UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURIDICAS

ELEMENTOS DIFERENCIADORES DEL DELITO DE ESTAFA REGULADO EN EL ARTICULO 215 DEL CODIGO PENAL CON LA ESTAFA INFORMATICA REGULADA EN LA LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS

TRABAJO DE GRADO PARA OBTENER EL TITULO DE

LICENCIADO EN CIENCIAS JURIDICAS

PRESENTADO POR:

AVILA UMAÑA, JONATHAN ALEXANDER

BARRERA ARGUETA, ANTONIO ALEXANDER

MONJARAS DIAZ, FRANCISCO JAVIER

DOCENTE ASESOR

LICDA. GEORLENE MARISOL RIVERA LOPEZ

CIUDAD UNIVERSITARIA, SAN SALVADOR, MARZO 2018

TRIBUNAL CALIFICADOR

LIC. FRANCISCO ALBERTO GRANADOS HERNANDEZ
(PRESIDENTE)

LIC. JONATHAN NEFTALY FUNES ALVARADO
(SECRETARIO)

LICDA. GEORLENE MARISOL RIVERA LOPEZ
(VOCAL)

UNIVERSIDAD DE EL SALVADOR

MSC. Roger Armando Arias
RECTOR

DR. Manuel de Jesús Joya
VICERRECTOR ACADEMICO

ING. Nelson Bernabé Granados Alvarado
VICERRECTOR ADMINISTRATIVO

LIC. Cristóbal Hernán Ríos Benítez
SECRETARIO GENERAL

LIC. Rafael Humberto Peña Marín
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DRA. Evelyn Beatriz Farfán Mata
DECANA

DR. José Nicolás Ascencio Hernández
VICEDECANO

MCS. Juan José Castro Galdámez
SECRETARIO

LIC. Rene Mauricio mejía Méndez
DIRECTOR DE LA ESCUELA DE CIENCIAS JURIDICAS

LICDA. Digna Reina Contreras de Cornejo
DIRECTORA DE PROCESOS DE GRADUACION

LICDA. MARÍA MAGDALENA MORALES
COORDINADORA DE PROCESOS DE GRADUACION
DE LA ESCUELA DE CIENCIAS JURIDICAS

INDICE

RESUMEN

Hace algunos años era impensable que el avance tecnológico pudiera tener el alcance de hoy en día, y con tal avance de nuevas herramientas tecnológicas también viene aparejado nuevas formas de delincuencia y una creatividad enorme de parte de los actores de este tipo de delitos llamados delitos tecnológicos, con la utilización de la informática como eje fundamental para el cometimiento de esta nueva forma de delincuencia.

En el presente trabajo se ha realizado un esfuerzo intelectual en base a la bibliografía consultada para la elaboración del mismo, es así como a lo largo del desarrollo del presente trabajo que se da a conocer algunos hechos históricos de relevancia histórica en el esfuerzo de las legislaciones por querer introducir algunas conductas delictivas como hechos antijurídicos con la dificultada que estas implican, ya que la tecnología avanza de una manera acelerada y las legislaciones de una manera más lenta, esto se da porque las herramientas tecnológicas se encuentran en constante evolución, y algunos de los Estados Recién están haciendo uso de las herramientas de carácter tecnológico para el perseguimiento de las conductas delictivas realizadas por sujetos con amplios conocimientos en estas nuevas herramientas.

En el presente trabajo producto de la investigación realizada se puedo determinar la dificultad que tiene el derecho penal y sus aplicadores para poder dar una alternativa a las reglas tradicionales en la persecución del delito y sobre todo, con esta novedosa forma de delincuencia y los sujetos que intervienen en los delitos de informáticos y sobre todo en los delitos de estafa informática.

En El Salvador se ha logrado un avance importante en materia penal con la Ley de Delitos Informáticos y Conexos, ya que el legislador trata en dicha norma jurídica de establecer algunas conductas delictivas que dañen algo más que el patrimonio protegido tradicionalmente.

ABREVIATURAS

A.C.	Antes de Cristo
A.L.	Asamblea Legislativa
Art.	Articulo
C.N.	Constitución de la Republica
D.L.	Decreto Legislativo
D.O.	Diario Oficial

SIGLAS

ARPANET	Advanced Research Projects Agency Network
EUA	Estados Unidos de América
IBM	International Business Machines
INTERPOL	Organización Internacional de Policía Criminal
OCDE	Organización de Cooperación y Desarrollo Económico
OEA	Organización de Estados Americanos
ODR	Online Dispute Resolution
OMC	Organización Mundial de Comercio
OMPI	Organización Mundial de la Propiedad Intelectual
TIC	Tecnologías de la información y de las comunicaciones
UN	Naciones Unidas

INTRODUCCION

El delito de Estafa Informática desde el enfoque del derecho penal es una labor novedosa, es por ello que en el presente trabajo de grado, que a continuación es presentado trata de reflejar las áreas, fines, alcances y posibles resultados con lo que se pretende desarrollar en esta investigación jurídica, los problemas que representa determinar los elementos diferenciadores de la estafa informática regulada en la ley especial contra delitos informáticos y conexos.

El tema que se aborda es de suma importancia, ya que por considerarse que los cambios producidos por la globalización y la informática, el delito de estafa no puede ser analizado bajo las aspectos tradicionales del derecho penal, por el grado de complejidad que se tiene en cuanto a la conducta delictiva realizada por el sujeto activo, en muchas ocasiones se desconoce con exactitud quien es este sujeto; en muchos de los casos se realizan los delitos informáticos desde distintas partes del mundo con diferentes direcciones IP (IP es un acrónimo para Internet Protocol), ya que estas son un número único e irrepetible, con el cual se identifica una computadora conectada a una red, que corre el protocolo IP distintas a las que realmente han sido utilizadas.

Asimismo se hace un abordaje del surgimiento de los delitos informáticos, y de ahí el porqué de la necesidad de investigar este tema; también se hace un análisis general de la situación problemática, que es parte fundamental en el desarrollo de este proyecto, ya que se establecen las unidades de análisis junto a las variables de investigación las cuales se transforman en un problema jurídico y se establece el por qué se genera un problema jurídico, y cuáles podrían ser las posibles soluciones para el problema en estudio.

En el presente trabajo de investigación se expondrán los aspectos conceptuales de la estafa informática, los aspectos generales del tema

presentado, así como se expondrá lo relacionado a los elementos diferenciadores de la estafa informática respecto de la estafa tradicional, profundizando en las clases de delitos y los sujetos que intervienen, así como el análisis jurídico dogmático del tema.

CAPÍTULO I

ANTECEDENTES HISTORICOS SOBRE LA INFORMÁTICA, CONCEPTOS Y SU RELACIÓN CON EL DERECHO

El presente capitulo trata sobre los antecedentes históricos de la informática, generaciones que dieron origen al desarrollo de las computadoras, Referentes de algunos Instrumentos relacionados a la Informática, Conceptos y Definiciones de la Informática, la Informática y su relación con otras Ciencias; Derecho Informático, y la era de la Informática.

