p. 58).

En este sentido, las conductas delictivas informáticas no son delitos nuevos, sino que son los mismos delitos tipificados en el Código Penal

venezolano que tienen una diferencia con estos, la utilización de la computadora como medio o elemento para cometer los delitos. En efecto, la legislación penal regula los delitos contra las personas, la propiedad; como el hurto, la estafa, y otros, pero no desde el punto de vista que una persona los haya cometido utilizando tecnología de información, lo cual es una novedad para el derecho.

A estos efectos, la tecnología puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio fácil para la comisión de actos antijurídicos, en especial de carácter patrimonial, como lo es el fraude, el hurto, entre otros. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Clasificación de los Delitos Informáticos

Los delitos informáticos han sido objeto de diferentes clasificaciones, y se han tenido en cuenta a estos efectos: el perjuicio causado, el papel que el computador desempeñe en la realización del mismo, el modo de actuar, el tipo penal en que se encuadren, clase de actividad que implique según los datos involucrados.

Para la autora Lima (citado por Cruz y Salvador, s/f, 25), clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica, de la siguiente manera:

> Como método; cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
> Como medio; en donde para realizar un delito utilizan una computadora como medio o símbolo.
> Como fin; conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Existen otras clasificaciones de los delitos informáticos, entre ellos, esta el autor Téllez (1996, 106), que los clasifica en atención a dos criterios: como instrumento o medio, o como fin u objetivo.

Como instrumento o medio, se tiene a las "conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito", tales como:

a. Falsificaciones de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b. Variación de los activos y pasivos en la situación contable de las empresas.
c. Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d. "Robo" de tiempo de computadora.
e. Lectura, sustracción o copiado de información confidencial.
f. Modificación de datos tanto en la entrada como en la salida.
g. Aprovechamiento indebido o violación de un código para penetrar a un sistema induciendo instrucciones

inapropiadas (esto es lo que se conoce en el medio como el método del “Caballo de Troya”).

h. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la “técnica de salami”.
i. Uso no autorizado de programa de cómputo.
j. Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios, tales como “consulta a su distribuidor”.
k. Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles “virus informáticos”.
l. Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m. Acceso a áreas informatizadas en forma no autorizada.
n. Intervención en las líneas de comunicación de datos o de teleproceso. (p. 106).

Así mismo, Téllez (1996, 106), clasifica a los delitos informáticos como fin u objetivo a las “conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física”. Algunos ejemplos son los siguientes.

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f. Secuestros de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etcétera). (p. 106).

Por su parte, para el autor Vázquez Perrota (citado por Cruz y Salvador, s/f), los delitos informáticos pueden ser:

1. Crímenes y Delitos: es la división esencial según el autor, este señala que no puede haber infracciones a través de una computadora que conlleve penas de simple policía.
2. Delitos relacionados con los servicios de computadora: trata de la utilización de la computadora como instrumento de producción económica o lucro en actividades diferentes a aquellas para las cuales fue asignado este instrumento tecnológico.
3. Delitos relacionados con los datos o secretos importantes almacenados: como por ejemplo, el espionaje comercial e industrial y la destrucción de data etc.
4. Delitos relacionados con los programas de computadora: como la reproducción ilegal de programas o cualquier otra forma de derecho de autor a través de las computadoras.
5. Delitos de tipo financiero: se trata del robo a través de computadoras. (p. 46).

Así mismo, existen otras clasificaciones de los delitos informáticos, como la de Klaus (citado por Cruz y Salvador, s/f, 113), el cual distingue cuatro grupos como son:

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

- Espionaje: En el ámbito del procesamiento de datos, el “espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin ningún problema a otro soporte”. El espionaje mediante computadoras, según el autor, “no es utilizado únicamente con propósitos económicos por empresas rivales, sino también con finalidades políticas por estados extranjeros”.
- Sabotaje: incluyen “las formas de destrucción y alteración de datos, así como los programas virus. Borran, suprimen o modifican sin autorización funciones o datos de computadoras con intención de obstaculizar el funcionamiento normal del sistema”. Las técnicas que permiten cometer sabotajes informáticos, los más conocidos son los “programas que ingresan al sistema a través de cualquiera de los métodos de acceso de información externa, se instalan, se reproducen y hacen daño”.
- Hurto de tiempo: según el autor, se trata de la “utilización indebida de instalaciones de cómputos por parte de empleados desleales o de extraños, lo que puede ocasionar pérdidas considerables”. Lo que debe corregirse en este caso no consiste tanto en el escaso consumo de energía eléctrica, ni en el mínimo desgaste del equipo de cómputos, sino en el “notable enriquecimiento del autor proveniente del uso indebido de la computadora”.

Otro de los grandes autores que diferencia esta conducta es Baón Ramírez (citado por Cuervo, 1998), explica que dentro de la criminalidad informática denominación que también se le da a los delitos informáticos, se distingue dos grandes grupos de delitos:

a. Un primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así se distinguen los delitos:
- Relativos a la destrucción o sustracción de programas o de material,
- Relativos a la alteración, destrucción o reproducción de datos almacenados,
- Los que se refieren a la utilización indebida de ordenadores,

b. En un segundo grupo se encuadraría la comisión de los delitos más tradicionales como los delitos contra:
- La intimidad,
- La propiedad,
- La propiedad industrial o intelectual,
- La fe pública,
- El buen funcionamiento de la Administración,
- La seguridad exterior e interior del Estado. (p. 7).

De igual manera, el autor Romero Casanova (citado por Cuervo, 1998), analiza las distintas facetas de lo que llama las repercusiones de las nuevas tecnologías de la información en el derecho penal, y de esta forma, divide su análisis en diferentes apartados bajo los títulos de:

- La protección penal de la intimidad e informática,
- La informática como factor criminógeno en el tráfico económico,
- El fraude informático,
- Implicaciones penales de las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética,

- Agresiones a los sistemas o elementos informáticos. (p. 7).

En consecuencia, la información ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien jurídico, dando eminente relevancia jurídico penal por ser posible objeto de conductas delictivas (hacking, craking, fraude informático, espionaje y hurto informático, y otros.), que integran la delincuencia denominada por algunos autores de cuello blanco y por ser instrumento de facilitación, aseguramiento y calificación de los ilícitos tradicionales. Casi todos los delitos, salvo aquellos que requieren una intervención físicamente directa y personal del autor como el abuso sexual con acceso carnal, son susceptibles de ser cometidos mediante el uso de sistemas de tratamiento, almacenamiento y flujo de la información. Se considera que el bien jurídico tutelado en los delitos informáticos es la información en sí misma, en toda su amplitud sin perjuicio de que con su ataque ocasione y tratándose de un interés colectivo, afectar otros bienes jurídicos como la intimidad o la propiedad.

Por otra parte, las Naciones Unidas (citado por el autor Ramírez, 2003, 16), ha diseñado una lista de tipos de delitos informáticos, a fin de evitar que existan facilidades para una actuación delictiva en ciertos países; existiendo una suerte de "paraísos" para la proliferación de estos delitos. Por ello, se

intenta difundir hacia los países que aún no han legislado, intentando armonizar las legislaciones. Así, dividen en tres grandes grupos de delitos:

I. Fraudes cometidos mediante manipulación de computadoras.

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

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

Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude 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, como afirma el autor Ramírez (2003, 12), en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

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

II. Falsificaciones informáticas.

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

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

III. Daños o modificaciones de programas o datos computarizados.

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

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

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

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

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

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

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

considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Regulación en el Derecho Comparado

Internacionalmente puede advertirse una tendencia, acentuada en los últimos años, a legislar sobre la materia. Como afirma el autor Estrada Garavilla (s/f):

> Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la expansión de virus o la interceptación de mensajes informáticos. (p. 12).

Es comprensible que la creación de una ley que regule los delitos cometidos mediante recursos de alta tecnología, sirva para lograr la unificación internacionalmente de una normativa legal, solucionando en gran medida la problemática generada con la expansión que puede tener un delito en internet; viajando por todos los países se tendría que tener en cuenta la jurisdicción, competencia, territorialidad, y otros factores. En cambio, con una ley que se relacione con este tipo de conductas que ayude de esta manera que los países encuentren la solución de poder regular ese delito desde su propia jurisdicción.

En la mayoría de las naciones occidentales, como afirma el autor Estrada Garavilla (s/f), “existen normas similares a los países europeos”. Estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible. En Venezuela la creación de una Ley Especial que regule estos delitos es un paso adelante para la seguridad de los usuarios que pueden utilizar la tecnología por que existe una ley que los respalda al momento de ser víctima de un acto delictivo.

En este sentido, tomando en consideración la Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, a continuación se presenta un resumen de países y sus legislaciones, en las cuales se han adoptado alguna regulación, en lo que respecta a los delitos informáticos:

En Alemania, para hacer frente a la delincuencia informática se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986, y empezó a regir a partir del 1 de agosto de 1986, en la que se contemplan los siguientes delitos:

- Espionaje de datos (artículo 202).
- Estafa informática (artículo 263).
- Falsificación de datos probatorios (artículo 269).
- Alteración de datos (artículo 303): es ilícito cancelar, inutilizar o alterar datos, inclusive la tentativa es punible.

- Sabotaje informático (artículo 303): destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (artículo 266). (Estrada Garavilla, s/f, 13).

Con relación al país de Austria, se reformó el Código Penal el 22 de diciembre de 1987. En este instrumento se contemplan dos modalidades de delitos informáticos:

> Destrucción de datos (artículo 126): en este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
> Estafa informática (artículo 148): en este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión. (Viega, 1999, 10).

En Portugal, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:

> Artículo 35: Utilización de la Informática.
> 1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.
> 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o

vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.
3. Queda prohibida la atribución de un número nacional único a los ciudadanos. (Ramírez, 2003, 27).

Por su parte, en Inglaterra debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento exitoso o no, de alterar datos informáticos es penado hasta con cinco años de prisión o multas. Así mismo, esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen. (Estrada Garavilla, s/f, 13).

En este sentido, para Klein (citado por Pinarello, s/f, 12) afirma que:

Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras. El artículo 3º inciso 2º establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora", y de esa manera:

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

Esta ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación

inglesa. En 1994, fue reformada para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos.

En Holanda, la Ley de Delitos Informáticos del año 1993, sanciona la utilización se servicios de telecomunicaciones evadiendo el pago total o parcial de dicho servicio, la inducción en error a fin de que el afectado suministre información que no aportaría en condiciones normales y la distribución de virus. Con respecto a esta última modalidad delictiva se admiten tanto la forma dolosa como la culposa.

En España, el Código Penal reformado en 1995 contempla una serie de conductas íntimamente vinculadas con la materia informática, es el caso, por ejemplo, de las estafas electrónicas, los daños informáticos, la interceptación de correo electrónico, la publicidad engañosa, la pornografía infantil y la revelación de secretos. Además, en la actualidad se ha propuesto un Anteproyecto de Ley de Comercio Electrónico en el que se plantean severas sanciones pecuniarias para quienes incurran, entre otras conductas, en afección a las comunicaciones comerciales por vía electrónica o se violente el contenido de un contrato celebrado por esa misma vía.

En este contexto, dentro de la legislación española (Viega, 1999, 20), se puede distinguir la aplicación de las siguientes medidas en el ámbito penal:

- Ataques que se producen contra el derecho a la intimidad. (artículos del 197 al 201 del Código Penal).
- Infracciones a la propiedad intelectual a través de la protección de los derechos de autor. (artículos 270 y otros del Código Penal).
- Falsedades, (artículos 386 y siguientes del Código Penal).
- Sabotajes informáticos. Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (artículo 263 y otros del Código Penal).
- Fraudes informáticos. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (artículos 248 y siguientes del Código Penal).
- Amenazas. Realizadas por cualquier medio de comunicación. (artículos 169 y siguientes del Código Penal).
- Calumnias e injurias. Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (artículos 205 y siguientes del Código Penal).
- Pornografía infantil. Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.
- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (artículo 187).
- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (artículo 189).
- El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición). (artículo 189).

- La posesión de dicho material para la realización de dichas conductas. (artículo 189).

En Francia, a través de la Ley sobre el Fraude Informático (Ley número 88-19 de 5 de enero de 1988) se sanciona además de la destrucción dolosa de datos, el acceso fraudulento a un sistema de elaboración de datos, la falsificación o uso de documentos (falsos) informatizados y el sabotaje informático. En este sentido, según el autor Ramírez (2003, 28), en Francia se tipifican los siguientes delitos informáticos:

- Acceso fraudulento a un sistema de elaboración de datos (artículo 462-2): En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (artículo 462-3): En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (artículo 462-4): En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (artículo 462-5): En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (artículo 462-6): En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

En Italia, la descripción y sanción de los delitos informáticos se encuentra contemplada en el Código Penal, instrumento que prevé, entre otros comportamientos, la falsificación informática, el acceso abusivo, el fraude informático, la violación de la correspondencia electrónica y la introducción de virus informáticos, entre otros. A continuación algunos delitos informáticos contemplados en el Código Penal italiano:

a. Acceso Abusivo: Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.
b. Abuso de la calidad de operador de sistemas: Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.
c. Introducción de virus informáticos: Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.
d. Fraude Informático: Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable. Intercepción abusiva: Es un delito que se comete junto con el delito de falsificación, alteración o supresión de

comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.

e. Falsificación informática: Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.
f. Espionaje Informático: Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.
g. Violencia sobre bienes informáticos: Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.
h. Abuso de la detentación o difusión de Códigos de acceso (contraseñas).
i. Violación de correspondencia electrónica, la cual tiene agravantes si causare daños. (Márquez, s/f, 19).

Los Estados Unidos de América se ha incorporado a esa tendencia regulatoria. Este país “adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986” (Manson, 1999, 13).

Con la finalidad de eliminar los argumentos técnicos acerca de qué es y que no es un virus, un gusano, un caballo de troya y en que difieren de los virus, “la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 a, 5, A)”. Esta nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. (Manson, 1999, 13).

Esta Acta Federal de 1994, diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

> Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
> Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión. (Manson, 1999, 13).

En efecto, esta nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro, a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la

nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

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

De igual manera, el Estado de California adoptó en 1992 la Ley de Privacidad en la que también se contemplan delitos informáticos. En el mismo sentido, la legislación del Estado de Florida.

Con respecto a Latinoamérica, Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Así mismo, dentro de esas consideraciones se encuentran los virus.

En este sentido, según el autor Ramírez (2003, 28), los primeros cuatro artículos menciona:

> Artículo 1: El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
> Artículo 2: El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
> Artículo 3: El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.
> Artículo 4: El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

En Argentina aún no existe una legislación especial que sancione los delitos informáticos, sin embargo, mediante el Decreto 165/94 del 8 de febrero de 1994 se agrega a la lista de comportamientos referidos a la propiedad intelectual la protección a las obras, bases de datos y software.

Por su parte Colombia, sancionó el 18 de agosto de 1999 la Ley 527, en la que si bien no se contemplan disposiciones penales, se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

En Perú, la Ley N° 27309 del 15 de julio de 2000, incorporó los delitos informáticos al Código Penal, tipificando la utilización o ingreso indebido a una base de datos, sistema o red de computadoras o cualquier parte de la misma, la interferencia, interceptación, acceso o copia de información en tránsito o contenida en una base de datos. De la misma manera se describió la utilización, ingreso o interferencia indebida de una base de datos, sistema, red o programas de computación con el fin de alterarlos, dañarlos o destruirlos.