1.1. Antecedentes de la Informática

La historia de la computación se remonta a la época de la aparición del hombre en la faz de la tierra, y se origina en la necesidad que tenía éste en ese entonces de cuantificar a los miembros de su tribu, los objetos que poseía, la cantidad de animales con los que contaba, entre otras cosas cuantificables. Cuando el hombre empezó a contar, utilizó los medios que tenía a su alcance, como eran sus dedos, piedritas, trocitos de madera, tablillas de arcilla o cordones anudados. La computación tiene como principal objetivo computar o contar, y eso era precisamente lo que necesitaron hacer aquellos primeros seres pensantes.[1] Por lo tanto, debido a la necesidad de tener que calcular sin errores dio paso a la calculadora, la mecánica que era una especie de ábaco, pero con ruedas dentadas en lugar de varillas y bolas, dotada de un

[1] José Alberto, Jaen Raquel Martínez y Ángel García Beltrán. *División de Informática*: Breve Historia de la Informática Industrial (Madrid: Universidad Politécnica, 2006), p. 2

mecanismo para el transporte de las unidades que se lleven, de una posición digital a la siguiente más significativa.

El origen de la máquinas de calcular fue dado por el ábaco, a través de sus movimientos se podía realizar operaciones de adición y sustracción. El nombre de una persona específica nunca ha sido acreditado con la invención del ábaco, pero se cree que el primer dispositivo de este tipo que fue inventado por los mesopotámicos antiguos durante el 2700 a 2300 a.C. Hay una creencia común que los chinos inventaron el ábaco pero el primer Ábaco chino fue inventado para el 500 a.c. y se desarrolló aún más, o se hizo famoso su uso, durante la Edad Media de China, durante la dinastía Ming ente 1368-1644.

En 1623 William Oughtred quien fue un ministro anglicano nacido en Inglaterra que se dedicó en vida a la Matemática, la Astronomía, la Gnomónica y que es conocido por haber inventado la moderna regla de cálculo, Oughtred invento un dispositivo para calcular al que denomino “Círculos de Proporción”.[2] El instrumento en mención fue el que llegaría a ser conocido como “Regla de Cálculo”. Otros de los hechos importantes de la informática les que lo sitúa en el siglo XVII, donde el científico francés Balies Pascal en el año de 1642 desarrollo una calculadora de ruedas giratorias que después se denominaría la calculara de escritorio. Aproximadamente 30 años después Gottfried Leibniz perfecciono el invento de Pascal y realizo una máquina de cálculo que podía sumar.

Herman Hollerith fue un inventor Estadounidense quien desarrolló un tabulador electromagnético de tarjetas perforadas para ayudar en el resumen de la información y, más tarde, la contabilidad. Fue el fundador de la compañía de

[2] Philippe Breton, *Historia y Crítica de la Informática*, (Madrid: Catedra, 1989), p.35.

máquinas tabulación que se fusionaron a través de adquisición de acciones, en 1911 con otras tres compañías para formar una quinta parte de la empresa, la Informática Tabulating Recording Company más tarde llamado International Business Machines (IBM). Hollerith es considerado como una de las figuras seminales en el desarrollo de procesamiento de datos. Su invención de la máquina de tarjetas perforadas de tabulación, esta marca el comienzo de la era de las maquinas semiautomáticas de procesamiento de datos de sistemas, y su concepto de que dominaba el paisaje durante casi un siglo. Está considerado como el primer informático, es decir, el primero que logra el tratamiento automático de la información (Informática = Información + automática).[3]

En 1924 Bullen Francia patenta algunos dispositivos electromagnéticos para análisis numéricos, crea una sociedad que luego sería la firma Bull en Europa.[4]

Entre los años 1934 Horward Iken construyó una máquina cuyo nombre fue "calculadora Automática de Secuencia Controlada," más conocida como MARK I, esta computadora está basada en relees y números de hasta 23 dígitos.[5]

En 1943 se construyó la ENIAC esta computadora poseía una capacidad y flexibilidad muy superior a MARK I utilizaba tubos al vació electrónicos con los cuales eran capaz de calcular una velocidad de 1000 veces mayor que la de los relees electrónicos.

En 1944 Jon Van Newmán Consultor de proyectos propuso el concepto de

[3] Breton, *Historia y Crítica de la Informática*, p. 37n2.
[4] Ibíd.
[5] Ibid.38-39

"programa almacenado" en el cual los datos podrían ser almacenados en el computador junto con las instrucciones.

En 1951 són desarrollados el Univac I y el Univac II, que fué la primera computadora digital verdadera, esta fue diseñada por un matemático inglés de nombre Charles Babbage,[6] quien invirtió todo su dinero y su vida para intentar construir una "máquina Analítica," pero a pesar de tanto esfuerzo nunca logró que funcionara como debería, sin embargo logró que funcionara mecánicamente. Esta máquina analítica que construyó no tenía sistema Operativo, fue así que Charles Babbage se da cuenta que necesitaba software para su máquina analítica.[7] Fue así que el contrató a Ada Lovalace, quien era hijo de un poeta inglés, ella era considerada la única programadora del mundo, por ese motivo que el lenguaje de programación fue llamado Ada en su honor.[8]

1.1.1 Generaciones que dieron origen al desarrollo de las computadoras

A continuación se detalla el desarrollo de las computadoras en cinco importantes generaciones que marcaron el rumbo y progreso de las mismas, desde los primero esfuerzos para la unificación de datos.

1.1.2 Primera Generación

Esta se desarrolló desde 1937 hasta 1950, después de la infructuosa labor de Charles Babbage hubo pocas computadoras digitales antes de la "segunda guerra mundial".[9] Fue hasta mediados de los años de 1940, los cuales fueron

[6] Breton, *Historia y Crítica de la Informática*, p.43n3.
[7] Ibíd.
[8] Ibíd. p.45
[9] Carlos Alberto Garrido López, "Historia de la Computación" (tesis de maestría, Universidad de San Carlos de Guatemala, 2008), p.9

vistos como los primeros tiempos, en el que un solo grupo de personas le correspondía la enseñanza, la construcción y la programación de computadoras, todo a que no existían los lenguajes de programación, y tampoco nadie habla oído de los sistemas operativos, la regla general era que casi todos los problemas eran cálculos numéricos simples, como la preparación de tablas de seno y coseno, fue hasta los primeros años de la década 1950, que era posible escribir programas en tarjetas y hacer que la maquina las leyera, debido a esto es que esta época se le considera como la primera generación.

1.1.3 Segunda Generación

Se desarrolló desde 1950 hasta 1960, la segunda generación fue a mediados de la década de 1950.[10] Las computadoras se volvieron más accesibles para poder venderse a clientes comerciales, estas máquinas tenían otro sistema ya que funcionaban con mainframes y microcomputadoras, este tipo de máquinas solo las grandes corporaciones podían pagar millones de dólares ya que eran muy costosas, cuando la computadora terminaba el trabajo que ejecutaba las hojas de la impresora eran reutilizadas en su mayoría para realizar cálculos científicos.

1.1.4 Tercera Generación

Esta se desarrolló desde 1960 hasta 1970.[11] Al principio de la década de 1960 la mayoría de los fabricantes de computadoras tenían dos productores diferentes pero eran completos, utilizado por primera vez procesadores

[10] Garrido, “Historia de la Computación” p.11n4.
[11] Ibíd. p.13

fabricados con circuitos integrados, esta generación también presentaba nuevas topologías en software de sus sistemas el cual fue el sistema de manejo de base de datos que fue el gran aporte de esta generación.

1.1.5 Cuarta Generación

Se desarrolló de 1970 hasta 1986, es en esta generación que se desarrolló los circuitos integrados a gran escala, este fue el punto de partida de las computadoras personales.