En este contexto, según la autora Viega (1999, 13), el ordenamiento jurídico peruano tipifica los siguientes delitos informáticos:

- Delito de violación a la intimidad (artículo 154 del Código Penal).
- Delito de hurto calificado por transferencia electrónica de fondos (artículo 186 segundo párrafo numeral 3 del Código Penal, modificado por Ley 16.319).
- Delitos contra los derechos de autor (artículo 216 Código Penal).
- Delito de falsificación de documentos informáticos (Decreto Legislativo 681, artículo 19, artículo 427 del Código Penal).
- Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (artículo 198, inciso 8 del Código Penal).
- Delito de daños aplicable al hardware (artículo 205 del Código Penal).

En México, específicamente en el estado de Sinaloa, también se ha regulado sobre los delitos informáticos. En esta legislación, dirigida

básicamente a proteger el patrimonio, se sanciona el acceso a una base de datos con el fin de defraudar u obtener información y la interceptación o destrucción de datos. A estos efectos, el Código Penal del Estado de Sinaloa, en el título décimo de los delitos contra la propiedad, en el capítulo quinto de los delitos informáticos, tipifica lo siguiente:

> Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:
> I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

Así mismo, en México otra regulación vinculada con la materia, se encuentra en la Ley Federal de Derechos de Autor donde se protege, bajo la amenaza de sanción, los programas de computación, las bases de datos y los derechos autorales relacionados con ambos. De la misma manera, el Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de fuero federal, sanciona como un delito contra la propiedad intelectual el uso de programas de virus.

De la relación anterior se deduce que Venezuela se incorporó a través de la promulgación de la Ley Especial contra los Delitos Informáticos en octubre del 2001, a este movimiento internacional regulador de conductas atentatorias contra diversos bienes jurídicos (propiedad, honor, fe pública, intimidad, y otros) perpetradas a través de sistemas que utilicen tecnologías de información.

Ley Especial contra los Delitos Informáticos

La modificación parcial del Código Penal puede ser algo complejo y un riesgo por la posible desnaturalización de su estructura. Es así como se consideró la necesidad de elaborar un instrumento especial destinado a regular los delitos informáticos, por ser este último un procedimiento más expedito. No obstante, se debió hacer una regulación completa y desarrollada recogiendo las más modernas variantes que podrían contemplarse como delictivas, a fin de que el instrumento diseñado, dentro de una tendencia codificadora en un futuro, pudiere pasar a conformar un título o capítulo del Código Penal. (Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, s/f, 5).

La Ley Especial contra los Delitos Informáticos aprovechó la experiencia del derecho comparado vigente y en proceso y,

fundamentalmente, las modalidades dadas a conocer por Naciones Unidas, como los fraudes cometidos mediante manipulación de computadoras, las falsificaciones informáticas y los daños o modificaciones de programas de datos computarizados.

Se afirma que la Ley Especial contra los Delitos Informáticos es del tipo amplio porque tiende a la protección integral de los sistemas que utilicen tecnologías de información, previniendo y sancionando los delitos que puedan llegar a cometerse contra esos sistemas o cualquiera de sus componentes, así como el uso de dichas tecnología. Es decir, que el fin de la Ley, es la prevención y punición de los delitos informáticos, según lo que la propia legislación define por tales, no sólo por la solución sino también por el medio empleado para cometer el delito. (Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, s/f, 6).

Esta Ley venezolana esta inmersa en dicha técnica legislativa y por lo tanto, en su artículo 2 establece qué interpretación debe dársele a sus distintos términos. Define en primer lugar, lo que debe entenderse por tecnologías de la información, para luego fijar los distintos conceptos empleados en su articulado; desde sistema, data e información, hasta firmware, software, programa, virus, y otros. Estos delitos, en un porcentaje muy alto, se cometen fuera de las fronteras del país, puesto que aún cuando

el lugar de comisión lo sea dentro de las fronteras del país, muchas veces los efectos tendrán lugar en otro u otros países, dispone en el artículo 3 que cuando dentro del territorio de la República se hubieran producido efectos del hecho punible y el responsable no hubiera sido juzgado por un tribunal extranjero se aplicará la ley venezolana.

La Ley consta de cuatro títulos. En un primer título contempla las disposiciones generales, en las que se precisa el objeto de la ley, se contemplan algunas definiciones básicas dado el carácter técnico de la materia.

Como lo han hecho otras leyes que rigen la materia, en los últimos años se ha considerado, en materia de legislación informática, que sea la propia ley la que defina sus conceptos, términos y alcances, ya que en la mayoría son términos en ingles que para la interpretación seria muy difícil. Así la ley permitió dejar los que son imposibles de traducir e incorporar en la misma ley sus significados, como otras palabras que son también conceptualizadas de una manera rápida para que las personas que hacen uso de esta norma puedan entenderla y que sea en un lenguaje universal.

La Exposición de Motivos de la Ley afirma que actualmente no es posible contar con una definición de delitos informáticos, pues cada país de

acuerdo a sus realidades, ha formulado un concepto en el cual de ordinario se procura incluir nuevas modalidades delictivas o describir en términos más actuales comportamientos tradicionales que, en razón del medio de comisión empleado adquieren la condición de informáticos. Sin embargo, al describirse el objeto de la ley, en el artículo 1º se está formulando un concepto de delito informático en términos bastante actualizados, al indicar la descripción, en términos generales, de las conductas que se pretende prevenir y sancionar en la Ley y al remitir al vocablo tecnologías de información el contenido global de la informática con todos sus componentes.

De este modo, la Ley en su artículo 1º establece:

> Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

En el título II se describen los delitos informáticos. Para la sanción de las conductas allí descritas se adopta el sistema binario, esto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última, se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en la Ley, afectan la viabilidad del sistema económico el cual se sustenta, fundamentalmente, en la confiabilidad de las

operaciones. (Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, s/f, 6).

Partiendo de la consideración anterior, la Ley procura agrupar en seis capítulos en el título II, una amplia gama de comportamientos discriminados en función del bien jurídico que, a través del uso de medios que utilizan tecnologías de información, resulta vulnerado.

En efecto, en el capítulo I se describen una serie de conductas que atentan contra los sistemas que utilizan tecnologías de información, tales como el acceso indebido, el sabotaje o daños a sistemas, el favorecimiento culposo del sabotaje o daño, el espionaje informático, la falsificación de documentos, entre otros.

El capítulo II se dedica a describir algunas conductas en las que los sistemas que utilizan tecnologías de información son utilizados como medio para afectar la propiedad. Entre ellos, el artículo 13 contempla el delito de hurto. En este caso es el propio autor, quien a través del acceso a sistemas que utilizan tecnologías de información, saca de la esfera de dominio de la víctima los bienes tangibles (como el dinero en efectivo) o intangibles (tal es el caso de los créditos o de bonos desmaterializados). La norma exige la concurrencia de un elemento subjetivo del tipo como lo es el ánimo de lucro.

Si bien la descripción típica del hurto presenta algunas similitudes con el de fraude (artículo 14), ambos se diferencian en que en el segundo son las instrucciones falsas o fraudulentas del autor las que, al alterar o modificar la secuencia lógica de los sistemas, dan lugar a que se produzca una operación que no estaba autorizada con la consecuencia de la obtención de un activo patrimonial en perjuicio ajeno.

El artículo 15 prevé un tipo especial de fraude perpetrado mediante la utilización de una tarjeta inteligente ajena o un instrumento destinado a los mismos fines para la obtención indebida de efectos, bienes o servicios con evasión del pago respectivo.

En los artículos 16 y 17 se sancionan, respectivamente, la creación, grabación, duplicación o eliminación de la data o información contenidas en una tarjeta inteligente o instrumentos análogos y la apropiación de tales instrumentos con el fin de usarlos o transferirlos a un tercero. En ambos casos, se sanciona a quien sin haber tomado parte en el hecho principal, realice cualquier tipo de intermediación con esas tarjetas o las adquiera o reciba. También se sanciona (artículo 18) la conducta de quien, a sabiendas de su procedencia ilícita, provee dinero, efectos, bienes o servicios al portador del instrumento. (Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, s/f, 8).

En el capítulo III describe algunos comportamientos en los que se afecta la privacidad de las personas y de las comunicaciones a través de sistemas que utilizan tecnologías de información. Las conductas contempladas en los artículos 20 (violación de la privacidad de la data o información de carácter personal) y 22 (revelación indebida de data o información de carácter personal) se diferencian del delito de espionaje informático propuesto en el artículo 11, en que en este último lo que se protege es la seguridad del sistema que contiene la data o información sea o no de carácter personal, mientras que en los dos primeros se tutela la data o información “personales” o sobre las cuales se tenga un interés legítimo.

Por su parte, el artículo 21 resguarda la privacidad de las comunicaciones garantizada en el artículo 48 de la Constitución, en la medida en que resulte vulnerada por el uso de tecnologías de información. Con esta regulación se actualiza el concepto de correspondencia, incluyéndose la intercepción de e-mails o cualquier otro mensaje de datos transmitido por un sistema de comunicaciones.

Se incluyó la difusión y exhibición de material pornográfico a niños o adolescentes y su utilización con fines exhibicionistas o pornográficos mediante el uso de tecnologías de información (Capítulo IV) dada la ausencia

de regulación de tales comportamientos en la Ley Orgánica para la Protección del Niño y del Adolescente.

En el Capítulo V se describen dos comportamientos: El artículo 25 sanciona la reproducción, copia, modificación distribución o divulgación de programas informáticos (software) u otras obras del intelecto, hecho éste que en la actualidad genera grandes pérdidas económicas para los propietarios legítimos. Ahora bien, en el documento de Naciones Unidas sobre los tipos de delitos informáticos se asienta que este no es un delito de esa naturaleza debido a que el bien jurídico a tutelar es la propiedad intelectual, no obstante, por afectar programas informáticos y aparecer dentro del elenco de comportamientos reconocidos por Naciones Unidas, se estimó pertinente su inclusión en la Ley. En razón de que se exige como un elemento subjetivo del tipo el fin de lucro, se propone como un delito contra el orden económico. (Exposición de Motivos de la Ley Especial contra los Delitos Informáticos, s/f, 6).

Así mismo, y sin perjuicio de la comisión de un delito más grave, en el artículo 26 se sanciona la oferta engañosa de bienes o servicios mediante el uso de tecnologías de información en la medida que pueda causar algún perjuicio a los consumidores.

La descripción como tipos agravados que se hace en el capítulo II de la Ley, en relación con algunas previsiones similares contempladas en el Código Penal y otras leyes, obedece a la peligrosidad que reviste el uso de sistemas que utilizan tecnología de información para la comisión de delitos, más aún cuando se trata de una delincuencia de ordinario especializada, pues en la mayoría de los casos el autor tiene habilidad en el manejo de medios informáticos, situación que inclusive puede ofrecer ventajas para intentar hacer desaparecer cualquier evidencia del ilícito cometido.

Se incluye en el artículo 31 un supuesto de indemnización civil especial, que impone al juez la obligación de ordenar en la sentencia de condena por alguno de los delitos que cause un perjuicio patrimonial a la víctima, el pago de una suma de dinero que aquél deberá fijar con el auxilio de expertos. Esta previsión, que persigue concretar uno de los objetivos del proceso penal, cual es la reparación del daño causado a la víctima (artículo 30 de la Constitución y 120 del Código Orgánico Procesal Penal) ofrece una respuesta inmediata a quien ha resultado afectado por alguno de esos delitos, al no forzarle al ejercicio de una acción civil a fin de obtener una reparación por el daño causado.

El título III, contentivo de las disposiciones comunes, comprende las circunstancias agravantes de la responsabilidad penal por los delitos que se

proponen y el régimen de imposición de las penas accesorias. Así mismo, en el título IV se contemplan las disposiciones finales referidas a la vigencia de la ley y la derogatoria de las normas conflictivas contempladas en otros instrumentos legales.

De acuerdo con los razonamientos que se han venido realizando con la descripción del marco jurídico de los delitos informáticos, se concluye que son acciones u omisiones, típicas, antijurídicas y culpables, realizado por el sujeto activo a través del uso indebido de la tecnología de información, obteniendo un beneficio para sí o para un tercero, en perjuicio de la víctima. Estos hechos ilícitos se encuentran tipificados en la Ley Especial contra los Delitos Informáticos y presentan las mismas características que los delitos comunes establecidos en el ordenamiento jurídico penal, pero se han llevado a cabo utilizando elementos informáticos y/o usando indebidamente las tecnologías de información, vulnerando derechos y libertades de las víctimas por parte del agente. En el siguiente Capítulo se explica las características del sujeto activo de los delitos informáticos, así como la descripción de sus comportamientos, todo con el fin de comprender las particularidades que presenta y para la cual el presente estudio los denomina delincuentes cibernéticos.

CAPÍTULO III

LOS DELINCUENTES CIBERNÉTICOS

En los delitos informáticos, entre ellos el delito de fraude de acuerdo con la Ley Especial contra los Delitos Informáticos, el sujeto activo presenta características diferentes a los delincuentes tradicionales, en el presente Capítulo se analiza al agente que realiza esta clase de delitos, así como se hace una descripción de comportamientos negativos efectuados mediante las tecnologías informáticas.

En la medida en que se va ampliando el internet, así mismo va aumentando el uso indebido de la misma. Es así como surgen los denominados delincuentes cibernéticos, que no son delincuentes comunes, sino sujetos con conocimiento para manejar los sistemas informáticos. Se pasean por el ciberespacio, incurriendo en delitos tales como el acceso indebido, el espionaje informático, el fraude, el sabotaje o daño a sistemas, entre otros.

Los delincuentes cibernéticos son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar

pista o rastro alguno. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en paraísos informáticos, es decir, en países que carecen de leyes o experiencia para su persecución.

Dentro de los delitos informáticos es necesario tomar en cuenta las características de los delincuentes, los cuales son muy diferentes a los delincuentes tradicionales, son personas con conocimiento en el área de la informática y que tienen acceso a la información; están dispuestos a dañar o sólo son personas que tienen un leve conocimiento en computadoras y agreden los sistemas de datos de otras personas.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas (ONU), en la prevención y control de delitos informáticos, (citado por Ramírez, 2003, 1), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Así mismo, otro reciente estudio realizado por la ONU en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y sólo el 23% a la actividad delictiva externa.

A estos efectos, la autora Dra. Viega (1999), afirma que no se esta hablando de delincuentes comunes. Los sujetos activos 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 debemos 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. (p. 3).

Así mismo, algunos autores como Téllez (1996), ya han catalogado o diferenciado algunos de los delincuentes informáticos, y establece que los delitos informáticos presentan las siguientes características principales:

a. Son conductas “criminógenas de cuello blanco (white collar crimes)”, se refiere a un determinado número de personas con ciertos conocimientos en la informática o con cierto manejo de la computadora y con conocimiento de alguna información, en este caso técnicos, que pueden llegar a cometerlas porque se desenvuelve en un campo donde tenga cerca cualquier información que lo beneficie.
b. Son “acciones ocupacionales”, muchas veces se realizan cuando el sujeto está trabajando y tiene la facilidad de penetrar y obtener todo tipo de información referente a esa actividad que quiere realizar. (p.104).

En este sentido, desde 1943 se ha catalogado a los delitos informáticos como "delitos de Cuello Blanco", por el criminólogo norteamericano Edwin Sütherland (Fernández, 2001, 25). En aquella etapa se le clasificaba de tal manera, porque se requería de un determinado conocimiento y posición ocupacional para poder llevar acabo este actuar, y con ello un cierto status socio-económico; en cambio actualmente cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente cibernético. Actualmente se ha llegado a denominar como "Delito de Cuello Dorado" por la “gran vistosidad con que se maneja esta figura delictiva, y la gran relevancia que tiene su proceder en comparación con las restantes figuras delictivas que son manejadas por los ordenamientos penales, por sus dañinas consecuencias”. (Arregoitia, 2003, 2).