1.1.6 Quinta Generación

Se desarrolló desde 1986 hasta nuestros días.[12] Aunque ciertos expertos consideran finalizada esta generación con la aparición de los procesadores Pentium, pero hay otra parte doctrinal que aún considera que aún no ha finalizado.

Esta quinta generación se caracteriza por el surgimiento de la PC, tal como se la conoce actualmente, es en esta generación que se considera la gran expansión de la computadora a nivel mundial.

1.2 Creadores de algunos Instrumentos Relacionados a la Informática

A continuación se mencionaran algunos creadores de instrumentos relacionados a la informática, claro que estos no son todos sin embargo son los de mayor relevancia para el desarrollo de los instrumentos informáticos:

[12] Garrido, “Historia de la Computación”, p.14n.

1.2.1 Leonardo Da Vinci el diseñador de una sumadora

Da Vinci fue el diseñador de una sumadora entre los años de 1452 y 1519, diseñó una sumadora que fue reconstruida hasta el año de 1967 a partir de uno de sus códices.

1.2.2. Blas Pascal el creador de la calculadora

El inventor Blas Pascal fue el creador de la Calculadora, entre 1623 y 1662, Pascal diseño su máquina aritmética, la cual posteriormente fue denominada la pascalina, creación que a la edad de 19 años, esto con el objetivo de que su padre que era recaudador de impuestos gozara de tiempo libre para jugar junto a él al paume, el cual también era conocido como el juego de raqueta, aunque el propósito de un inicio era el tener más tiempo junto a su padre, este invento resulto de gran beneficio para el desarrollo de la ciencia informática, a pesar que Pascal trabajo en el mismo con un propósito familiar, y sobre todo el de compartir junto a su padre del juego que le gustaba a ambos.

1.2.3 Whilem Schickard inventó una calculadora con combinación de los rodillos de neper

Whilem Schickard entre los años 1592-1635 había inventado una calculadora que era una combinación de los rodillos de Neper con una sumadora restadora similar a la de Pascal, obviamente no sólo era superior a la Pascalina, sino que se construyó el año en que nació Pascal, por lo que se le considera el primero en construir una calculadora de avanzada al filósofo y matemático alemán.[13]

[13] Schickard cursó estudios en la Universidad de Tubinga hasta el año 1613 en las áreas de teología y lenguas orientales

1.2.4 Gottfried Leibniz e Isaac Newton inventores del cálculo infinitesimal

Gottfried Leibniz invento junto con Isaac Newton el cálculo infinitesimal aunque de forma independiente. Fue denominada calculadora universal, su elemento característico era un tambor cilíndrico con nueve dientes de longitud variable, llamado rueda escalonada, que se encuentra en prácticamente todas las calculadoras mecánicas posteriores, incluso las del siglo XX.

Las técnicas de producción tan poco eficientes de aquella época, impidieron que el invento de Leigniz se fabricara masivamente. Se llegaron a construir 1500 unidades, pero hubo que esperar hasta 1820 para que Carlos Thomas, director de una aseguradora diseñara un modelo capaz de ser producido a bajo costo y a escala industrial.

1.2.5 Ramón Varea García patentó una calculadora

Ramón Varea García (1833-1899) patentó en Nueva York una calculadora por la que se le otorgó la medalla de oro de la exposición de Matanzas en Cuba.

Varea García aseguraba que no había fabricado la máquina para patentarla y venderla, sino para demostrar que era posible que un español pudiera inventar tan bien como un norteamericano, a partir de entonces sólo se dedicó al periodismo, combatiendo la política de colonialismo de Estados Unidos, por lo que tuvo que exiliarse en Guatemala y posteriormente en argentina.

Por lo anterior se puede notar que fueron varios los esfuerzos intelectuales que se realizaron a lo largo de la historia que contribuyeron para la elaboración de lo que hoy una de las herramientas más utilizadas como lo es la pc.

1.3. Concepto y definición de la informática

Luego de conocer algunos de los grandes inventos que han contribuido a la realización de algunas técnicas que han permitido el desarrollo de la computadora, es necesario también el poder conocer algunas de las ramas relacionas con la informática.

1.3.1. La Electrónica

Para entender la diferencia esencial entre un delito informático y los conocidos como los delitos electrónicos, es necesario entender lo que es la Electrónica y qué es la Informática, “La electrónica es parte de la ciencia que estudia los fenómenos que intervienen electrones en estado libre”. Lo cual prácticamente no dice nada, por lo que la electrónica como técnica: “es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos”.

Para distinguir de una manera sencilla en su funcionamiento dentro de un aparato electrónico se tiene que tomar en cuenta que el flujo de estos electrones genera corriente eléctrica y ésta a su vez usada en dispositivos cambian la energía eléctrica en calor, luz o movimiento, a lo que se conoce como Eléctrica, pero usada en dispositivos provistos de inteligencia surge lo que es una radio, una televisión y una computadora, ahí es conocida como Electrónica.

1.3.2. La Informática

Los aparatos informáticos son electrónicos pero no necesariamente todos los

aparatos electrónicos son informáticos, como el ejemplo de una licuadora a comparación de una computadora. Ya siendo parte esencial el flujo de corriente eléctrica para transformarlo en otro tipo de energía de ambos, la palabra clave es el procesamiento de información, dando nacimiento a la informática, siendo esta: “una rama del saber humano que se ocupa de todo lo relacionado con los sistemas operativos, su comportamiento, su diseño y desarrollo de todo tipo de programas así como los sistemas operativos hasta los más modesto programas de aplicación, operación y uso de los software de avanzada.”

La informática es una rama de la ingeniería que estudia el tratamiento de la información mediante el uso de máquinas automáticas. Proviene del vocablo francés Informatique, que a su vez por la conjunción de las palabras información y Automatique, para dar idea de la automatización de la información, que se logra con los sistemas computacionales.

La Informática es un amplio campo que incluye los fundamentos teóricos, El diseño, la programación y el uso de las computadoras también llamados ordenadores, como herramienta de solución de problemas. Dicho lo anterior esto puede ser entendido como la interpretación y procesamiento lógico de los impulsos eléctricos de manera ordenada, por ejemplo, los audio cassettes, éstos poseen las cintas magnéticas, el cual su funcionamiento básicamente consistía en que a través de esta cinta plástica quedaba un registro magnético entre una combinación lógica y ordenada de cargas positivas y negativas por así decirlo, que en el caso de un audio cassettes estaban acomodados según las vibraciones generadas por el sonido, ya en el caso de dispositivos informáticos como lo son los disquetes, discos flexibles, memorias Usb, está relación ordenada de cargas son entendidos como “cero y uno”, el lenguaje binario; las cuales están procesadas y

entendidas lógica y matemáticamente mediante una computadora permitiendo reproducir o almacenar información.[14]

1.3.3. La Cibernética

Cibernética: del griego Piloto o el arte de pilotear un navío, aunque Platón la utilizó en La República con el significado de "arte de dirigir a los hombres" o "arte de gobernar". Las investigaciones con fines militares a partir de la segunda guerra mundial propiciaron la creación del concepto moderno de la Cibernética moderna la cual es descrita: como una ciencia de la comunicación y el control.

Otra forma de entender a la Cibernética moderna es como: “Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas y en particular, el de las aplicaciones de los mecanismos de regulación biológicas a las tecnológicas”.[15]

1.3.3.1 Orígenes de la Cibernética

En 1948 el matemático norteamericano Norbert Wiener (1894 -1964) en su obra “Cibernética o el control y comunicación en animales y máquinas” (Cybernetics, or control and communication in the animal and machina), la cual fue publicada en 1948, empleó el término para designar a la nueva Ciencia de la comunicación y control entre el hombre y la máquina.