Así mismo, este criminólogo estadounidense (citado por Landaverde, Soto y Torres, 2000, 56), asegura que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos se tiene: "El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja

educación, ni por poca inteligencia, ni por inestabilidad emocional". (Manson, 1999, 5).

Por su parte, para el autor Bloom Becker, J., director del “Nacional Center for Computer Crime” (citado por Fernández, 2001, 25), habla de ocho ambientes para delitos por computador, demuestra que los individuos propensos a cometer esta clase de faltas son generalmente personas inteligentes, ansiosas, muy motivadas, valerosas, aventureras, calificadas y deseosas de aceptar estos retos técnicos. Tienen exactamente las características que lo hacen altamente deseables como empleados para procesamiento de datos. La actitud que prevalece parece ser la de que cualquier adicción, está bien siempre y cuando promueva la economía. Esta premisa es necesaria para entender la actitud juguetona hacia los delitos por computador, lograr que los estudiantes, los trabajadores y aficionados se “enganchen a los computadores es la mayor meta de un gran sector de la economía norteamericana y de la mayoría de las potencias del mundo libre”. (Fernández, 2001, 25).

De igual manera, otro tipo de ambientes para cometer delitos por computador, son los que seducidos por la oportunidad, como lo afirma la autora Fernández (2001):

> Es el típico caso de los engañadores de datos, como el tipo más común de delincuentes por computador, se trata de personas que cometen fraudes cambiando los datos que serán procesados. Mientras haya mejor seguridad menor será la oportunidad para el delito. (p. 26).

En relación con el tipo de comportamiento que puede realizar el delincuente informático, según Hance (citado por Manson, 1999), en su libro "Leyes y Negocios en Internet", considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

> a. Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.
> b. Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre se es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).
> c. Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él. (p. 6).

En efecto, el delincuente cibernético tiene conductas que merecen ser amonestadas siempre adecuándose a las normas que regulan tales faltas,

como el Código Penal y la Ley Especial. Estos delitos tienen por instrumento o elementos de destreza a la informática, que están relacionadas significativamente, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

En el mismo orden de ideas, los criminales informáticos tienden a realizar un tipo de actividades que reuniendo los requisitos que determinan la significación de delito, son llevados a cabo utilizando un elemento informático como simple herramienta para cometer una conducta negativa, o vulnerando los derechos de las personas o de su bien jurídico.

El abuso informático se refleja en el momento en que las personas le dan otra finalidad a las computadoras, comportándose de una manera ilegal o contraria a las normas que regulan la delincuencia informática. En Venezuela se promulgó la Ley contra los Delitos Informáticos, toda vez que era necesario llevar a cabo una armonización más adecuada de la legislación penal, entre las personas que eran víctima de estas conductas y el Estado, como ente que regula lo concerniente a la seguridad de todos los ciudadanos; y además de tener buenas relaciones con todos los países respecto a los hechos ilícitos relacionados con las tecnologías de información.

A estos efectos, la Ley Especial contra los Delitos Informáticos adopta una serie de disposiciones generales aplicables sólo a esta materia, dadas las particularidades del delincuente informático. Así mismo, afirma la exposición de motivos de la Ley, que es “un delincuente de ordinario solitario, sofisticado, que puede actuar con dolo directo o eventual en la medida en que dirija su acción a la afección del bien que se tutela o que previsto el posible resultado lo acepte”. Tal Ley contempla además la inclusión de comportamientos culposos. (s/f, 5).

Descripción de Comportamientos

1. Hacker

Los hackers suelen ser expertos en el uso de las computadoras y por lo general rehúsan hacer un uso delictivo de sus conocimientos, aunque no tienen dificultad en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada, siempre con la finalidad de investigar las defensas de estos sistemas, sus lados débiles y adjudicarse el mérito de haber logrado burlar a sus administradores. Muchos de ellos dan a conocer a sus víctimas las fallas encontradas en la seguridad e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas web de poder hacerlo.

Para la presente investigación, el hacker es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas.

El término de hacker en castellano significa "cortador" (Ramírez, 2003, 3). Las incursiones de los hackers son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión.

En efecto, el hacker es fanático de la informática, generalmente joven, que tan sólo con un ordenador personal, un modem, gran paciencia e imaginación es capaz de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, “saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla”. (Ramírez, 2003, 3).

De igual manera, para el autor Ramírez (2003), considera que hay dos tipos de hackers, que son:

1. Los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad;

2. Los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables. (p. 5).

Por su parte, el jurista chileno Manzur (citado por Carrion, 2002), señala que el hacking puede clasificarse en directo o indirecto. El hacking propiamente dicho, explica este autor es:

> Un delito informático que consiste en 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, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor. La voluntad de divertirse generalmente se traduce en paseos por el sistema haciendo alarde de la intromisión. Es lo que se ha llamado “joy riding”, o paseos de diversión. (p. 16).

A estos efectos, como características de esta clase de hacking, se encuentra que el hacker es una persona experta en materias informáticas y generalmente sus edades están comprendidas entre los 15 y los 25 años. Es por ello que esta delincuencia se ha nominado "short pants crimes", es decir, crímenes en pantalones cortos; su motivación no es la de causar un daño, sino que se trata de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Esta clase de hacking no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

En relación al hacking indirecto, el Dr. Manzur (citado por Carrion, 2002, 17), considera que es el medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje. Señala que en el caso del hacking indirecto, “el ánimo del delincuente está determinado por su intención de dañar, de defraudar, de espiar, entre otros, entendiendo que no desaparece el delito de acceso indebido, dándose la hipótesis del concurso ideal o formal de delitos”.

En otras palabras, el hacker puede actuar solo o en grupo, pero generalmente cuando se reúnen, es para intercambiar información, no para que los demás miembros le enseñen a hackear. Comúnmente los hackers bajan todo lo que pueden de internet sobre vulnerabilidad, sistemas operativos, ingeniería social, phreaking, (programación), inventan un nick (sobrenombre), para que los demás los reconozcan.

Así mismo, el hacking es una conducta que se refiere al acceso no autorizado que realiza el sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido. La finalidad del actuar del agente (hacker) puede ser diversa, ya que buscará a través de ella conocer, alterar o destruir la información contenida en el sistema ya sea parcial o totalmente.

2. Cracker

Los crackers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. Según la autora Arregoitia (2003), tiene dos variantes:

- El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.
- El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia. (p.2).

De igual manera, el cracker es aquel hacker fascinado por su capacidad de romper sistemas y software, se dedica única y exclusivamente a crackear sistemas. Obviamente, que antes que llegar a ser un cracker se debe ser un buen hacker. Es importante destacar que no todos los hackers se convierten en crackers.

Los crackers son un dolor de cabeza para muchos ingenieros informáticos, debido a que este tipo de persona se adentra en los sistemas informáticos, pero para causar daño.

Por su parte, para el autor Paredes (2003, 6), cracker es aquella “persona que haciendo gala de grandes conocimientos sobre computación y con un obsceno propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo”.

Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente, puedan lograr vulnerar claves de accesos de los sistemas.

En efecto, para los grandes fabricantes de sistemas y la prensa, este grupo es el más rebelde de todos, porque siempre encuentran el modo de romper una protección. Pero el verdadero problema radica en que esta rotura es difundida normalmente a través de la red para conocimientos de otros; y en este aspecto comparten la idea y la filosofía de los hackers. En la actualidad es habitual ver como se muestran los cracks de la mayoría de software de forma gratuita a través de Internet.

Cabe destacar que crack es sinónimo de rotura, y por lo tanto, cubre buena parte de la programación de software y hardware. Un cracker debe

conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

En este contexto, como su nombre lo indica, se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos en el mercado negro. Estos crean códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información, ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos.

Las herramientas de los crackers, según la autora Arregoitia (2003), suelen ser:

> Potentes editores hexadecimales y debuger's mediante los cuales "desmontonan" los programas, lo que se conoce como ingeniería inversa, hasta llegar a las protecciones que son generalmente utilidades de tiempo que se representan en el reloj interno de la máquina o en el sistema operativo para desencadenar una cuenta regresiva que descontará los días posibles a usar el software hasta que el mismo caduque y el usuario este obligado a pagarlo o renunciar a él. (p. 2).

Los crackers pueden ser empleados rencorosos o frustrados de alguna compañía que tengan fines maliciosos o de venganza en contra de alguna empresa o persona, o pueden ser estudiantes que quieran demostrar sus habilidades pero de la manera equivocada o simplemente personas que lo hacen sólo por diversión.

3. Phreaker

El phreaker es el especialista en telefonía (cracker de teléfono). Como afirma el autor Morales (s/f, 9), “un phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles”. En la actualidad, también poseen conocimientos de tarjetas prepago, debido a su empleo constante por parte de la telefonía celular. Así mismo, un buen phreaker debe tener también amplios conocimientos sobre informática.

El prhreaking se convirtió en una actividad de uso común cuando se “publicaron las aventuras de John Draper, en un artículo de la revista Esquire, en 1971” (Merlat, Paz y otros, 1999, 2). Se trata de una forma de evitar los mecanismos de facturación de las compañías telefónicas. Logran llamar a cualquier parte del mundo sin costo prácticamente. En muchos casos, también evita, o al menos inhibe, la posibilidad de que puedan trazar el camino de la llamada hasta su origen, evitando así la posibilidad de ser atrapado.

Sin embargo, para la mayor parte de los miembros del submundo informático, esta actividad es simplemente una herramienta para poder realizar llamadas de larga distancia sin tener que pagar enormes facturas. La cantidad de personas que se consideran phreakers, contrariamente a lo que

sucede con los hackers, es relativamente pequeña. Pero aquellos que si se consideran phreakers lo hacen para explorar el sistema telefónico.

En este contexto, para la presente investigación el phreaker es una persona con amplios conocimientos de telefonía, que puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares.

En este sentido destaca Paredes (2003, 3), “construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello”. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

En efecto, los phreakers buscan burlar la protección de las redes públicas y corporativas de telefonía, con la finalidad de poner a prueba conocimientos y habilidades (en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores.

Dentro de las actuales manifestaciones de phreaking, según la autora Arregoitia (2003, 2), se tienen:

a. Shoulder-surfing: esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.
b. Call-sell operations: el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas.
c. Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección.
d. Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los

usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:

- Utilizar los códigos de transferencia de mensajería automática manejados por el sistema.
- Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

e. Monitoreo pasivo: por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.

4. Lammers

Los lammers son aquellas personas que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos hackers que los desprecian por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría. Como lo afirma Paredes (2003):

> Un lammer es simple y sencillamente un tonto de la informática, una persona que se siente Hacker por haber bajado de Internet el netbus, alguien a quien le guste bajar virus de la red e instalarlos en la PC de sus amigos, aunque

> mas bien podría decírsele como un cracker de pésima calidad; en general alguien que cree que tiene muchos conocimientos de informática y programación, pero no tiene ni la más mínima idea de ello. (p. 7).

5. Gurús

Los gurús son maestros y enseñan a los futuros hackers. Normalmente se trata de personas adultas, porque la mayoría de los hackers son personas jóvenes. Tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma, para enseñar o sacar de cualquier duda al joven hacker. El gurú no esta activo, pero absorbe conocimientos porque sigue practicando, pero para conocimientos propios y sólo enseña las técnicas más básicas. (Arregoitia, 2003, 2).

6. Virucker

Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir virus y destruir, alterar y/o inutilizar la información contenida.

Por su parte, para el autor Ramírez (2003, 8), existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para

instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

7. Pirata Informático

El pirata informático es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor. Se considera también piratería descargar música de Internet y grabarla en un disco compacto para escucharla. Existen programas donde se puede descargar gratuitamente el software para descargar la música gratis.

8. Bucaneros

Los bucaneros son como los comerciantes. Es decir, venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la red. Como lo afirma el autor Morales (s/f, 7), “sólo se dedican a explotar este tipo de tarjetas para canales de pago que los hackers o crackers crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero si de negocios. El bucanero compra al copyhacker y revende el producto bajo un nombre

comercial”. En realidad es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

9. Newbie

Es una traducción literal de novato. Es alguien que empieza a partir de una web basada en hacking. Inicialmente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página web para seguir las instrucciones de nuevo. Es el típico sujeto simple y nada peligroso.

10. Trashing

Esta conducta tiene la particularidad de haber sido asociada recientemente con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social. (Arregoitia, 2003, 2).

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

Para dar por terminado el presente Capítulo, existen una diversidad de delincuentes informáticos, los cuales pueden transgredir, dañar, ingresar sin autorización a sistemas informatizados, o pueden hacer un uso indebido de las tecnologías de información, así como pueden interceptar información o datos personales que afectan a derechos individuales o patrimoniales de las víctimas. En el siguiente Capítulo se analiza el delito de estafa de acuerdo al Código Penal venezolano, con el fin de comprender este tipo penal el cual es diferente al delito de fraude objeto de este estudio, así mismo la acción que ejecuta el sujeto activo del delito de estafa es igualmente diferente al que se ejecuta en el delito de fraude informático.

CAPÍTULO IV

EL DELITO DE ESTAFA DE ACUERDO CON EL CÓDIGO PENAL DE VENEZUELA

En el presente Capítulo se determinan las diferentes características del delito de estafa contemplado en el Código Penal venezolano, a través del estudio de su concepto y regulación, abordando brevemente sus antecedentes históricos, así como el análisis dogmático que presenta este tipo penal.

El Código Penal venezolano establece el delito de estafa en el artículo 464, que dispone lo siguiente:

> El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco anos.

El término estafa es conocido en varios países con diferentes acepciones. En México la estafa es conocida como "fraude", en Italia se conoce como "truffa" y en Francia como "escroquerie".

Consideran algunos autores, tales como Cruz y Salvador (s/f, 3), que la diversidad de medios o formas que el delito de estafa puede presentar es una de las principales dificultades que se encuentran a la hora de definir al

mismo. La doctrina coincide en que el engaño es el elemento que diferencia este delito de los demás delitos contra la propiedad. Es así, porque en la estafa no hay violencia como la puede haber en el robo, sino que es un delito en que el sujeto activo actúa con inteligencia y astucia de entre todas las modalidades que puede asumir para engañar a la víctima y hacerse de un provecho injusto para sí o un tercero.

Por su parte, considera Grisanti (1989), que no es difícil definir la estafa. En el “Derecho Penal moderno no hay delitos indefinidos, ni por tanto indefinibles”. (p. 299).

Así mismo, el mencionado autor cita la definición de Antón Oneca (1989), el cual establece que la estafa es:

> Una conducta engañosa, con ánimo de lucro injusto, propio u ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero. (p. 299).

El diccionario de vocabulario jurídico de Capitánt (1930), define la estafa como:

> El delito consistente en apropiarse en perjuicio ajeno del dinero, títulos u otros muebles corporales que el agente se ha hecho remitir o entregar usando de falsos nombres o falsas calidades, o empleando maniobras fraudulentas para persuadir la existencia de falsas empresas o de un poder o crédito imaginario, o para suscitar la esperanza o temor de un

> suceso, accidente o cualquier otro acontecimiento quimérico. (p. 264).

A su vez, Balestra, (citado por Grisanti, 1989, 300), define la estafa del siguiente modo: “una disposición de carácter patrimonial perjudicial, viciada en su motivación por el error que provoca el ardid o el engaño del sujeto activo, que persigue el logro de un beneficio indebido para sí o para un tercero”.

El Dr. Grisanti (1989, 300), considera que la estafa “entraña una lesión patrimonial causada por fraude. La estafa es un fraude. El fraude por antonomasia...”.

Ramírez (1994, 160), define al fraude como “una sustracción hecha maliciosamente a las normas de la ley o del contrato en perjuicio de alguien. Es una de las causas de nulidad de los actos jurídicos”.

En el Diccionario Espasa (s/f), define al fraude, como equivalente a engaño, que consiste en:

> Cualquier falta de verdad debida simulación entre lo que se piensa o se dice o se hace creer, instigando o induciendo a otra persona a actuar en la forma que interesa, o en la falta de verdad en lo que se dice o se hace. (p. 434).

A estos efectos, para la presente investigación, el delito de estafa es una disposición patrimonial perjudicial producida por error, el cual ha sido logrado mediante ardid o engaño del sujeto activo, tendiente a obtener un beneficio indebido para sí o para un tercero.

Tal como se ha visto, en el delito de estafa el perjuicio consiste en lograr que la víctima haga una disposición patrimonial, a raíz de que el agente la ha hecho caer en error mediante artificios o sorprendiendo su buena fe.

En definitiva, dando una caracterización general, el delito de estafa se produce cuando la cosa que se quiere despojar, ya sea en beneficio propio o en el de un tercero, se ha conseguido con el consentimiento del propietario o dueño, mediante artificios que engañaron a éste sorprendiendo su buena fe y viciando su consentimiento.

Antecedentes Históricos

Como antecedente histórico del delito de estafa se puede ubicar en el Derecho Romano, el llamado “crimen stellionatus”, el cual aparece según el autor Arteaga (1983, 16), en la “época de Antonio Pío, y en Severos (principios del siglo III d. c.), para reprimir hechos de fraude que no

constituían ni hurto ni falsedades". Se trata de un crimen extraordinario cuyo conocimiento correspondían a los funcionarios imperiales, y que no era considerado por ley alguna.

El concepto de stellionatus, para el Derecho Romano era sumamente vago e impreciso. Se comprendía bajo este título una serie de casos de fraude que no encuadraban en otras figuras delictivas y correspondía al pretor decidir si había o no materia suficiente para proceder criminalmente.

En las Siete Partidas, no se encuentra una alusión directa de lo que se conoce actualmente como estafa. Sin embargo en la Séptima Partida, título XVI, bajo el enunciado "de los engaños malos o buenos, e de los barajadores", han quedado descritos interesantes conceptos de gran valor para el estudio del delito de estafa.

En forma general, señalan Las Partidas los modos o maneras en que puede llevarse a cabo los engaños, señalando que, si bien son múltiples las formas de engañar que tienen los hombres, dos son los principales modos: "por palabras engañosas o arteras, o por medio del silencio engañoso o las palabras encubiertas" (Arteaga, 1983, 18). De esta forma, ya se alude en Las Partidas a la simulación o disimulación como constitutivos de la acción del moderno delito de estafa, y se acepta el engaño por omisión, actualmente

tan debatido en la doctrina penal por lo que atañe a su reconocimiento entre los medios para configurar este tipo de delito.

En los siglos posteriores, permanece la confusión doctrinal y la falta de precisión legal, hasta comienzos del siglo XIX, con la promulgación del Código Penal francés de 1810.

En efecto, el código napoleónico tiene el gran mérito de haber sentado las bases de la moderna estructuración del delito de estafa, distinguiendo claramente la llamada escroquerie de otras figuras delictivas. De este código se inspiraron otros códigos del siglo XIX, los cuales, prácticamente, se limitaron a seguir el criterio napoleónico, con variantes accidentales.

El Código Penal austríaco, promulgado el 27 de mayo de 1852 (citado por Arteaga, 1983), reviste una gran importancia, por haber sido el indicador del sistema que establece una definición genérica de estafa. Como lo señala en el artículo 197:

> El que, mediante maniobras fraudulentas o promesas, induce a un tercero en error o de este modo explota el error o la ignorancia de éste, con el propósito de causar daño a los bienes u toros derechos, ya fueren del Estado, de un Municipio o de cualquier otra persona, comete una estafa, haya obrado por interés o por pasión, con el objeto de favorecer a alguien violando la ley, o bien movido por otro móvil cualquiera". (p. 23).

Así mismo, el Código Penal alemán promulgado en 1871 (citado por Arteaga, 1983, 23), asume el mismo sistema conceptual que el austríaco, el cual en su artículo 263 proporciona una definición de estafa (betrug), al establecer que será castigado por tal hecho todo individuo que “con objeto de procurarse o procurar a un tercero una ventaja pecuniaria ilícita, haya perjudicado la fortuna de otro, provocando o manteniendo un error, ya fuere alegando hechos manifiestamente falsos o deformando o disimulando hechos verídicos”.

Es importante resaltar, sobre todo por su decisiva influencia en mucho ordenamientos jurídicos penales hispanoamericano, la fórmula, de índole también definitoria de la estafa (truffa) adoptada por el Código Penal italiano de 1889 (citado por Arteaga, 1983), el cual señala en su artículo 413, enmarcado en el capítulo III “de la estafa y otros fraudes”, en el título relativo a los delitos contra la propiedad, lo siguiente: el que, con artificios o medios aptos para engañar o sorprender la buena fe ajena, induciendo a alguno en error, se procura a sí mismo o a otro un provecho injusto con daño ajeno, será castigado…” (p. 24).

De las consideraciones anteriores, se obtiene una idea de las principales orientaciones legislativas y de la sistemática adoptada en los comienzos por la codificación, en relación con el delito de estafa.

Análisis Dogmático

Para Manzini, (citado por Grisanti, 1989, 302), artificio es “toda astuta simulación o disimulación apta para engañar, de modo tal que el engaño sea generado por la percepción inmediata de una falsa apariencia material, positiva o negativa”.

Así mismo, Maggiore (citado por Arteaga, 1983, 56), afirma que artificio “es toda estudiada y astuta transfiguración de la verdad. Y ésta puede desfigurarse, o simulando lo que no es… o disimulando, es decir, escondiendo lo que es…”.

Tal como se ha visto, se exige una conducta activa, en el delito de estafa, desplegada por el sujeto activo para engañar a la víctima. Para el Dr. Grisanti, (1989, 302), esta necesidad se concreta en la doctrina francesa, “en la exigencia de una mise en scéne (puesta en escena), aunque no se requiere una gran aparatosidad”. La simple mentira, no acompañada de alguna acción exterior, no es delictiva porque a nadie más que a sí misma debe imputar la víctima el daño sufrido por propia credulidad.

Así mismo, establece Soler (citado por Grisanti, 1989, 303), el problema del silencio se resuelve de modo semejante al de la mentira; se

requiere que vaya acompañado de un actuar engañoso positivo, o bien que exista el deber jurídico de hablar o de decir la verdad. A ese fin, no basta que medie una obligación moral o caballeresca; debe tratarse de una obligación jurídica estrictamente determinable como tal, cuestión que depende del examen particular de cada situación. Cuando el Código quiere asignar carácter de artificio al silencio, lo indica expresamente, sin apartarse de las normas comunes de la omisión típica. Como en el caso del ordinal 6° del artículo 465 del Código Penal venezolano vigente, que se refiere a enajenar o gravar bienes como libres, sabiendo que estaban embargados o gravados o que eran objeto de litigio.

Por su parte, para el autor Arteaga (1983, 57), la expresión del Código Penal “con artificios o medios capaces de engañar”, quiere hacer referencia al proceso engañoso y astuto, que se vale de tretas, ficciones o fingimientos, trampas, dobleces, disimulos o simulaciones, o de cualquiera otros medios de la misma índole.

En este sentido, la idoneidad del artificio o engaño ha de apreciarse en cada caso concreto, tomando en cuenta las circunstancias del mismo y, en especial, las condiciones personales del sujeto pasivo, porque el mismo

artificio o engaño no puede tener idéntica eficacia en relación a la generalidad de los hombres.

La consecuencia del empleo de los medios fraudulentos ha de ser inducir en error a la víctima. El error es una falsa representación de la realidad. Cabe destacar, la afirmación de Finzi (citado por Grisanti, 1989, 305), “el error representa el resultado de la acción engañosa y se convierte en causa de la disposición patrimonial. Hay una sucesión de nexos causales: el artificio provoca el error y éste, a su vez, determina la prestación perjudicial”. La estafa no se concibe sin el error de la víctima.

En relación con el error, Soler expone (citado por Grisanti, 1989):

> Dentro del proceso sucesivo de los hechos que integran una estafa, la situación del error podría decirse que es central. Debe ocupar un lugar intermedio entre el ardid y la disposición patrimonial, y con ambos ha de mantener una estrecha relación de razón suficiente. El ardid debe haber determinado el error y éste, a su vez, debe haber determinado la prestación. Sí no existe esa perfecta consecutividad, tampoco hay estafa. Por ejemplo, si un sujeto, mediante ardides, logra distraer al empleado de la ventanilla y de este modo logra apoderarse del dinero, hay hurto y no estafa, porque aun cuando hay ardid y error, el error no es determinante de la prestación. La cadena causal se haya interrumpida. (p. 305).

Para Maggiore, (citado por Arteaga, 1983, 56), el engaño “es un artificio acompañado de maquinación dolosa, para inducir a error de manera

más fácil. Precisamente se diferencia del artificio por la característica de ser siempre positivo, o sea, por consistir en una acción".

En consideración con lo antes expuesto, el engaño es la falta de verdad en lo que se dice, se piensa o se hace creer. En otras palabras, es dar a una mentira la apariencia de verdad, acompañándola de actos exteriores que levan a error.

El ardid es todo artificio o medio empleado hábilmente para el logro de algún intento. Es decir, es el empleo de tretas, astucias o artimañas para simular un hecho falso o disimular uno.

En este contexto, para la presente investigación, sin el error no existe estafa. El ardid o engaño debe provocar el error de la víctima. El error es el falso conocimiento; la víctima cree saber, pero sabe equivocadamente. Así como los medios fraudulentos deben provocar el error, éste a su vez, debe provocar en la víctima la determinación de entregar la cosa al estafador. Se afirma, que en la estafa la voluntad de la víctima esta viciada desde el comienzo, por el error provocado mediante la actividad fraudulenta.

El sujeto activo en el delito de estafa es indiferente. Pero como afirma Grisanti (1989, 305), "no se debe confundir al autor de la inducción a error

con el beneficiario del provecho injusto". Ambas cualidades coinciden, de ordinario, pero pueden estar separadas. Así se deduce de la expresión del Código "procure para sí o para otro un provecho injusto". De modo que, como escribe Maggiore (citado por Grisanti, 1989, 305), "uno puede ser el estafador y otro el que obtiene el provecho".

La pluralidad de autores, tan frecuente en la estafa, no está prevista como calificante, a diferencia del delito de hurto (artículo 455, ordinal 9°). Para el autor Finzi (citado por Grisanti, 1989, 305), asegura que "esta exclusión no ha de aprobarse, porque el concurso de varias personas en la estafa vuelve más creíble lo que no es verdadero y más insidioso el engaño, y aumenta, por consiguiente, la peligrosidad del hecho". Sin embargo, debe aplicarse la circunstancia agravante genérica consagrada en el ordinal 11° del artículo 77 del Código Penal venezolano, el cual se refiere a la ejecución de un delito con armas o en unión de otras personas que aseguren o propicien la impunidad.

En relación con el sujeto pasivo, al igual que el sujeto activo, es indiferente. La víctima del engaño es la persona que sufre el error causado por el artificio del agente. El sujeto pasivo de la estafa es la persona

perjudicada en su propiedad. Estas cualidades pueden recaer en la misma persona o en personas distintas.

Así mismo, no son susceptibles de error los inconscientes, ni los incapaces en medida que les impida discernir. Tampoco lo son las personas jurídicas en sí mismas, porque carecen de raciocinio; pero pueden resultar sujetos pasivos de la estafa, en relación con el error de quienes las representan. Es este un caso de desdoblamiento entre la víctima del error provocado por el engaño y la del perjuicio patrimonial (sujeto pasivo del delito).

Con respecto al objeto material, además de las cosas, muebles o inmuebles, el objeto material sobre el cual recae la acción delictiva es la persona engañada. La conducta del agente actúa sobre las facultades cognoscitivas y volitivas de la víctima, sea determinando una falsa representación del entorno existencial, sea provocando un acto de voluntad viciado por error.

Por su parte, el objeto jurídico es el interés del Estado en la tutela de los bienes patrimoniales, contra los engaños realizados con el fin de alcanzar un provecho injusto, antijurídico.

El provecho injusto es cualquier beneficio, económico o moral, que el sujeto activo deriva de su conducta, para sí o para otro, sin tener motivo legítimo para ello. Por lo tanto, como afirma Grisanti, (1989, 308), “no hay estafa cuando el acreedor logra, mediante artificios, que el deudor le entregue lo que le debe”. En este caso, como afirma el mencionado autor, “ni siquiera hay autojusticia o ejercicio arbitrario de la propia razón, delito previsto en los artículos 271 y 272 del Código Penal”, porque no ha habido violencias sobre las cosas ni sobre las personas.

Por consiguiente, el perjuicio ajeno es el daño económico, jurídicamente apreciable y correlativo al provecho obtenido, causado a otro.

En efecto, cuando los resultados del provecho injusto con perjuicio ajeno son varios y están regidos por la misma resolución delictiva, previa, la estafa es continuada, como lo establece el artículo 99 del Código Penal venezolano.

Es evidente entonces, el perjuicio económico para la víctima es un elemento fundamental de la estafa, porque ella es un delito contra la propiedad. Si no existe perjuicio, no existe estafa.

Así mismo, el perjuicio debe ser de naturaleza patrimonial, y además, debe existir realmente, es decir, debe ser efectivo, no siendo suficiente el daño potencial. El perjuicio patrimonial significa que el daño debe tener un valor o significado económico; puede consistir en cualquier acto que afecte el patrimonio o el derecho a propiedad de la víctima.

La estafa es un delito doloso. El agente ha de obrar con la voluntad consciente (intención) de inducir a alguno en error, por medio de artificios o engaños, con el fin de lograr, para sí o para un tercero, un provecho, económico, injusto y perjudicial para el sujeto pasivo.

Cabe agregar, el vocablo dolo tiene dos significados; intención de cometer un delito, y engaño o fraude (de conformidad con los artículos 1.146 y 1.154 del Código Civil). Para Grisanti, (1989, 308) la estafa es un fraude. De manera que, en ambos sentidos, la estafa es un acto doloso.

En otras palabras, la estafa es un delito doloso y exige, en todos los casos, que el autor haya realizado la actividad fraudulenta con el fin de engañar, es decir, con el propósito de producir error en la víctima.

No se puede hablar de ardid ni de estafa, cuando el propio autor del hecho es el primer engañado, es decir, cuando él a su vez actúa engañado

por las circunstancias. De igual manera, es necesario que el autor obre con el fin de obtener un beneficio indebido. No es necesario que este fin se logre realmente, es suficiente con que haya actuado con ese fin.

El error esencial excluye el dolo. Según la Casación italiana (citado por Grisanti, 1989, 308), el error para excluir el dolo y, por lo mismo, la estafa, debe corresponder a una representación de la realidad objetivamente falsa, pero cierta en la mente del agente, de modo que produzca en él un convencimiento firme. Al contrario, si falta esta certeza, la situación psíquica de la duda no elimina el dolo, que existe como eventual.

En relación al momento de la consumación del delito, la estafa se consuma cuando el agente obtiene el provecho injusto con perjuicio ajeno. Como afirma Crivellari (citado por Grisanti, 1989, 308), el legislador utiliza la palabra procurar, que equivale a obtener, conseguir, hacerse dar.

De igual manera, el Dr. Arteaga (1983), afirma que de acuerdo con el ordenamiento penal, el delito de estafa se consuma cuando:

> El sujeto activo, valiéndose de artificios y engaños que logran inducir en error a una persona, obtiene o se procura a sí o a un tercero un provecho injusto, con perjuicio ajeno. Ahora bien, se entiende, como señala Manzini, que se ha obtenido el provecho, cuando la cosa ha pasado de la esfera de disponibilidad del estafado a la del estafador, o cuando este último, de otra manera, ha obtenido para sí o para otro la

> prestación deseada, y todo ello, en forma tal que se siga un daño patrimonial correlativo. (p. 78).