Punto importante es resaltar la diferencia que existe entre la Informática y la

[14] Michael Joseph Miller, *Introducción a la informática*, (España: 2006), p.25.
[15] Norbert Winer, *Cibernética: El control y la Comunicación* (Barcelona: 1998), p. 21.

Cibernética, que vistos de cierta manera parecerían que son iguales, pero aunque guardan una relación entre sí las partes que las componen son distintas.

La Cibernética: “es la ciencia que trata de explicar y dar solución a eventos de control y comunicación, ya sean fenómenos acontecidos en la naturaleza, sociedad o humanos,” de tal manera la Informática busca desarrollar máquinas capaces de “Inteligencia Artificial”, que es aquella que trata de simular actividades y capacidades humanas como la robótica, la búsqueda de solución de problemas y la toma de decisiones por sí mismas, conocido como Heurística o Método Heurístico, muchos de los teóricos de esta línea establecen que llegara el día en que la maquina sustituya en la gran mayoría de las actividades que el ser humano realiza, mejorando con ello la calidad y el tiempo empleado en cada una de las actividades realizadas.

1.3.4. Internet

Para entender los delitos informáticos es necesario poder comprender lo que es Internet, el cual se define como “un conjunto de servidores conectados entre sí mediante un sistema maestro de computadoras dentro de una red alrededor de todo el mundo”.

Internet fue concebida por el Ministerio de Defensa de los Estados Unidos de América, con el fin de lograr crear una red de computadoras interconectadas que no dependiera de una computadora central, con el objetivo de que en ataques hacia la nación Estadounidense esta red serviría para la comunicación interna de la defensa Nacional, y con ello el poder evitar ataques de los grupos anti-Estadounidense, y que en dicho caso la información no se perdiera; por lo que la información no comprometida se encontrara protegida en su totalidad

o en parte, así como en la funcionalidad de la red que se vería comprometida al destruir el servidor central.[16]

En el año de 1960 comenzó a desarrollarse un sistema de red, el cual las computadoras interconectadas no dependieran de un servidor central, sino que cada computadora actuase de manera independiente de las otras, con lo que nació la idea de ARPANET (Advanced Research Projects Agency Network), con lo cual para el funcionamiento de esta red fue necesario la creación de procesadores especiales denominados Procesadores de Mensaje de Interfaz[17] (IMP en sus siglas en inglés), y que el primer procesador de este tipo entró en funcionamiento el 01 de Agosto de 1969, en la Universidad de California, Los Ángeles E.U.A, con una computadora Honetwell 516, con una memoria de 12 MB, extendiéndose a otras Universidades del país, dando origen al ARPANET; para 1972 se habían instalado 37 Procesadores de Mensaje de Interfaz, ARPANET fusionaba con un programa denominado Network Control Protocolo (NPC), facilitando su uso debido a que era compatible con diversas computadoras y programas operativos, creciendo de tal forma que los propósitos militares del ministerio de defensa fueron cambiados por los fines científicos y educativos de las Universidades en los que se encontraba ya instalado.

En el año de 1980 el NPC fue sustituto por TCP/IP un programa más eficiente el cual convertía la información en pequeños paquetes, los cuales pueden ser enviados a diversos puntos con base a su dirección a través de diferentes puntos de enlace de Internet y la computadora de

[16] Rafael Rodríguez Prieto y Fernando Martínez Cabezudo, *Poder e Internet:* un análisis crítico de la red (Madrid: Cátedra, 2016), p.11.
[17] Fernando Jiménez Conde, *Internet y Derecho*, (Madrid: Sepin, 2001), p.65.

destino, en este mismo año ARPANET se desligó por completo de sus objetivos militares para los que fue diseñado.

En 1986 se fundó la NSFNET (National Science Foundation's Network), financiada por el gobierno de los Estados Unidos, creando diferentes líneas de enlace para Internet, facilitando la transferencia de datos dando lugar a la expansión de la Internet fuera del país, para 1995 NSFNET intentó crear una política de uso científico y no comercial para la Internet lo cual no fue aplicado debido a la privatización de Internet extendiendo su uso a niveles comerciales.[18]

1.4. La Informática y su relación con otras ciencias

Luego de establecer algunas definiciones afines con la informática, procede identificar las relaciones de la informática con otras ciencias; se platean a continuación algunas relaciones más sobresalientes.

1.4.1 La informática y su relación con el Derecho

Entre el Derecho y la Informática se podrían apreciar dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la informática jurídica. Pero al considerar a la informática como objeto del Derecho, se hace alusión al Derecho de la Informática o simplemente Derecho Informático.[19]

De esta manera, tenemos a la ciencia informática y por otro lado a la ciencia

[18] Pekka Himanen, *La ética del hacker y el espíritu de la era de la* información (Barcelona: Planeta, 2004), p.33.
[19]Jiménez, *Internet y Derecho*, p.66n13.

del derecho; ambas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el derecho en su aplicación, es ayudado por la informática; pero resulta que ésta debe de estar estructurada por ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas informáticas; por lo que este conjunto de normas, doctrina y jurisprudencia, son las que van a establecer y regular las acciones, procesos, aplicaciones y relaciones jurídicas en su complejidad de la informática, y por otro lado encontramos a la informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.[20]

En efecto, la informática no puede juzgarse en su simple exterioridad, como utilización de aparatos o elementos físicos electrónicos, pura y llanamente; sino que, en el modo de proceder, se crean unas relaciones inter subjetivas de las personas naturales o jurídicas y de entes morales del Estado.

surgen entonces un conjunto de reglas técnicas conectadas con el Derecho, que vienen a constituir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la Ciencia informática, con autonomía propia; esos principios conforman las directrices propias de la institución informática, y viene a constituir las pautas de la interrelación nacional universal, con normas mundiales supra nacionales, cuyo objeto será recoger mediante tratados públicos, los cales logren hacer posible el proceso comunicacional en sus propios fines con validez y eficacia universal, con lo que lleva una mayor comunicación global entre los Estados interconectados a través de esta red que logra poner a disposición de la investigación que se realiza por medio de las normas establecidas en el derecho y sus medios que lo constituyen.

[20] Jiménez, *Internet y Derecho*, p.66nn13-14.

1.4.2 Derecho Informático y la Informática Jurídica como verdaderas ciencias

Se plantea una discusión sobre si la informática es una ciencia y para eso es necesario establecer algunas definiciones fundamentales, para poder dilucidar esta pregunta, es necesario hacer un análisis de las siguientes definiciones que son: Ciencia, Informática jurídica y Derecho Informático.

1.4.2.1 Ciencia

Según la Real Academia Española la Ciencia es: "El conocimiento cierto de las cosas por sus principios y causas". "Cuerpo de doctrina metódicamente formado y ordenado que constituye un ramo particular del humano saber, Habilidad, maestría, conjunto de conocimientos en cualquier cosa".[21] Sin duda alguna, tanto la informática jurídica como el derecho informático constituyen conocimientos, principios y doctrinas, que catalogan a estas como ciencias, que tienen como marco estricto a la iuscibernética, y como marco amplio a la cibernética.

1.4.2.2 La Informática Jurídica

Luego de establecer en el apartado anterior que es una ciencia, es necesario fundamentar en que consiste la Informática Jurídica, que "es la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que éste uso presta al desarrollo y aplicación del derecho."