En evidente entonces, si el estafador no logra sus últimos designios en relación con lo estafado, si la cosa le es arrebatada o si obsta por reintegrarla, ello no logra borrar el delito de estafa cometido.

En cuanto a la tentativa, tomando en consideración lo establecido en el artículo 80 del Código Penal venezolano, que establece que habrá tentativa cuando “con el objeto de cometer un delito, ha comenzado alguien su ejecución por medios apropiados y no ha realizado todo lo que es necesario a la consumación del mismo, por causa independientes a su voluntad”.

En otras palabras, si alguien ha comenzado la ejecución del delito de estafa con medios idóneos y no llega a realizar todo lo que es necesario para consumarla, de acuerdo con las exigencias del tipo, debido a causas independientes de su voluntad, deberá ser castigado a título de tentativa de estafa.

Por consiguiente es importante destacar, de acuerdo a la norma que regula la tentativa del delito, el momento en que comienza la ejecución de la estafa. Se tendrá como principio de ejecución tan sólo cuando un sujeto haya

utilizado artificios o engaños idóneos con el fin de inducir en error a una persona determinada y con miras a la obtención de un provecho injusto. De esta manera, se requiere al menos, que se hayan usado artificios o engaños con respecto a una persona determinada, considerándose que antes de este momento solamente pueda hablarse de actos preparatorios.

En efecto, como afirma Arteaga (1983, 84), para que pueda enmarcase el hecho dentro de las previsiones de la tentativa de estafa, no es suficiente el mero artificio o engaño; es necesario “que este medio se haya utilizado y dirigido a una persona determinada para engañarla, inducirla en error y obtener el provecho injusto”. Así mismo, se requiere también que los medios sean los idóneos.

Por lo tanto, la estafa admite el grado de tentativa, pero no el de frustración. En efecto, para que pueda haber frustración, de acuerdo al artículo 80, 2° aparte, se requiere, y en ello radica la diferencia fundamental con la tentativa, que el sujeto activo haya realizado con el objeto de cometer un delito, todo lo necesario para consumarlo, es decir, que haya habido consumación subjetiva, lo cual no ha entenderse, como a veces se ha afirmado, en el sentido de que el sujeto haya realizado todo lo que debía o le correspondía hacer personalmente.

En consecuencia, el delito de estafa se consuma cuando el agente ha obtenido el provecho, esto es, cuando ha logrado la disposición patrimonial beneficiosa para sí o para otro con el correlativo daño ajeno. Si tales extremos se han dado, hay consumación objetiva y subjetiva, el delito es perfecto: pero si el sujeto no ha logrado la disposición patrimonial, que no tiene nada que ver con el provecho último buscado, no se puede catalogar como frustración, ya que no ha habido consumación subjetiva del delito, existiendo por tanto, elementos que sólo se puede encuadrar como tentativa de estafa.

Con respecto a las agravantes del delito de estafa, éstas se consagran, a partir del primer aparte del artículo 464, estableciendo que la pena será de dos a seis años si el delito de ha cometido:

1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el estado o de un instituto de asistencia social.
2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad.

En cuanto a la primera agravante, su fundamento radica en que la estafa ha vulnerado un interés colectivo. Cuando se estafa a la Administración Pública o a un ente autónomo estatal, se perjudica a toda la comunidad, porque se vulneran los recursos económicos destinados a satisfacer necesidades sociales. Si la estafa se comete contra un instituto de

asistencia social, público o privado, se toma en cuenta, la función colectiva que cumple tal institución en favor de los desvalidos.

En el caso de la segunda agravante, su fundamento se encuentra en la peculiar gravedad y eficacia del medio usado por el agente. Como señala Manzini (citado por Arteaga, 1983, 86), la razón que explica la agravación de la pena, deriva de la "particular gravedad y eficacia del medio usado". En efecto, el artificio o engaño escogido por el estafador para defraudar a su víctima está dotado de una particular fuerza, ya que consiste en explotar, en orden a la obtención de un provecho económico injusto, el natural temor del ser humano ante el peligro y la disposición a cumplir las órdenes que emanan de la autoridad.

De igual manera, el artículo 464 del Código Penal venezolano en su último aparte, establece una agravante específica, de la siguiente manera:

> El que cometiere el delito previsto en este artículo, utilizando como medio de engaño un documento público falsificado o alterado, o emitiendo un cheque sin provisión de fondos, incurrirá en la pena correspondiente, aumentada de una sexta a una tercera parte.

En efecto, en el delito de estafa se regula la falsificación o alteración de documento público. La estafa se agrava específicamente porque se comete mediante un documento público falsificado o alterado.

Esto se justifica, en razón de que al utilizarse tales engaños para defraudar a otro, no sólo se lesiona la propiedad ajena, sino que también se atenta contra la fe pública, bien jurídico que merece la más efectiva protección de la ley penal.

Tal como se ha visto, quien se sirve de un documento que ha sido falsificado total o parcialmente, en forma tal que aparezca con las apariencias de un instrumento que hace plena fe; o así mismo, quien altera un documento público verdadero en orden a estafar a otro, desvirtúa la naturaleza misma de tales instrumentos y contribuye a sembrar desconfianza en relación a tan valiosos medios de la seguridad jurídica, burlando de esta forma la fe y la confianza pública. Y de la misma manera, quien estafa emitiendo un cheque sin provisión de fondos o con fondos insuficientes, desnaturaliza un instrumento de pago, que sólo circula por la confianza del público y que está destinado al uso normal en el tráfico mercantil.

Para dar por terminado el presente Capítulo, el delito de estafa produce una disposición patrimonial perjudicial, inducida por el error o engaño del sujeto activo, mediante artificios o sorprendiendo la buena fe de la víctima, con el fin de obtener un beneficio indebido para sí o para un tercero. En el siguiente Capítulo, se analiza el delito de fraude establecido en la Ley Especial contra los Delitos Informáticos, mejor conocido como fraude

informático, el cual presenta características diferentes al delito de estafa regulado en el Código Penal venezolano.

CAPÍTULO V

EL FRAUDE INFORMÁTICO

En el presente capítulo se analizan las novedades que presenta el delito de fraude contemplado en la Ley Especial contra los Delitos Informáticos. A través del análisis de la imposibilidad de subsumir el fraude informático en el tipo penal de la estafa, así como el estudio de las diferentes definiciones realizadas por los doctrinarios y el análisis dogmático del delito de fraude establecido en la Ley especial, y por último la descripción de los tipos de fraudes informáticos.

La informática es una ciencia o técnica que ha permitido simplificar y agilizar una gran variedad de actividades en diferentes áreas. La informática se hace cada día más imprescindible, es una época en la cual la tecnología juega un papel sumamente importante.

Se ha afirmado en la presente investigación, que las tecnologías de la información avanzan rápidamente en la cultura mundial, invade en todos los ámbitos de las relaciones sociales y, por tanto, el derecho debe enfrentarse a esos grandes cambios.

Igualmente, se ha destacado que al lado de los numerosos beneficios que ha traído el desarrollo de las tecnologías de la información, se han abierto grandes oportunidades a conductas antisociales y delictivas, siendo un aspecto negativo que presentan, estos sistemas ofrecen complicadas formas de violar la ley y han creado la posibilidad de cometer delitos de tipo tradicional pero en una forma no común, es decir a través del uso indebido de las tecnologías de información, o a través de la manipulación fraudulenta de los sistemas informáticos.

La informatización de las transacciones financieras, comerciales y bancarias, la generalización del pago a través de procedimientos electrónicos, el desarrollo de la gestión y de los procesos contables mediante sistemas de esta naturaleza, ha abierto formas inéditas de comisión a los delitos patrimoniales y económicos, mejor conocidos como delitos informáticos y bancarios, entre ellos el fraude informático. Las redes de transmisión de datos, igualmente, facilitan aún más la posibilidad de delito, al permitir que el autor pueda efectuar las modificaciones desde su propio domicilio, si dispone de un terminal y un instrumento de transferencia de datos adecuado.

Imposibilidad de adecuación del tipo penal de Estafa al Fraude Informático

Arduamente se ha discutido por la doctrina, especialmente la extranjera, si se configura el delito de estafa utilizando como medio de comisión una computadora. Se ha llegado a afirmar que no existe precisamente una estafa informática como tal o una inducción en error de un computador, sino más bien de una conducta informática análoga, que se la ha denominado fraude informático.

La razón radica en que la estafa, en el aspecto relativo a la inducción en el "error", debe darse sobre una persona y no sobre una máquina. Esto ha permitido que la doctrina y la misma ley, como sucede en Italia y Francia, se refieran al fraude informático como aquella conducta donde la intención de defraudar (ánimus defraudandi), debe entenderse como, "integrada a la alteración de un sistema informático o a la abusiva intervención mediante cualquier medio sobre datos de información o programas contenidos en los sistemas informáticos" (Fernández, 2001, 115).

En el ordenamiento penal venezolano, la estafa esta contenida en el artículo 464 del Código Penal, es una conducta destinada a perjudicar el

patrimonio económico ajeno con el fin de obtener provecho ilícito, mediante artificios o engaños idóneos o sorprendiendo la buena fe de otro.

Sin embargo, el delito de fraude informático, no cumple con los supuestos del delito de estafa, debido a que no se aprecia la existencia de un ardid o engaño que induzca en error a una persona y que la motive para la realización de una determinada conducta ocasionándole un perjuicio. En este mismo sentido, Santiago Acurio Del Pino (citado por Ramírez, 2003, 14) sostiene que:

> 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 vendría 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.

De igual manera, Noelia García (citado por Ramírez, 2003, 14), sostiene que los principales elementos que constituyen el delito de fraude informático son: “el ánimo de lucro; la acción de valerse de una manipulación informática o artificio semejante; la transferencia no consentida del patrimonio de otra persona sin utilizar violencia y la existencia de perjuicio a tercero”. Como se advierte, desaparece el engaño y el error del sujeto pasivo

Mucho se ha discutido si las conductas asociadas al fraude informático pueden ser sancionadas al amparo del delito de estafa tipificado en el artículo 464 del Código Penal. El delito de estafa presupone que una persona sea engañada, y que se la induzca como consecuencia de esa conducta a un error que la lleve a realizar un acto de disposición patrimonial lesivo, pero en los fraudes informáticos, este engaño no ocurre. No se puede engañar a una máquina (computadora), el engaño supone una relación psicológica entre el sujeto activo y el pasivo.

En este sentido, unas de las dificultades que surge para tratar de subsumir el fraude informático en el delito tradicional de estafa es la consideración de cosa corporal como el objeto de dicho delito. Las cosas que pueden ser objeto del delito de estafa, en efecto, son sólo las cosas corporales muebles o inmuebles. Además, si mediante la manipulación fraudulenta de datos lo que se afecta es al dinero escritural o contable (cosas incorporales), mediante las alteraciones de los registros de crédito y débito no se afecta a ninguna cosa corporal, 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.

Por lo tanto, se considera que dentro del delito de estafa no podría hablarse de cosas incorporales para los efectos de los delitos contra la

propiedad, pues ni siquiera se puede afirmar que el despojo de un derecho de crédito, pueda ser considerado en función de cosa corporal mueble, sino sólo de protección a un derecho concreto, pues no se puede despojar del derecho, que está en la persona, sino que se puede despojar del ejercicio del derecho o de la cosa sobre la cual recae ese derecho.

En este contexto, en el delito de fraude informático, el sujeto activo sustrae del ámbito de disposición del legítimo poseedor los efectos del delito, privándole del crédito de que era titular, con lo cual se produce el mismo efecto que en la aprehensión 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 el dinero en metálico, entendiéndose que desde ese momento el sujeto activo puede disponer del dinero fraudulentamente conseguido.

A estos efectos, 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 contraría al principio de legalidad, dado que la corporeidad es una característica intrínseca de las cosas corporales.

En el derecho comparado las soluciones a esto problemas han sido distintas pero siempre concordantes con lo afirmado anteriormente, por ejemplo: en Alemania las lagunas legales que este tipo de casos dejaban en evidencia, especialmente por la necesidad típica en la figura de la estafa, de un engaño que genere el error de una persona, determinó la introducción de un agregado al tipo penal del fraude, contemplado en el párrafo 263 del Código Penal alemán, (citado por los autores Cruz y Salvador, s/f), en el que establece:

> El que, con la intención de procurarse a sí mismo o a un tercero un beneficio patrimonial antijurídico, causare un perjuicio en el patrimonio de otro, determinando el resultado de una operación de proceso de datos mediante la incorrecta configuración del programa, el empleo de datos incorrectos o incompletos, el empleo no autorizado de datos o cualquiera otra intervención ilegitima en el curso del proceso, será sancionado con pena de prisión de hasta cinco años o pena de multa. (p. 49).

Por su parte, en España, el nuevo Código Penal español de 1995, agregó al delito tradicional de estafa (artículo 248, numeral 1) un párrafo donde se incluye el fraude informático (artículo 248, numeral 2), el cual viene a superar los inconvenientes señalados por la doctrina en cuanto a la imposibilidad de aplicar la estafa tradicional, debido a que no concurre el engaño sobre una persona sino sobre una máquina. Este es uno de los casos en que el legislador español ha optado por la introducción de un tipo

específico, que, en cumplimiento del principio de legalidad del derecho penal, viene a regir esta nueva forma de delincuencia.

En Argentina, el profesor Marcos Salt (citado por Ramírez, 2003), manifiesta que en el ordenamiento penal argentino la discusión sobre la posibilidad de adecuación del fraude informático a los delitos tradicionales gira alrededor de dos problemas:

> Por un lado, la adecuación de esta modalidad de conductas en el tipo penal del hurto (artículo 162 del Código Penal) 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 sino, antes bien, un crédito. Además no se produce la acción de apoderamiento sino que el objeto es recibido por el autor. (p. 22).

En cuanto al tipo penal de estafa, el nombrado autor menciona (artículo 172 del Código Penal argentino) que este requiere del engaño, de un ardid que determine el error de la víctima. Por este motivo, sostiene que, en los casos en que el autor manipula el sistema causando un perjuicio pero sin inducir en error a una persona (casos de "engaño al computador"), su conducta no sería típica de los delitos de defraudación.

En Francia las dificultades para incorporar el fraude informático a la figura tradicional de la estafa no se presenta en dicha legislación, por cuanto

en el tipo penal francés no se presenta las limitaciones que denotan los otros tipos penales de estafa, regulados en diversos países.

A estos efectos, la imposibilidad de la adecuación del tipo penal de estafa al fraude informático en Venezuela, deriva en una atipicidad relativa respecto al Código Penal si cabe el término, porque sus elementos objetivos como subjetivos no encontrarían fundamento (a excepción del ánimo de apropiación) dentro del llamado fraude informático, ya que serían tipos completamente diferentes. Así que, en aplicación del principio de legalidad, el tipo penal de estafa no podría ser aplicado al fraude informático en razón de que sus elementos subjetivos y objetivos tienen connotaciones distintas, lo que torna en inaplicable a dicho tipo penal clásico.

Lo realmente cierto es que el fraude informático es uno de los comportamientos delictivos que se presenta con mayor frecuencia, afectando el llamado comercio electrónico, las ventas a distancia o fuera del local comercial o telemáticas y principalmente las operaciones de banca electrónica como las transferencias electrónicas de fondos. Por lo tanto, era necesario regular esta conducta, a través de la Ley Especial contra los Delitos Informáticos, la cual fue publicada en Gaceta Oficial N° 37.313 el 30 de octubre del 2001.

El delito de Fraude en la Ley Especial

contra los Delitos Informáticos

La Ley Especial contra los Delitos Informáticos tipifica el delito de fraude informático en el artículo 14, definiéndolo de la forma siguiente:

> Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Para la Dra. Di Totto (s/f, 46), en el caso del delito de fraude, previsto en el artículo 14 de la Ley Especial, afirma:

> Se está en presencia de la manipulación de los sistemas para insertar instrucciones falsas o fraudulentas que produzcan un beneficio económico en perjuicio ajeno; como se advierte de la lectura del tipo penal, concurre con los elementos de la estafa pero mucho más generales y sin el requerimiento de la mise en scéne (puesta en escena) propia de ésta. El tipo penal consiste, entonces, en crear, introducir, enviar instrucciones erróneas de modo que el sistema (que fue programado para producir un determinado resultado) arroje un resultado totalmente imprevisible que no estaba en el programa, que no estaba diseñado para eso y que produce un beneficio económico en perjuicio ajeno.

Con respecto a un concepto de fraude informático, para el autor español Romero Casanova (citado por Ramírez, 2003, 14) es “la incorrecta utilización del resultado de un procesamiento automatizado de datos,

mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero".

Por su parte, para el autor Camacho Losa (citado por Cruz y Salvador, s/f, 48), considera al fraude informático como "toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito".

Así mismo, para el nombrado autor (s/f, 48), los elementos constitutivos del fraude informático, son:

a. Un sujeto, que es quien comete el fraude.
b. Un medio, que es el sistema informático.
c. Un objeto, que es el bien que produce el beneficio ilícito.

De igual manera, para Camacho Losa (citado por los autores Cruz y Salvador, s/f, 48), es evidente que lo que caracteriza al fraude informático es el medio a través del cual se comete, la computadora.

En efecto, el fraude informático, dentro del fenómeno de la delincuencia informática, se presenta como el fraude más impune y que mayores problemas enfrenta en cuanto a su prevención, represión y detención.

Para que exista fraude informático se necesita la utilización de un medio fraudulento, el cual sería la propia manipulación informática. Esto tiene importancia para poder distinguir el fraude informático de otros delitos, que no obstante, por ser realizados por medios informáticos, no constituían antes de la promulgación de la Ley Especial, en defraudaciones.

Es evidente entonces, que el fraude informático tendrá todas las conductas de manipulaciones defraudatorias cuando se tiene el ánimo de obtener un provecho, produciendo así un perjuicio económico o material.

Cabe agregar, para los autores Cruz y Salvador (s/f), el fraude informático no es más que:

> La alteración y producción de documentos electrónicos falsos e información privilegiada de ciertas entidades financieras mediante el manejo doloso de la información por medios técnicos y automáticos. Así como la obtención de dinero o de crédito por medio de fraudes hechos por un computador. (p. 49).

En el mismo orden de ideas, para Lorenzo (2003, 7), el fraude a través de las computadoras, consiste “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”.

A estos efectos, de acuerdo a las definiciones antes expuestas, se puede sacar las siguientes diferencias entre la estafa y el fraude informático:

- En la estafa se obtiene la entrega física del dinero o del objeto corporal querido y en el fraude informático no.
- En la estafa se realiza un engaño de manera directa con la víctima, ya que hay una relación entre dos seres humanos y en el fraude informático no.
- En la estafa existe un destinatario del engaño que sufre un error como consecuencia del estado psicológico de la puesta en escena y desvirtuación de la realidad que se crea.
- La estafa se realiza a través de cualquier modalidad que el agente pueda emplear utilizando su inteligencia o astucia para poder engañar a su víctima, mientras que en el fraude informático el agente utiliza un sistema informático o un computador como medio para poder cometer el fraude.

Con respecto al hurto informático, la Exposición de Motivos de la Ley (s/f, 14), expone que si bien su descripción típica, tipificado en el artículo 13, presenta algunas similitudes con el fraude informático, ambos se diferencian en que, “en el segundo son las instrucciones falsas o fraudulentas del autor las que al alterar o modificar la secuencia lógica de los sistemas, dan lugar a

que se produzca una operación que no estaba autorizada con la consecuencia de la obtención de un activo patrimonial en perjuicio ajeno".

Así mismo, en el artículo 15 se establece un tipo especial de fraude perpetrado mediante la utilización de una tarjeta inteligente ajena o un instrumento destinado a los mismos fines para la obtención indebida de efectos, bienes o servicios con evasión del pago respectivo.

En relación con los distintos métodos para realizar estas conductas de fraude se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos en un ordenador. Esta forma de realización se conoce como manipulación del input.

En segundo lugar, es posible 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 como al adicionar al sistema programas especiales que introduce el autor.

A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta

modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: A esta modalidad se le conoce como manipulación del output. Una característica general de este tipo de fraude, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho, incluso en los casos de manipulación del programa la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún

más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Con respecto a los objetos materiales sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles, (por ejemplo los depósitos monetarios, los créditos, entre otros), en otros casos, los datos que son objeto del fraude, representan objetos corporales (como la mercadería, el dinero en efectivo) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser “creado” por el autor.

Por otra parte, el objeto jurídico que la Ley ampara en el delito de fraude informático es el derecho de propiedad. Siguiendo el sistema predominante de la mayoría de las otras legislaciones, el objeto jurídico no es más que el bien o interés jurídico que el hecho delictuoso hiere o amenaza, y que la Ley penal especial protege de un modo abstracto y concreto.

En cuanto al sujeto activo o el agente en este tipo penal, es la persona que lo perpetra. En otras palabras, es la persona física que utiliza como herramienta, tanto a los computadores como a los programas de computación, así como el uso indebido de las tecnologías de información, para manipular los sistemas o sus componentes, o la data, con el fin de insertar instrucciones falsas o fraudulentas y así obtener un provecho injusto perjudicando a otro, que no es más que el sujeto pasivo. En ambos casos los sujetos son indiferentes, simples, es decir no son calificados.

El perjuicio cometido es uno de los presupuestos fundamentales para que exista el delito de fraude informático. En efecto, los delitos de daño, entre los cuales se encuentra el fraude, son aquellos que, para existir, necesitan que la acción realizada por el sujeto activo produzca una modificación en el mundo exterior, que afecte de una manera directa y adecuada un bien jurídico amparado legalmente; bien jurídico que, según se ha visto, es en este delito la propiedad. En este caso, es indudable que el insertar instrucciones falsas o fraudulentas a través del mal uso de las tecnologías de la información por parte del agente es una actuación de alta tecnología, por consiguiente, necesaria e inexorablemente sólo se puede concluir que la actuación intelectual malintencionada cumple con una función causal o creadora en la producción de los daños.

Así mismo, el perjuicio real y efectivo que se requiere para que exista este delito, debe constituir, la pérdida, disminución o restricción de un bien que, en este delito, debe ser contra la propiedad. Por consiguiente, el perjuicio, que es el resultado (efecto) de la acción (causa) debe ser:

- Efectivo: Si el perjuicio no es concreto, no es real, no es efectivo, no se puede hablar de delito fraude.
- Directo: El perjuicio debe ser consecuencia directa de la acción punible, que es el insertar instrucciones falsas o fraudulentas.
- Cierto: El perjuicio debe ser indudable, no dudoso.
- Contra la propiedad: Si el perjuicio no afecta a la propiedad, faltará un elemento necesario para la configuración del delito de fraude informático.

En el delito de fraude informático existe sólo una de las formas de culpabilidad, que es el dolo específico. Un comportamiento contrario al deber ser. Se aprecia que el dolo específico en el delito de fraude, consiste en la intención de insertar instrucciones falsas o fraudulentas con el fin de obtener un provecho injusto en perjuicio ajeno, es decir, apropiarse de la cosa ajena recibida por el engaño o la defraudación de instrucciones y hacer de ella un uso contrario que el determinado inicialmente. Se tiene que elaborar con mucha astucia toda una logística tecnológica con ayuda de las tecnologías

de la información, sobre un plan delictuoso antes de materializarlo, con frialdad de ánimo, con deliberada intención y madura voluntad de defraudar.

Según lo expuesto, los elementos del dolo específico de este delito, son los siguientes:

- Conocimiento del presupuesto material: artificios técnicos, ofertas engañosas, un e-mail con falsas promesas, que inducen en error a los cibernautas, engañados prestan su inocente consentimiento a través de una pantalla de computador y su buena fe, para que se produzca el provecho injusto.
- Conciencia y voluntad de cumplir una acción ilícita: Algo muy bien preparado y ejecutado, con una conciencia deliberada que concluye en engaño. Se realiza un acto constitutivo de fraude, con previsión de sus efectos.

Es importante destacar que la Ley Especial contra los Delitos Informáticos establece en el artículo 3 el principio de extraterritorialidad, de manera tal, cuando alguno de los delitos previsto en la Ley se cometa fuera del territorio de la República el sujeto activo quedará sometido a sus disposiciones, si dentro del territorio de la República se hubieren producido

efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

En el artículo 5 de la Ley Especial contempla la responsabilidad de las personas jurídicas. Cuando los delitos previstos en la Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

Así mismo, la persona jurídica será sancionada en los términos previstos en la Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Con respecto al tipo de sanción, la Ley Especial establece en el artículo 4, que las sanciones por los delitos informáticos serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito que se trate.

En el caso del delito de fraude informático contemplado en la Ley Especial, establece una pena principal de tres a siete años de prisión y multa de trescientas a setecientas unidades tributarias.

Las penas accesorias están contempladas en el artículo 29 de la Ley Especial, de la forma siguiente:

> Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes:
> 1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.
> 2. El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.
> 3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privadas, respectivamente.
> 4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Las agravantes que se aplican en los delitos tipificados en la Ley Especial se encuentran contempladas en el artículo 27. El cual dispone, que la pena correspondiente a los delitos previstos en dicha Ley se incrementará entre un tercio y la mitad:

1. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.
2. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

Así mismo, se establece una agravante especial en el artículo 28. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de la Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Tipos de Fraudes Informáticos

Existen diferentes clasificaciones de tipos de fraudes, pero en la presente investigación, se mencionan las más usuales e importantes. Entre ellos se tiene la clasificación dada por García de la Cruz (2005, 5), que toma en consideración la clasificación de los delitos informáticos dada por las Naciones Unidas.

- Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común, es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- La manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado caballo de troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
- Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude 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

basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

- Fraude efectuado por manipulación informática: Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
- Estafas electrónicas: El hacer compras en línea mediante el uso de Internet o alguna red de servicio, y no cumplir con lo establecido en el acuerdo de compra en entregar el producto de forma completa o parcial se considera fraude, lo que es muy común al hacer compras por Internet donde se requiere pagar a la cuenta de alguna persona antes de recibir el pedido.

Las personas que se dedican a este tipo de fraudes, consiguen clientes, gente que se interese en comprarles el producto que venden y cuando esas personas se deciden por hacer la compra y pagan a la cuenta que se les dio, ya no se entrega nada, pues lograron engañar a todas esas personas.

Además aquellos lugares o sitios donde se hacen citas, ofrecen cosas que luego no son verdad, a esto se le considera fraude informático. Teniendo como consecuencia que no se pueda tener la suficiente confianza para hacer las compras en línea.

Por lo tanto, es mejor limitarse a hacer las compras sólo en aquellos lugares que están garantizados y son conocidos. Es necesario evitar aquellos lugares que son sospechosos o que no son conocidos y no dan confianza, porque ahí se podría generar un fraude.

Para la presente investigación, se puede resumir las formas de fraude informático en:

- Manipulación fraudulenta de los sistemas informáticos: Entendidos éstos como un gran sistema compuestos de dos subsistemas: de cómputo y de información, que a su vez tienen componentes físicos, lógicos y humanos.

Éste ha sido la forma frecuente de comisión del fraude informático. Mediante este procedimiento se manipula el computador en casos como la obtención ilícita de pagos (sueldos, pensiones, facturas), alteración de saldos

(en cuentas bancarias por ejemplo), transferencia de fondos, alteración de inventarios de mercancías.

Así mismo, este tipo de manipulación se logra en cualquiera de las etapas del proceso informático (que comprende el input; ingreso y validación de los datos, el procesamiento de los mismos y el output; la salida de información).

- Sabotaje, mediante destrucción de programas o datos, implantación de virus, bloqueo de redes o servidores y, en general, cualquier maniobra para alterar el funcionamiento del sistema o sus componentes. Incluye el caso de crackers, terroristas, y empleados despedidos que toman venganza de la compañía.

Así mismo, se tiene como los casos más frecuentes de fraudes informáticos los siguientes:

- Eliminación de ordenes de no pago.
- Operaciones fraudulentas de notas de crédito.
- Fraude mediante numerosas operaciones pequeñas.
- Fraude mediante pocas operaciones grandes.
- Transferencia electrónica de fondos sin soporte numerario.

En fin, el fraude tipificado en la Ley Especial contra los Delitos Informáticos tiene como característica principal conseguir insertar instrucciones falsas o fraudulentas por medio del uso indebido de las tecnologías de información; siendo este su aspecto innovador, produciendo un resultado totalmente diferente al esperado por la víctima y obteniendo un provecho injusto. Así mismo, se afirma que estos hechos ilícitos ocurren a menudo afectando el comercio electrónico, las operaciones bancarias, entre otros. Razones por las cuales el Legislador Venezolano reguló este tipo de conducta en una Ley especial, siendo imposible adecuarla al tipo penal de la estafa por ser diferente su forma de comisión.

CONCLUSIONES

De acuerdo con los razonamientos que se han venido realizando y cumpliendo con los objetivos específicos y general del presente estudio, se llega a las siguientes conclusiones:

- La información que se obtiene de las tecnologías ha adquirido un valor superior desde el punto de vista económico, constituyéndose en un bien esencial del mundo jurídico, adquiriendo importante relevancia jurídico-penal por ser objeto de conductas delictivas. Las tecnologías de la información son un conjunto de conocimientos en materia informática utilizados para el manejo de toda clase de información; auxiliándose de los medios y avances en materia de comunicación y el desarrollo de la computación en cuanto al procesamiento automático de la información. En efecto, el medio idóneo para encontrar esa información es el internet, que es el conjunto de computadoras, redes y dispositivos de telecomunicaciones conectados por medio de enlaces a través de un protocolo común, tanto nacional como internacionalmente y permiten la comunicación y el intercambio de información y servicios.

  Así mismo, las tecnologías de la información pueden ser el objeto del ataque o el medio para cometer otros delitos. Reúnen unas

características que la convierten en un medio idóneo para la comisión de muy distintas modalidades de delitos informáticos, en especial de carácter patrimonial (fraudes, apropiaciones indebidas, hurtos, entre otros). Esto proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente sencilla manipulación de esos datos, como existe gran cantidad de información y todo se puede encontrar en un solo lugar.

A partir de la promulgación de la Constitución de 1999, Venezuela ha experimentado un avance legislativo al consagrarse el acceso a la tecnología como un derecho fundamental de los ciudadanos, reconociéndose dentro de los derechos culturales el carácter de interés público de la ciencia, la tecnología, el conocimiento y la innovación, tal como lo establece el artículo 110.

- Venezuela ha dado un paso adelante en materia de delitos informáticos con la concepción y adopción de un ordenamiento jurídico penal, el cual fue publicado en Gaceta Oficial N° 37.313 el 30 de octubre del 2001, llamado Ley Especial contra los Delitos Informáticos, cuyo propósito ha sido dar respuesta sancionatoria a las conductas que vulneran bienes jurídicos dignos de protección penal a través del uso indebido de las tecnologías de información o a las desplegadas justamente para atentar

contra la información como bien jurídico de indubitable valor en esta nueva sociedad informatizada.