[21] Faustina Zarich, *Derecho informático*, (Argentina: Juris, 2005), 32.

1.4.2.3 Derecho de la Informática

También es importante definir el derecho informático el cual ya no se dedica al estudio del uso de los aparatos informáticos como ayuda al derecho, sino que el Derecho Informático "constituye el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática." Es decir, que la informática en general desde este punto de vista es objeto regulado por el derecho.

Ahora bien, la informática jurídica constituye una ciencia que forma parte del ámbito informático, demostrando de esta manera que la informática ha penetrado en infinidad de sistemas, instituciones, etc.; y prueba de ello es que ha penetrado en el campo jurídico para servirle de ayuda y servirle de fuente. Es por ello que "la informática jurídica puede ser considerada como fuente del derecho", criterio propio que tal vez encuentre muchos tropiezos debido a la falta de cultura informática que existe en nuestro país.

Al penetrar en el campo del derecho informático, se obtiene que también constituye una ciencia, ya "es la que estudia la regulación normativa de la informática y su aplicación en todos los campos".

En vista de lo anterior cuando se dice derecho informático, entonces se analiza si esta ciencia forma parte del derecho como rama jurídica autónoma; así como si el derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal y como se menciona el derecho civil, derecho penal, así como la rama del derecho contencioso administrativo, la Informática Jurídica y el Derecho informático tienen sus propios principios, se pueden logar complementarse entre ambas.

1.4.2.4 El derecho informático como una rama del derecho

Al respecto, según encuentros sobre informática realizadas en Facultades de Derecho en Europa partir de 1987, organizados por ICADE, siempre surgían problemas a la hora de catalogar al Derecho Informático como rama jurídica autónoma del derecho o simplemente si el derecho informático debe diluirse entre las distintas ramas del derecho, asumiendo cada una de estas la parte que le correspondiese.[22]

Por exigencias científicas, por cuanto un conjunto de conocimientos específicos conllevan a su organización u ordenación, o por razones prácticas que llevan a la separación del trabajo en vías de su organización, se encuentra una serie de material de normas legales, doctrina, jurisprudencia, que han sido catalogadas y ubicadas en diversos sectores o ramas. Dicha ordenación u organización del derecho en diversas ramas, tiene en su formación la influencia del carácter de las relaciones sociales o del contenido de las normas, entonces se van formando y delimitando en sectores o ramas, como la del derecho civil, penal, constitucional, contencioso administrativo, etc.

Sin poderse establecer límites entre una rama jurídica y otra por cuanto, existe una zona común a todas ellas, que integran a esos campos limítrofes. De manera que esta agrupación u ordenación en sectores o ramas da origen a determinadas Ciencias Jurídicas, que se encargan de estudiar a ese particular sector que les compete. Para poder determinar las bases que sustentan a una rama jurídica autónoma, se debe establecer algunas situaciones con las que debe contar como lo son:

[22] Hiram Raúl Piña Libien, *La Informática y el Derecho* (México: Universidad Autónoma del Estado de México, 2002), p. 33n.

a) Una legislación específica (campo normativo);
b) Estudio particularizado de la materia (campo académico);
c) Investigaciones, doctrinas que traten la materia (campo científico);
d) Instituciones propias que no se encuentren en otras áreas del derecho, (campo institucional).

Generalmente el surgimiento de una rama jurídica se da a consecuencia de cambios sociales reflejados en las soluciones normativas en el transcurso de los años. Pero, resulta que en el caso de la informática no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo; se lograron de esta manera sociedades altamente informatizadas, que sin la ayuda actual de la informática colapsarían.[23]

No obstante, a pesar de esta situación existen países desarrollados como España en los que sí se puede hablar de una verdadera autonomía en el derecho informático, haciendo la salvedad de que esta ciencia como rama jurídica apenas nace y se está desarrollando, pero se está desarrollando como una rama jurídica autónoma.

En el caso de Venezuela, son muy pocos los sustentos que encontramos para el estudio de esta materia, tal vez su aplicación se limita fundamentalmente a la aparición de libros con normativas (doctrina), y comentarios de derecho informático.

Resulta, sin embargo, que esta situación no se acopla con la realidad informática del mundo, ya que existen otras figuras como los contratos para

[23] Norbert, Wiener, *Cibernética y Sociedad*, 3ª ed. (Buenos Aires: Ed. Sudamericana 1988), p. 97.

Registros electrónicos y documentos electrónicos, que llaman a instituciones que pertenezcan a una rama autónoma del derecho.

Entonces se puede concluir que en el derecho informático si existe legislación específica, que protege al campo informático.

Tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero si existe en el derecho informático, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de nuestras naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.[24]

Con respecto a las instituciones propias que no se encuentren en otras áreas del derecho (campo institucional), se encuentra el contrato informático, el documento electrónico, el comercio electrónico, entre otras, que llevan a la necesidad de un estudio particularizado de la materia (campo docente), dando como resultado las Investigaciones, doctrinas que traten la materia (campo científico).

En efecto, se pueden conseguir actualmente grandes cantidades de investigaciones, artículos, libros, e inclusive jurisprudencia que esté enmarcada en la interrelación entre el derecho y la informática, como se ha constatado en los Congresos Iberoamericanos de Derecho e Informática,[25]que es uno de los mayores aportes en Iberoamérica en esta materia, y con ello aportar herramientas jurídicas a los técnicos en esta rama.

[24]Wiener, *Cibernética y Sociedad*, p. 98n19.
[25] Julio Téllez Valdés, *Derecho Informático*, 3ª ed. (México: McGraw Hill, Serie Jurídica, 2003), p. 17.

1.5 Derecho Informático

Es aquí donde se pretende realizar una especificación de lo que se le considera derecho informático, y para se debe hacer algunas menciones de los términos que se deben de establecer.

1.5.1 Introducción al Derecho Informático

En la actualidad los términos informática, telemática, ofimática están introducidos en el lenguaje popular, al parecer la mayoría de personas intuye de una u otra forma que la incidencia que tiene el desarrollo tecnológico en la actividad diaria, ya que el uso de estas herramientas se han convertido en algo indispensable en la realización de actividades en el diario vivir del ser humano.

Aunque la evolución de la informática, entendida como la ciencia de tratamiento automático de la información, es uno de los fenómenos que más ha influido en el vertiginoso cambio social que estamos viviendo, no implica en absoluto su conocimiento ni su aprovechamiento en beneficio de la humanidad.

Debe por tanto, adaptarse la sociedad a los nuevos métodos que proporcionan las técnicas asociadas al ordenador y adecuar la actividad jurídica al desarrollo tecnológico. Por otro lado, de todos es sabido que la información da un gran poder a quien la posee, pero no basta con poseer la información, es necesario también saber manejarla. Actualmente el desarrollo alcanzado en los sistemas de telecomunicación que han permitido que una misma información sea accesible a un gran número de personas está cambiando radicalmente la forma de vida. Si se une la informática con las posibilidades que ofrece de almacenamiento, tratamiento y recuperación de la información registrada en

soportes magnéticos, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control de masas.

Por todo ello, el interés en regular el mundo de la informática y de aprovechar sus posibles aplicaciones al Derecho, crece llegando a límites insospechados, el impacto que el nuevo entorno de la información puede tener sobre la sociedad, es tan grande que no permite a los juristas vivir ajenos a él.

No hay que olvidar tampoco que en el mundo tecnológico y en su relación con el económico (así en principio se regulaba el hardware, debido a que era un buen "aporte económico", y cuando se empezó a comercializar los software fue cuando se empezó a regular este otro campo), se mueven diversos e importantes intereses que el derecho se ve obligado a regular. Parece lógico, por tanto, que el Derecho puede proporcionar a la informática una regulación jurídica que es necesaria para su desarrollo. Es lo que se conoce como derecho informático. El fenómeno de la comunicación a través de Internet, el desarrollo de programas para procesar información, y la manufactura y perfeccionamiento de las tecnologías necesarias para hacer esto y muchas otras cosas posibles, no son ajenos al ámbito del derecho.

El Estado tutela la actividad creadora del hombre, protegiendo ésta a través de lo que en el ámbito jurídico se denomina propiedad Intelectual e Industrial. El derecho debe regular los nuevos fenómenos. Por ejemplificar de alguna manera, podemos pensar en:

a) La disposición de un bien, sin el consentimiento del propietario del mismo, realizada mediante equipos informáticos;
b) El apoderamiento de información contenida en registros electrónicos;
c) Destrucción de la información.

El Derecho de la Informática puede abarcar un campo de estudio, por lo que la clasificación tradicional en público, social y privado no restringe científicamente esta disciplina, debido a que la informática se encuentra relacionada en muchos de los campos de estudio de las ramas antes mencionadas.

1.5.2 Definiciones de Derecho Informático

El Derecho de la Informática ha sido considerado por algunos autores, como "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones".

Otros autores lo definen como el "conjunto de leyes, normas y principios aplicables a los hechos y actos derivadas de la informática" [26]

Puede ser definido el derecho de la Informática como "el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, y aplicación de la informática, o los problemas que se deriven de la misma en las que existe algún bien que es o deba ser tutelado jurídicamente por las propias normas." Todavía hoy es cuestionable si existe esta disciplina como tal, por ello, la mayoría de estudiosos de esta materia prefieren estudiar los siguientes puntos:

a) Protección jurídica de la información personal;
b) Protección jurídica del software;
c) Flujo de datos fronterizos;
d) Convenios o contratos informáticos;
e) Delitos informáticos; y

[26] Marcelo Valle Fonrouge, *Introducción a la Informática Jurídica*: El Derecho Informático y Otras disciplinas (Argentina: LL, 1979), p.784.

f) Valor de los documentos electromagnéticos (Firma digital)

1.5.3 Características distintivas del Derecho informático

El Derecho informático es una materia jurídica dirigida a la regulación de las nuevas tecnologías de la información, es decir, a la informática y a la telemática (combinación de las palabras “telecomunicaciones “e “informática”, ddisciplina que asocia las telecomunicaciones con los recursos de la informática).

Dentro del derecho informático también se encuentran las sentencias de los tribunales sobre materias informáticas y los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer o criticar el sector normativo que disciplina la informática y la telemática.[27]

1.5.4 Naturaleza del Derecho Informático

Las fuentes y estructura temática del Derecho Informático afectan a las ramas tradicionales del Derecho, por lo que se puede decir que esta afectación no es exclusiva para una sola rama del Derecho.

1.5.4.1 Derecho público

a) Flujo internacional de datos informatizados;
b) Libertad informática (defensa frente a eventuales agresiones);
c) Delitos informáticos (tienden a crear un ámbito propio del Derecho Penal).

[27] Felipe Rodríguez, *Derecho Informático* (Córdoba: Universidad Nacional de Córdoba, 2014), 32.

1.5.4.2 Derecho privado

a) Contrastes informáticos (hardware, software);
b) Protección jurídica de los programas

Las fuentes y estructuras del Derecho informático no están aparte del "Derecho tradicional," así se inscriben en el ámbito del Derecho público el problema de la regulación del flujo internacional de datos informatizados, la libertad informática o la defensa de las libertades frente a posibles agresiones realizadas por las tecnologías de la información y la comunicación, o los delitos informáticos que tienden a configurar un ámbito propio en el Derecho penal actual.

Mientras que en el Derecho privado estarían recogidas cuestiones tales como: los contratos informático, que pueden afectar lo mismo al hardware que al software, dichos contratos pueden ser de compraventa, alquiler, copropiedad, multipropiedad, etc. así mismo en el Derecho privado están recogidos los distintos sistemas para la protección jurídica de los programas de ordenados, temas que afectan a los objetos tradicionales de los Derechos civil y mercantil.

El hecho de que el Derecho informático afecta a distintas disciplinas dentro del Derecho ha suscitado un debate teórico sobre si se trata de una nueva disciplina jurídica o si por el contrario se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas.

1.5.5 Derecho a la Informática y a la Información

El conocimiento científico del derecho implica distinguirlo del mero objeto del derecho.

Aquí se demuestra la posibilidad latente de la existencia de la autonomía del Derecho Informático como nueva rama del Derecho. Es válido decir que un conocimiento para ser científico debe contener al menos tres elementos necesarios que son: Materia, Teoría y Método propios. Esta opinión es simple o básica para distinguir al conocimiento científico de cualquier otro tipo de conocimiento; pero, no nos arroja a grandes luces para diferenciar al conocimiento meramente jurídico del de las disciplinas jurídicas, como es el caso del Derecho Informático; ello en virtud de que la problemática jurídica que representa la informatización de la sociedad se vincula con figuras jurídicas previstas en las áreas de derecho público, privado y social.[28] En materia jurídica son distintos y variados los modelos que tratan de explicar a la ciencia del derecho; por lo que puede utilizarse un modelo bastante simple; consistente en la distinción del objeto del derecho y la ciencia del derecho.[29]

El primero el objeto del derecho, tiene como función el estudio de la norma; la exteriorización de una conducta humana y sus efectos; y, el valor intrínseco de la norma al buscar la realización de los axiomas jurídicos. La segunda es la ciencia del derecho, por su parte, busca: la descripción de la norma; la verdad o falsedad de la norma; el entendimiento de la actividad jurisdiccional; y, la comprobación de las hipótesis contenidas en la norma.

Necesariamente la norma jurídica que contiene al supuesto normativo debe emanar de una autoridad legitimada para llevar a cabo dicha tarea. Finalmente, la norma jurídica debe cumplir con sus objetivos, es decir, ser coactiva y sancionadora; esto es, que por una parte la norma jurídica debe

[28] McGraw Hill, *Derecho a la Informática y a la información*, 3ª ed. (México: Patria, 2006), p.56.
[29] Téllez, *Derecho Informático*, p.17n20.

obligar a su cumplimiento y, por otra, en el caso de su violación debe castigar al infractor.

El Derecho como ciencia a diferencia del objeto del derecho, tiene por cometido describir la norma; es decir, observar al derecho como es y no como derecho que debe ser.

El Derecho Informático como rama del Derecho tiene una incipiente y corta evolución, la cual data a partir del año de 1949, en el que Norbert Wiener, con su obra, consagra al "derecho y las comunicaciones", al expresar la influencia que ejerce la cibernética respecto de la ciencia jurídica, afirma "Así los problemas de la ley deben considerarse como comunicativos y cibernéticos, es decir, son problemas de regulación ordenada y reproducible de ciertas situaciones críticas." [30]

En ese mismo año el Juez Norteamericano Lee Loe Vinger, publicó un artículo En la revista "Minnesota Law Review" bajo el título "The Next Step Forward" (el siguiente paso adelante), el cual hace ver que "El Próximo paso adelante en el largo camino del progreso del hombre, debe ser el de la transición de la teoría general del derecho a la jurimetria, es decir la investigación científica acerca de los problemas jurídicos.[31]

1.5.6 Autonomía del Derecho Informático

En el debate respecto a la autonomía y clasismo del Derecho Informático, tiene su origen en el hecho de que la legislación no lo considera como tal.