La Ley Especial contra los delitos Informáticos regula diferentes conductas delictivas, tales como los delitos contra los sistemas que utilizan tecnologías de información, delitos contra la privacidad de las personas y de las comunicaciones, delitos contra niños o adolescentes, delitos contra el orden económico y delitos contra la propiedad, entre los cuales se ubica el fraude objeto del presente estudio.

Los delitos informáticos son aquellas conductas típicas, antijurídicas y culpables que lesionan la seguridad informática de los sistemas tecnológicos, dirigidas contra bienes tangibles o intangibles como datos, programas, informaciones y otros, almacenados electrónicamente o cualquier otro tipo de bien.

Los delitos informáticos se han clasificado de diferentes maneras, teniendo en cuenta diferentes aspectos, tales como los efectos que producen, los perjuicios causados, la utilización de las tecnologías de la información, el tipo penal en que se encuadren, o la clase de actividad que impliquen según los datos involucrados.

Se advierte internacionalmente, la tendencia a legislar en materia de delitos informáticos con la finalidad de lograr la unificación de una normativa legal para solucionar el problema generado por los efectos que puede tener un delito en internet. En la mayoría de los países

occidentales existen normas similares a los países europeos. Sus lineamientos están basados en lograr que las comunicaciones electrónicas, las transacciones e intercambio de la información o datos sean lo más confiables y seguros posibles.

- Los delincuentes cibernéticos tienden a realizar un tipo de conductas que reuniendo los requisitos que determinan un delito, son llevados a cabo utilizando un elemento informático como simple herramienta para cometer una conducta negativa, o vulnerando los derechos de las personas o de su bien jurídico. Suelen ser personas con conocimiento en el área de la informática y tienen acceso a la información, están dispuestos a dañar o a agredir los sistemas de datos de otras personas.

  La descripción de comportamientos de los delincuentes cibernéticos son tan diversos como los delitos informáticos, pueden ser hackers; quienes interceptan dolosamente un sistema informático, con la finalidad de dañar, apropiarse, difundir o destruir información que se encuentra almacenada en los computadores de entidades públicas o privadas, o pueden ser crackers; se dedican a destruir datos de los sistemas remotos, niegan el servicio a los usuarios legítimos, rompen cualquier sistema y software, y en general a causar problemas. Así mismo, existen los phreakers; personas con amplios conocimientos en telefonía e

informática y realizan actividades no autorizadas, y otros tipos de comportamientos menos relevantes, tales como los lammers, gurús, virucker, pirata informático, entre otros.

- Históricamente el delito de estafa se puede ubicar en el Derecho Romano y ha ido evolucionando a través de los años en diversas legislaciones de diferentes países, hasta ser lo que es hoy en día. En Venezuela el delito de estafa esta contenida en el artículo 464 del Código Penal, como una conducta destinada a perjudicar el patrimonio económico ajeno, con el fin de obtener provecho ilícito, mediante artificios o engaños idóneos o sorprendiendo la buena fe de otro.

  En el delito de estafa se exige una conducta activa desplegada por el autor con la finalidad de engañar a la víctima inducida por el error, es decir, sin el error no existe estafa. El ardid o engaño debe provocar el error de la víctima. Los sujetos activos y pasivos en esta clase de delitos son indiferentes. El objeto material son las cosas muebles o inmuebles y el objeto jurídico son los bienes patrimoniales. La estafa es un delito doloso y exige que el agente haya realizado la actividad fraudulenta con el fin de engañar, es decir con el propósito de producir error en la víctima.

- El delito de fraude de acuerdo con la Ley Especial contra los Delitos Informáticos, se caracteriza por conseguir insertar instrucciones falsas o fraudulentas, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consigan obtener un provecho injusto en perjuicio ajeno.

  El delito de fraude informático no cumple con los supuestos del delito de estafa establecido en el Código Penal Venezolano, debido a que no se aprecia la existencia de un ardid o engaño que induzca en error a una persona y que la motive para la realización de una determinada conducta ocasionándole un perjuicio. En el fraude informático, están incorporadas todas aquellas conductas defraudatorias que, por tener a la informática como herramienta de comisión, no puede ser subsumida en el tipo penal clásico de la estafa. Como se advierte, desaparece el engaño y el error del sujeto pasivo.

  La novedad en el delito de fraude es la utilización indebida de las tecnologías de información, el autor crea, introduce, inserta o envía instrucciones falsas o engañosas, de manera que el sistema produzca un resultado totalmente diferente al esperado por el sujeto pasivo, obteniendo el sujeto activo una ganancia que no le correspondía en perjuicio ajeno. Lo realmente cierto, es que el fraude informático es uno

de los comportamientos delictivos que se presenta con mayor frecuencia afectando el llamado comercio electrónico, las ventas a distancia o fuera del local comercial o telemáticas y principalmente las operaciones de banca electrónica como las transferencias electrónicas de fondos, entre otros.

Existe en el derecho penal vigente una tipificación básica de los delitos informáticos que afectan el interés social y el patrimonio público. A pesar de toda la información que pueda existir en internet referente a los delitos informáticos, las personas deben notificarlo a las autoridades correspondientes, que no parezca que son hechos que se producen por acceder a ella. Tales comportamientos están tipificados en una ley que regula y sanciona todo los delitos cometidos a través del uso indebido de las tecnologías de información. Se hace referencia que son muchas las actividades del hombre que necesariamente son realizadas por un sistema tecnológico y necesitan de una debida protección tanto a nivel informático como legal. Así mismo, existen personas que interfieren en la confianza y su buen funcionamiento, desfavoreciendo la agilidad de los servicios que presta la tecnología de la información.

En consecuencia, no son los grandes sistemas de información los que perturban la vida privada sino la manipulación indebida de ello, por parte de

individuos irresponsables que consiguen insertar instrucciones falsas o fraudulentas, produciéndose el delito de fraude informático. La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede darles, la utilicen para satisfacer sus propios intereses, a costa de las libertades individuales y daños a la propiedad ajena. Así mismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías de la información.

REFERENCIAS BIBLIOGRÁFICAS

Andrades, J. (2000). Formación de Precios de los Productos de Información en Redes Digitales. ***Revista Venezolana de Gerencia del Vice-Rectorado Académico de la Universidad del Zulia***, 11, Mayo - Agosto.

Arregoitia, S. (2003). ***Posibles sujetos de los delitos informáticos*** (Trabajo en línea). Universidad de La Habana, Facultad de Derecho. Disponible: http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp (Consulta: 2004, Julio 23).

Arteaga, A. (1983). ***La estafa y otros fraudes en la legislación penal venezolana*** (3ª. ed.). Caracas: Ediciones Homero.

Barrios, O. (2001). ***Internet y Derecho. Fundamentos de una Relación*** (Trabajo en línea). Revista Electrónica de Derecho Informático (REDI). Disponible:http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_id=179442&s ort=score&n=7 (Consulta: 2004, Julio 23).

Capitánt, H. (1930). ***Vocabulario Jurídico***. Buenos Aires: Ediciones Depalma.

Carrion, H. (2002). ***Presupuestos para la incriminación del hacking*** (Trabajo en línea). Universidad del Museo Social Argentino y la Universidad de Burgos Disponible: http://www.alfa-redi.org/upload/documento/110801--19-58-PRESUPUESTOS%20PARA%20LA%20INCRIMINACION%20DEL%20HACKING.doc (Consulta: 2004, Octubre 26).

Casanova, R. (1987). ***Poder Informático y Seguridad Jurídica***. Madrid: Funesco.

Centro Nacional de Tecnologías de Información (CNTI) (s/f). (Trabajo en línea). Disponible: http://www.cnti.ve/cnti_docmgr/glosario.html?Letra=T (Consulta: 2004, Mayo 10).

Código Penal Venezolano. (2000). ***Gaceta Oficial Nº 5.494 Extraordinario***. Octubre 20, 2000.

Congreso de la República. (s/f). ***Exposición de Motivos de la Ley Especial contra los Delitos Informáticos*****.** Venezuela: Servicio Autónomo de información Legislativa.

Constitución de la República Bolivariana de Venezuela. (1999). ***Gaceta Oficial No.36.860*****.** Diciembre 30, 1999.

Cruz, E., y Salvador, L. (s/f). ***El Delito de Estafa y otros tipos de Fraude*** (Trabajo en línea). Disponible: http://www.geocities.com/CapitolHill/Senate/8569/estafa3.html (Consulta: 2004, Febrero).

Cuello, E. (1982). ***Derecho Penal, Parte Especial*** (Vol. II). Barcelona: Bosch

Cuervo, J. (1998). ***Delitos informáticos: Protección Penal de la Intimidad*** (Trabajo en línea). Disponible: http://www.informatica-juridica.com/trabajos/delitos.asp (Consulta: 2005, Julio 5).

Delitos Informáticos (s/f). (Trabajo en línea). Disponible: http://www.lafacu.com/apuntes/informatica/delitos_informaticos/default.htm (Consulta: 2004, Julio 23).

Di Totto, B. (2003). **Conferencia sobre la Ley Especial contra los Delitos Informáticos** (Trabajo en línea). Disponible: http://derechoinformatico.net.ve/imagenes/conferencia.pdf (Consulta: 2005, Junio 10).

Estrada, M. (s/f). ***Delitos Informáticos*** (Trabajo en línea). Disponible: http://www.unifr.ch/derechopenal/articulos/pdf/DELITOS.pdf (Consulta: 2005, Julio 6).

Fernández, C., y Dahnke, G. (1998). ***La Comunicación Humana***. México: Mc Graw Hill.

Fernández, M. (2001). ***Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos***. Trabajo de grado no publicado. Universidad Sergio Arboleda: Santa Marta.

García, J. (2005) ***Delitos Informáticos*** (Trabajo en línea). Disponible: http://www.ilustrados.com/publicaciones/EEEFuVEppAyTYhionA.php (Consulta: 2005, Enero 17).

Grandinetti, R. (2000). Nuevas Tecnologías de la Información y Gestión de Recursos Humanos en el ámbito Público Local: El caso de la Municipalidad de Rosario. ***Revista Venezolana de Gerencia del Vice-Rectorado Académico de la Universidad del Zulia***, 11, Mayo - Agosto.

Grisanti, A. (2000). ***Lección de Derecho Penal***. *Parte General*. Caracas: Mobil-Libros.

Grisanti A., y Grisanti F. (1998*). **Manual de Derecho Penal, Parte Especial*** (7ª. ed.). Caracas: Mobil-Libros.

Hance, O. (1996). ***Leyes y Negocios en Internet***. México: Mc Graw Hill.

Hernández, R., Fernández, C. y Baptista, P. (2003). ***Metodología de la investigación*** (3da ed.). México: McGraw-Hll.

Landaverde, M., Soto, J., y Torres, J. (2000). ***Delitos Informáticos*** (Trabajo en línea). Universidad de el Salvador. Disponible:

http://www.lafacu.com/apuntes/informatica/delitos_informaticos/default.htm (Consulta: 2004, Octubre 26).

Ley Especial contra los Delitos Informáticos. (2001). ***Gaceta Oficial de la República de Bolivariana Venezuela N° 37.313***. Octubre 30, 2001.

Lorenzo, P. (2003). ***Conceptualización y generalidades del Fraude Informático*** (Trabajo en línea). Disponible: http://www.monografias.com/trabajos12/conygen/conygen.shtml (Consulta: 2004, Mayo 10).

López, M. (1999). ***Delincuencia y Fraude Informático***. Santiago de Chile: Editorial Jurídica de Chile.

Manson, M. (1999). ***Legislación sobre Delitos Informáticos*** (Trabajo en línea). Disponible: http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml (Consulta: 2004, Agosto 03).

Márquez, A. (s/f). ***La necesidad de contemplar los delitos informáticos en el Código Penal del Estado de Michoacán*** (Trabajo en línea). Disponible: http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Introduccion.htm (Consulta: 2005, Junio 10).

Merlat, M., et al. (1999). ***Seguridad Informática: Hackers*** (Trabajo en línea). Disponible: http://www.monografias.com/trabajos/hackers/hackers.shtml (Consulta: 2004, Octubre 26).

Morales, E. (s/f). ***Delitos Informáticos*** (Trabajo en línea). Disponible: http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml (Consulta: 2005, junio 5).

Moreno, C. (2001). ***Planificación de Sistemas y Tecnologías de la Información*** (Trabajo en línea). Disponible:

http://www.monografias.com/trabajos7/psti/psti.shtml#objetivos (Consulta: 2004, Julio 10).

Páez, N. (2004). Introducción a la Informática (Trabajo en línea). Disponible: http://www.monografias.com/trabajos22/aspectos-informatica/aspectos-informatica.shtml (Consulta: 2005, Junio 2).

Palazzi, P. (2000). ***Delito Informático***. Buenos Aires: Editorial Ad-Hoc.

Paredes, C. (2003). ***Hacking*** (Trabajo en línea). Disponible: http://www.ilustrados.com/publicaciones/EpyFyuyVVFxxXuSfcc.php#PLANT (Consulta: 2004, Octubre 26).

Pinarello, M. (s/f). ***Delitos Informáticos*** (Trabajo en línea). Disponible: http://www.todoiure.com.ar/monografias/lapeyre.htm (Consulta: 2005, Febrero 2).

Ramírez, J. (1994). ***Diccionario Jurídico***. Buenos Aires: Editorial Caridad S. A.

Ramírez, R. (2003). ***Inclusión de los delitos informáticos dentro del Código Penal del Estado*** (Trabajo en línea). Disponible: http://www.ilustrados.com/publicaciones/EpyAuuyuEAqTwTZHbL.php (Consulta: 2004, Julio 23).

Riquet, A. (1998). ***Informática y el Derecho Penal Argentino***. Buenos Aires: Ed. Ad-Hoc.

Rodríguez, F. (1998). (Trabajo en línea). Disponible: http://www.a2c.uam.mx/gestión/nu9m/indíce.htm (Consulta: 2004, Diciembre 13)

Romeo, C. (1987). ***Poder Informático y Seguridad Jurídica***. España: Funesco.

Tablante, C. (2001). ***Delitos informáticos delincuentes sin Rostros***. Caracas: Editorial En Cambio.

Tellez, J. (1996). ***Derecho Informático*** (2ª. Ed). México: Edición Mc Graw Hill.

Universidad Católica Andrés Bello. (1997). ***Manual para la elaboración del Trabajo Especial de grado en el área de Derecho para optar al título de Especialista***. Caracas.

Viega, M. (1999). ***Delitos Informáticos*** (Trabajo en línea). Disponible: http://publicaciones.derecho.org/redi//No._09_-_Abril_de_1999/viega (Consulta: 2005, Febrero 2).

Wikipedia (2005) ***Enciclopedia libre***. (Página en línea). Disponible: http://es.wikipedia.org (Consulta: 2005, Junio 10).

Witket, J. (1995). ***La Investigación Jurídica***. México: Serie Jurídica Mc Grau Hill.

Zabale, E., Herrera, R., y Beltramone, G. (1999). ***Delitos Informáticos***. Boletín Hispanoamericano de Informática y Derecho, 3, agosto.

ANEXOS

ANEXO A

GLOSARIO

Antivirus: Programa que busca, detecta y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, diskette u otro soporte. (Tablante, 2001, 189).

Archivo: Datos estructurados que pueden recuperarse fácilmente y usarse en una aplicación determinada. Se utiliza como sinónimo de fichero. Todos los datos en disco se almacenan como un archivo con un nombre de archivo asignado que es único dentro del directorio en que reside. (Páez, 2004, 25).