[30] Wiener, *Cibernética y Sociedad*, p.97nn 19-20
[31] Carlos Barriuso Ruiz, *Interacción del Derecho y la Informática*, (Madrid: Dykinson, 1996), p.63.

Si se considera al derecho informático como clasista, lo mismo debe suceder con el derecho minero, derecho marítimo, etc. como ramas muy especializadas. Es más, bajo estos principios, en la mayoría de las sociedades latinoamericanas el derecho procesal civil y el derecho mercantil serían clasistas ya que el común de la población no tiene acceso a la justicia por vía de estas ramas tan básicas del derecho.[32]

El Derecho Informático es considerado clasista debido a la mínima cantidad De personas que se "conectan" a Internet; no obstante, el Derecho Informático no solamente se refiere al uso de Internet, también se refiere a actos jurídicos en que se ven inmersos aquellos individuos que no poseen un grado significativo de informatización, es así que el Derecho Informático se refiere en su vertiente de Derecho de la Informática "a la regulación de todo lo que acontece con los medios electrónicos, ópticos y de cualquier otra tecnología." En este sentido, debemos tener en consideración que nuestras leyes contemplan supuestos generales que pueden ser aplicados a las operaciones realizadas por medios electrónicos. El error de muchos profesionales del Derecho en lo que respecta a esta materia, es querer que todo esté regulado por una sola ley, todos los aspectos relacionados con el derecho informático los quieren unidos en un solo compendio legal informático.

La discusión respecto a la inexistencia de autonomía del Derecho Informático, se puede resumir en dos corrientes a saber: La primera, sostiene su autonomía como rama independiente del derecho; lo hace en base a que el Derecho Informático constituye un cuerpo autónomo de normas jurídicas que tienen por objeto regular las actividades que derivan de la informática, dentro de un orden eficiente y justo. Esta corriente estima de su carácter interdisciplinario,

[32] José Ovidio Salgueiro, Derecho clasista, (México: congreso-fiadi), 10 oct. 2000

cuestión que no le priva de la autonomía, ya que “el Derecho Informático tiene por objeto sistematizar y ordenar los elementos que le informan con respecto al impacto de las Tecnologías de la Información en la Sociedad de la Búsqueda”. Asimismo, se esgrime que el Derecho Informático cuenta con bases (Teoría, Métodos y Materia) científicas con respecto a su objeto.

Finalmente, desde este punto de vista, se afirma que el Derecho Informático cumple con todos los supuestos que requiere una rama jurídica autónoma, o sea, una legislación específica (campo normativo), un estudio particularizado de la materia (campo académico), investigaciones y doctrinas que traten la materia (campo científico), instituciones propias que no se encuentren en otras áreas del derecho (campo institucional).

De otro lado, se tiene a la postura que anula la autonomía del Derecho Informático desde el punto de vista de que en cada rama jurídica la actividad Informática se encuentra presente, rechazando así la integración de normas en un cuerpo aislado.

Niega la autonomía del Derecho Informático en virtud de que no existe claridad Respecto a su área jurídica de influencia; es decir, como el Derecho Informático tiene relación con otras disciplinas jurídicas como lo es el derecho civil, penal, laboral, administrativo, etc., y es a través del espectro normativo de estas, la forma en cómo pueden incluirse las conductas y problemáticas jurídicas del impacto tecnológico.

Por último, esta corriente objeta la autonomía del Derecho Informático en virtud de su constante y necesaria recurrencia a los principios jurídicos de otra rama para la solución de los casos concretos, debido a que esta corriente cuestiona esta búsqueda de los principios jurídicos de alguna rama en particular.

En otro sentido, deben también mencionarse otras tres causas que impiden la autonomía del Derecho Informático; dos de ellas son: la variedad de denominaciones con que se le identifica, y la confusión del Derecho Informático con otras disciplinas jurídicas.

En el primer caso el de la variedad de denominaciones, se identifica al Derecho Informático con sus ramas disciplinarias, es decir, con la Informática Jurídica y con el Derecho de la Informática; esto se presenta fundamentalmente al desconocimiento de su objeto de estudio. También, se le ha denominado como Derecho de las Tecnologías de la Información, Derecho del Comercio Electrónico entre otras.

En el segundo caso, por ejemplo, se confunde al Derecho Informático con el Derecho a la Información. No es ocioso mencionar que el Derecho a la Información “es la rama de la ciencia del derecho que estudia la facultad que tiene todo ciudadano para difundir, investigar y recibir información por cualquier medio” y, en este sentido, es notorio que se trata de dos disciplinas jurídicas distintas, aunque cabe aclarar que el Derecho Informático asume como suyo el reto de regular jurídicamente este campo del Derecho a la Información, tal y como es el caso del estudio e investigación del derecho fundamental a la autodeterminación informativa y su mecanismo de tutela y garantía jurídica.

Finalmente, una tercera y última causa que afecta notoriamente al reconocimiento de autonomía al Derecho Informático, es la relativa al conflicto entre Regulación jurídica y la Autorregulación.

Estas dos posturas y por obviedad opuestas, justifican desde su particular óptica la política que debe imperar para controlar el flujo de información y la

realización de ciertas conductas en la denominada red de redes. La regulación jurídica, se presenta como el "Conjunto de normas que integran el derecho; es decir, de aquellas reglas de conducta elaboradas y expedidas por el Órgano Legislativo y aplicadas por el Órgano Ejecutivo conforme a los procedimientos establecidos en el sistema de producción normativa de un país determinado".[33] Esta concepción deja en claro que se trata "del conjunto de disposiciones jurídicas que tienen por objeto la protección de los intereses individuales y colectivos en los medios electrónicos, ópticos y de cualquier otra tecnología".

1.6 La Era de la informática

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad 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 de campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información" [34] a lo que con más propiedad, podríamos decir que más bien estamos frente a la **"**era de la informática**".**

Por tanto, al abordar el estudio de las implicaciones de la informática en el fenómeno delictivo, resulta una cuestión interesante para quienes observan el impacto de las nuevas tecnologías en el ámbito jurídico-social. Justamente, el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a debates tales como: a) el análisis de la insuficiencia del sistema jurídico actual para regular las nuevas posiciones, b) los nuevos escenarios, en donde

[33] Fernando Octavio Islas Gutiérrez, *Internet: El medio inteligente*, (México: Cecsa, 2000), p.76.
[34] Ulrich Sieber, *Aproximación al Delito Informático* (Barcelona: PP, 1992), p.65.

se debaten los problemas del uso y abuso de la actividad informática y c) su repercusión en el mundo contemporáneo.

Es por esta razón, que paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos y en algunos casos de difícil tipificación en las normas penales tradicionales. La doctrina ha denominado a este grupo de comportamientos, de manera genérica, "delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática**"**.[35] Esta dependencia de la Sociedad a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida; cobra importancia entonces la seguridad con la que han de contar los equipos informáticos y las redes telemáticas, con el fin de poner obstáculos y luchar contra dichas conductas delictivas; produciendo la necesidad de tipificar y reformar determinadas conductas, con la finalidad de que estas sean efectivas y positivamente perseguidas y castigadas en el ámbito penal.