Ataques asincrónicos: Es uno de los procedimientos más complicados de saboteo. Periódicamente se graban determinados datos en un sistema y si alguien logra que el sistema se caiga o se paralice, es posible entonces modificar determinados archivos, de manera que cuando se pone de nuevo en funcionamiento el sistema, éste operará con la nueva información, provocando alteraciones o errores. (Tablante, 2001, 189).

Backdoor: Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal. (Merlat y otros, 1999, 78).

Banda ancha: Característica de cualquier red que permite la conexión de varias redes en un único cable. Para evitar las interferencias en la información manejada en cada red, se utilizan diferentes frecuencias para cada una de ellas. La banda ancha hace referencia también a una gran velocidad de transmisión. (Merlat y otros, 1999, 76).

Base de datos: Conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos. (Tablante, 2001, 190).

Bit (bit, bitio): Se trata de la unidad mínima de información que se maneja en una computadora. Se deriva de la contracción de la expresión binary digit (dígito binario). (Tablante, 2001, 190).

Bug (error, insecto, bicho): Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa. (Merlat y otros, 1999, 78).

Caballo de Troya: Esta técnica consiste en introducir dentro de un programa una rutina (conjunto de instrucciones que realizan una tarea) no autorizada y desconocida por la persona que lo ejecuta, para que dicho programa actúe de una forma diferente a como estaba previsto; el creador del programa tiene la oportunidad de accesar al interior del sistema que lo procesa. (Tablante, 2001, 190).

Cazador de contraseñas: Este programa intenta desencriptar o decodofocar las claves o contraseñas (password) de un sistema de información y eliminar la protección que aquéllas le brindan. Una vez desencriptada la clave se consigue el acceso al sistema de datos y por ende se puede fácilmente manipular la información. (Tablante, 2001, 190).

Chat (conversación, charla, chateo, platicar): Servicio ofrecido en Internet mediante el cual las personas pueden conversar en salas o canales de conversación en línea mediante el envío y recepción de textos. (Tablante, 2001, 190).

Chip (microprocesador): La parte más importante de una computadora la representa este circuito con soporte de silicio e integrado por transistores y

otros componentes electrónicos. Es el cerebro de los computadores. (Tablante, 2001, 191).

Ciberespacio: Fue utilizado por la primera vez en la novela “Neuromancer” de William Gibson en donde se aplicaba para describir un universo de computadoras y una civilización creada en torno a estas máquinas. Lugar indefinido, donde los seres humanos se encuentran y comunican a través de la red. Aunque no es exactamente “real”, es un lugar que existe. Hay cosas que ocurren allí que tienen consecuencias muy reales. (Tablante, 2001, 190).

Cibernauta (cybernaut o internauta): Usuario que navega por la red. (Tablante, 2001, 190).

Cibernética: Ciencia que estudia los sistemas de control y comunicación en las máquinas, de forma que reaccionen como un ser humano ante determinados estímulos. (Merlat y otros, 1999, 76).

Clonación (de tarjetas): Procedimiento mediante el cual se captura digitalmente la información de seguridad contenida en una tarjeta electrónica y luego se reproduce una copia ilegal de la misma, que es usada con fines de defraudación. (Tablante, 2001, 190).

Computador: Dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas. (Ley Especial contra los Delitos Informáticos, 2001).

Congestión: Se produce una congestión cuando la carga existente sobrepasa la capacidad de una ruta de comunicación de datos. (Páez, 2004, 26).

Contraseña (password): Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema. (Ley Especial contra los Delitos Informáticos, 2001).

Cookie (cuqui, espía, delator, fisgón, galletita, pastelito): Se trata de un conjunto de programas, en ocasiones encriptados en el mismo navegador, que se almacena en el disco duro de la computadora del usuario cuando éste entra a determinadas páginas en Internet. (Tablante, 2001, 191).

Correo electrónico: Servicio telemático similar al sistema postal ordinario, pero sobre un sistema informático. También llamado e-mail. Es un nuevo y eficaz medio de comunicación entre ordenadores y bancos de datos de todo el mundo. (Wikipedia, 2005).

Cortafuegos (Firewall): Computadora que registra todos los paquetes de información que entran en una compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella. Es como un embudo que mira si la información que desea entrar a un servidor tiene permiso para ello o no. Los hackers deben contar con gran creatividad para entrar ya sea buscando un bug (error de diseño) o mediante algún programa que le permita encontrar alguna clave válida. (Merlat y otros, 1999, 78).

Cracker (intruso, saboteador): Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad. Se tiende a diferenciar del Hacker en la intención. (Tablante, 2001, 192).

Cracking: Modificar un programa para obtener beneficios. Normalmente se basa en quitar pantallas introductorias, protecciones o, como en unas

modificaciones de cierto programa de comunicaciones, conseguir nuevos passwords de acceso a sistemas. (Merlat y otros, 1999, 78).

Criptografía (cryptos grafos): Arte o ciencia de la escritura secreta. Procura ocultar los mensajes o información de ojos ajenos. Consiste en cifrar y descifrar mensajes. En computación se refiere a los mensajes que son enviados por un emisor que oculta el contenido del mensaje a manera de que sólo ciertas personas tendrán acceso a la información por medio de una clave. Resuelve los siguientes problemas: privacidad, autenticidad, no rechazo, integridad. (Tablante, 2001, 193).

Criptología: Es el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor. (Wikipedia, 2005)

Cyberpunk: Corriente literaria dentro de la ciencia-ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras. (Merlat y otros, 1999, 78).

Data (datos): Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o

procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado. (Ley Especial contra los Delitos Informáticos, 2001).

Desencriptar: decodificación o revelación de códigos de seguridad. (Tablante, 2001, 193).

Disco duro: Dispositivo de almacenamiento de datos mediante tecnología magnética que consta de un disco en el que se graba la información, para recuperarla posteriormente gracias a una o varias cabezas lectoras-grabadoras. (Páez, 2004, 28).

Documento: Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos. (Ley Especial contra los Delitos Informáticos, 2001).

Encriptar: Proceso general de codificación de datos con un propósito de seguridad. (Tablante, 2001, 193).

Encriptación (encrytion, cifrado): Se trata de un mecanismo de seguridad en Internet cuya principal función es la de hacer llegar la información a un determinado usuario sin que nadie más pueda tener acceso a ella. Existen diversos tipos de cifrados que en cierta manera son la base de la seguridad de la red. (Tablante, 2001, 193).

Fibra óptica: Sistema de transmisión que utiliza fibra de vidrio como conductor de frecuencias de luz visible o infrarrojas. Este tipo de transmisión tiene la ventaja de que no se pierde casi energía pese a la distancia (la señal no se debilita) y que no le afectan las posibles interferencias electromagnéticas que sí afectan a la tecnología de cable de cobre clásica. (Wikipedia, 2005).

Firewall (barrera contra fuegos): se denomina así al sistema de seguridad que se coloca entre la red local e internet, de esta manera la empresa o compañía regulará completamente toda la comunicación hacia internet estableciendo sus políticas de seguridad. En ocasiones este sistema incorpora autentificación de usuarios entre otras cosas. (Tablante, 2001, 193).

Firma electrónica: Información creada o utilizada por el signatario, asociado al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido utilizado. (Tablante, 2001, 193).

Firmware: Programa o segmento de programa incorporado de manera permanente en algún componente del hardware. (Ley Especial contra los Delitos Informáticos, 2001).

Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos, pero es diferente del virus porque no se puede regenerarse. (Tablante, 2001, 193).

Hacker (pirata): Persona con destrezas y conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer. (Tablante, 2001, 194).

Hardware: Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes. (Ley Especial contra los Delitos Informáticos, 2001).

Información: Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas. (Ley Especial contra los Delitos Informáticos, 2001).

Internet (La Red): Se denomina así a la red de telecomunicaciones que surgió en Estados Unidos. Primero se le llamó ARPAnet y fue pensada para cumplir funciones de carácter meramente militar; para convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural, económico, y otros. (Tablante, 2001, 195).

Internet 2: Proyecto de interconexión de más de cien universidades estadounidenses. El objetivo es desarrollar una red de altísima velocidad para la educación y la investigación. (Tablante, 2001, 196).

Intranet: Red de redes de una empresa o institución. Se le conoce como la red interna de una institución. (Tablante, 2001, 196).

Lamer: Tonto, persona con pocos conocimientos. Principiante. (Merlat y otros, 1999, 78).

Login: Procedimiento de identificarse frente a un sistema para luego usarlo. Este identificativo más el password o clave permite acceder a información restringida. (Merlat y otros, 1999, 78).

Malwere (malgrama programa maligno): Se trata de cualquier tipo de software que tiene como meta el causar un daño o perjuicio, ya sea a una computadora o a una red. (Tablante, 2001, 196).

Mensaje de datos: Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones. (Ley Especial contra los Delitos Informáticos, 2001).

Módem: Es un modulador y demodulador de datos que participa en una comunicación como ETCD. Su uso más común y conocido es en transmisiones de datos por vía telefónica. Como los ordenadores procesan datos de forma digital y las líneas telefónicas de la red básica sólo transmiten datos de forma analógica, los módem lo que hacen es transformar mediante diferentes técnicas las señales digitales en analógicas y viceversa. (Wikipedia, 2005).

Newbie: Alguien nuevo en Internet, o en el mundo de los ordenadores, en general. (Wikipedia, 2005).

Nick (del inglés nickname): Es un pseudónimo, o mote que un usuario se asigna en la red, para que otros usuarios le identifiquen más fácilmente que si utilizara la dirección IP. También se conoce como nombre de usuario. (Wikipedia, 2005).

On line (en línea, conectado): Estado en que se encuentra una computadora cuando se conecta directamente con la red, a través de un dispositivo. (Tablante, 2001, 196).

Operador: Persona que usa una computadora. A menudo se llama "operador" al administrador del sistema. (Merlat y otros, 1999, 78).

Página web: Una de las páginas, archivos o documentos que componen un sitio en la World Wide Web. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se le llama "home page". (Tablante, 2001, 196).

Password (contraseña): Secuencia alfabética, numérica o combinación de ambas (alfanumérica), protegidas por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para

acceder a la data o a la información contenidas en un sistema. (Tablante, 2001, 196).

Patch o Parche: Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento. (Merlat y otros, 1999, 78).

Phracker (fonopirata): Es un individuo de alta capacidad en el manejo y manipulación de las redes telefónicas, las cuales utiliza para obtener cierta información de redes ajenas. En muchas ocasiones se pone en jugo este tipo de prácticas para evadir el pago de los recibos telefónicos. Acceden a la red utilizando vías gratuitas de las que disfrutan inicialmente o de forma no autorizada. (Tablante, 2001, 196).

Procesamiento de datos o de información: Realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo. (Ley Especial contra los Delitos Informáticos, 2001).

Programa: Plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador. (Ley Especial contra los Delitos Informáticos, 2001).

Protocolo: Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor). Estos protocolos "gobiernan" formatos, modos de acceso, secuencias temporales, entre otros. (Wikipedia, 2005).

Realidad Virtual: Simulación de un medio ambiente real o imaginario que se puede experimentar visualmente en tres dimensiones. La realidad virtual puede además proporcionar una experiencia interactiva de percepción táctil, sonora y de movimiento. (Tablante, 2001, 196).

Recogida de basura electrónica: Consiste en aprovechar la información que queda abandonada en forma de residuo. Se explora la zona de memoria o zonas del disco en las que queda información residual que no fue realmente borrada y puede ser usada posteriormente. (Tablante, 2001, 197).

Red: En tecnología de la información, una red es un conjunto de dos o más computadoras o recursos interconectados. (Tablante, 2001, 197).

Remoto: La palabra se utiliza en tecnologías de la información para definir sistemas o elementos de sistemas que se encuentran físicamente separados

de una unidad central. Un puente remoto es un dispositivo que hace posible la comunicación entre, por ejemplo, una LAN y una red de área amplia. El uso del término es muy frecuente: para referirse al mantenimiento de sistemas a distancia, al acceso a aplicaciones residentes en unidades físicamente distantes, entre otros; naturalmente, esto implica la utilización de un software especializado. Algunos ejemplos del uso de esta palabra: gestión remota de los datos; acceso remoto a los archivos; acceso a periféricos remotos; monitorización remota. (Wikipedia, 2005).

Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación. (Ley Especial contra los Delitos Informáticos, 2001).

Servidor: Genéricamente, dispositivo de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes. (Páez, 2004, 29).

Shareware: Es una clase de software o programas para poder evaluar de forma gratuita pero por un tiempo, uso o características limitadas. Para

adquirir el software de manera completa necesita de un pago económico (muchas veces modesto). No se debe confundir con un programa tipo freeware que es totalmente gratuito en sí aunque generalmente su código no está disponible (también conocido como Código cerrado). (Wikipedia, 2005)

Signatario: Es la persona, natural o jurídica, pública o privada, titular de una firma electrónica o certificado electrónico. (Tablante, 2001, 197).

Simulación de identidad: Consiste en usar un terminal de un sistema en nombre de otro usuario, ya sea porque se conoce su clave, o porque de alguna forma se tuvo acceso al terminal de forma no autorizada. El término también es aplicable al uso de tarjetas de crédito o documentos falsos en nombre de otra persona. Este método es utilizado frecuentemente para cometer fraude y otros delitos mediante el uso de información adquirida ilícitamente de otras personas en la res, e identifica claramente los peligros que deben encarar quienes hacen negocios por internet. (Tablante, 2001, 197).

Sistema: Cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes

interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas. (Ley Especial contra los Delitos Informáticos, 2001).

Sistema de información: Aquel utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma mensajes de datos. (Tablante, 2001, 197).

Sistema operativo (SO): Es un conjunto de programas o software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera cómoda y eficiente. Comienza a trabajar cuando se enciende el ordenador, y gestiona el hardware de la máquina desde los niveles más básicos. Hoy en día un sistema operativo se puede encontrar normalmente en ordenadores o productos electrónicos como teléfonos móviles. (Wikipedia, 2005)

Sniffer: Es un recurso o proceso que captura la información que viaja a través de la red, para ser analizados posteriormente, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. (Tablante, 2001, 198).

Software: Información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que los computadores realicen funciones específicas. (Ley Especial contra los Delitos Informáticos, 2001).

Spam (bombardeo publicitario, buzonfia): Los odiados spams no son más que los envíos masivos e indiscriminados de publicidad a través de correo electrónico no grato para el destinatario. (Tablante, 2001, 198).

Tarjeta inteligente: Rótulo, cédula o carnet que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla. (Ley Especial contra los Delitos Informáticos, 2001).

Telemática (teleinformática): Combinación de las palabras "telecomunicaciones" e "informática". Disciplina que asocia las telecomunicaciones con los recursos de la informática. (Tablante, 2001, 198).

Teleproceso: Denominación para el proceso de datos desde terminales distantes con la unidad central. Es el caso típico de las transacciones que realizan, en gran volumen, las entidades financieras. (Páez, 2004, 29).

Tracear: Seguimiento exhaustivo. Se utiliza cuando se intenta desproteger un programa y se tiene instalado un Debugger. Este término también es utilizado en caso de que la línea telefónica esté pinchada por la policía. (Merlat y otros, 1999, 80).

Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema. (Ley Especial contra los Delitos Informáticos, 2001).

World Wide Web (del inglés, telaraña mundial): La web o WWW, es un sistema de hipertexto que funciona sobre internet. Para ver la información se utiliza una aplicación llamada navegador web para extraer elementos de información (llamados "documentos" o "páginas web") de los servidores web (o "sitios") y mostrarlos en la pantalla del usuario. El usuario puede entonces seguir hiperenlaces que hay en la página a otros documentos o incluso enviar información al servidor para interactuar con él. A la acción de seguir

hiperenlaces se le suele llamar "navegar" por la web. No se debe confundir la web con internet, que es la red física mundial sobre la que circula la información. (Wikipedia, 2005).