Se menciona doctrinariamente que la tecnología de la Información y comunicación, fue de gran impacto en los años noventa y específicamente Internet reformó las pautas de interacción social. En ese sentido, se entiende por tecnologías de la información y comunicación (TIC), "un término dilatado empleado para designar lo relativo a la informática conectada a Internet, y especialmente el aspecto social de éstos. Ya que las nuevas tecnologías de la información y comunicación designan a la vez un "conjunto de innovaciones

[35] Santiago Acurio del Pino, *Delito penal informático*, (Ecuador: Universidad Andina Simón Bolívar, 2015), p.4.

tecnológicas pero también las herramientas que permiten una redefinición radical del funcionamiento de la sociedad".[36] La Tecnología de la Información y Comunicación, se ha convertido según la doctrina[37], en un conjunto de herramientas indispensables para casi cualquier actividad, ya que en muchos de los casos, sólo se requiere de cierto acercamiento, por ejemplo por mensajes electrónicos, en este orden de ideas y debido a que a través de las nuevas tecnologías, se ha creado una eficiente comunicación de alcance global, es factible la comunicación inmediata entre las personas, ya que se traspasa barreras de tiempo y espacio a bajo costo.

Según parte de la doctrina,[38] las denominadas nuevas tecnologías de la información y comunicación en general y en especial internet, otorgan a las personas un mayor acercamiento a todo tipo de información sin límite de tiempo y espacio; por ello es preciso mencionar que el país pionero en el desarrollo y evolución técnica y jurídica de las Tecnología de la Información y Comunicación, es Estados Unidos de América. Así las cosas y a raíz de la necesidad de resolver un número mayor de conflictos, surgen los sistemas privados de solución en línea de conflictos (ODR, por sus siglas en inglés Online Dispute Resolution)[39].

Se menciona doctrinariamente que internet tiene su origen en 1969, en un proyecto experimental de la "Advanced Research Project Agency" ("ARPA"), llamado ARPANET, que unía Universidades y redes de ordenadores de titularidad militar, contratistas de defensa y laboratorios universitarios que

[36] José Manuel Huidobro, *Tecnologías de información y comunicación*, (Madrid: Universidad Politécnica de Madrid, 2010), p.34.
[37] Néstor Raúl Londoño Sepúlveda, El uso de las TIC en el proceso judicial: una propuesta de justicia en línea",Medellin,n.40 (2010): p.112
[38] Ana Montesinos García, *Arbitraje y nuevas tecnologías*, (España: Civitas, 2007), 23.
[39] Londoño, "una propuesta de justicia en línea",p.113

realizaban investigaciones militares[40]. Por otra parte, se menciona por los estudios en esta materia[41], que en los últimos años, los órganos públicos están incorporando las tecnologías de la información y comunicación a su quehacer diario.

En la actual sociedad de la información se encuentra la denominada "cibercriminalidad," que se presenta en la cotidianeidad de las personas bajo las más variadas formas, expresadas en una amplia diversidad de fenómenos delictivos, y renovadas modalidades en comisión de los delitos tradicionales, especialmente, a través de sistemas o redes informáticas de transmisión e intercambio de datos por Internet, cuya complejidad operativa dificulta su persecución y, consecuentemente, incrementa los niveles de impunidad; y aunque en realidad, no exista un concepto de "cirbercriminalidad" unánimemente aceptado, podríamos decir que se trata de un término que hace referencia a un "conjunto de actividades ilícitas cometidas mediante el uso y abuso de las tecnologías de la información y la comunicación, poniendo en peligro, lesionando intereses o bienes jurídicos de naturaleza individual, o amenazando la seguridad de los sistemas sociales.

A causa de lo anterior, es pues que con el surgimiento de la informática, que dicho mecanismo o herramienta da la pauta para que el ser humano utilice dicho instrumento para el cometimiento de actividades ilícitas que conllevan al delito informático, lo cual implica actividades criminales que los países han tratado de resolver con figuras típicas de carácter tradicional, tales como: robos, hurtos, fraudes, falsificaciones, estafas, sabotajes, etc. Sin embargo,

[40] Paloma Llaneza González, *Internet y comunicaciones digitales*, (Barcelona: Bosch, 2000), p.37.
[41] Agustín Cerrillo, "las tecnologías de la información y el conocimiento al servicio de la justicia Iberoamericana en el siglo XXI", Honduras, n.2 (13 de febrero de 2007), p.17.

debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades para el uso indebido de las computadoras, lo que ha creado la necesidad de su regulación por parte del Estado.

En el año de 1983, la Organización de Cooperación y Desarrollo Económico (OCDE)[42] inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad". Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica, donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos".

Los delitos informáticos se realizan necesariamente con la ayuda de los

[42] OCDE es una organización intergubernamental compuesta actualmente por 42 países (34 miembros plenos) y ocho países adherentes. Su misión es promover políticas que mejoren el desarrollo económico y el bienestar social de personas en todo el mundo.

Sistemas Informáticos, pero tienen como objeto del injusto la información en sí misma. Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

La estafa, delito que comienza a ser objeto de elaboración y tratamiento dogmático desde mediados del siglo XIX, todavía es fruto de intensas discusiones. Los distintos desarrollos que a su respecto se dan en el seno del Derecho comparado, la disparidad de sus elementos típicos o la delimitación de su bien jurídico protegido a efectos de centrar el ámbito que buscaría resguardar el tipo, van de la mano de su aspecto propia y particular.

Por lo que, a medida que el ser humano ha ido desarrollando nuevas tecnologías y herramientas que ha logrado desplegar rápidamente la información, y a partir de la segunda mitad del siglo xx que los sistemas informáticos se han ido convirtiendo en instrumentos habituales de nuestra vida social actual. Estos métodos, técnicas, procesos, han proporcionado al ser humano un avance incalculable en la agilización para la realización de tareas, que sin ellas se requeriría de mayor tiempo y recurso humano; pero así como también, avanza la facilidad en la utilización de herramientas tecnológicas para lograr que los sujetos realicen más y mejores actividades tales como: económicas, culturales, educativas, entre otros; han venido a abrir una infinidad de nuevas posibilidades para las comunicaciones, ya que el uso de los sistemas informáticos, en concreto, el de las redes que se pueden formar entre ellos, y también ha permitido una relativización cuando una absoluta desaparición de las barreras temporales y espaciales a las que se enfrenta tradicionalmente el flujo de información, han proporciona al ser humano un avance incalculable en cuanto a la realización de tareas.

El extraordinario desarrollo de las tecnologías de la información en las últimas décadas no ha pasado inadvertido; algunas veces de forma abierta, y otras de manera un tanto sutil, y en otras su huella se ha ido imprimiendo en el proprio ser humano y en los grupos sociales en que este se integra, hasta mutar sus comportamientos y sus valores esenciales, tal es así, que el cambio hacia la civilización tecnológica afecta profundamente las condiciones de la vida humana; porque prácticamente son todos los sectores del quehacer humano, sea este individual o social con los que se hallan en mayor o menor medida afectados.

algunos sectores sociales especialmente sensibles a los peligros que podrían generar el uso y abuso de estas nuevas tecnologías; que al no gozar de una adecuada protección penal, han obligado al legislador, así como a los organismos internacionales, a crear nuevas figuras delictivas especialmente destinadas a otorgarles tal protección.

Este es el caso del delito de estafa informática. Este fenómeno ha llevado a su vez, a que se comience a hablar de la existencia de los denominados “delitos informáticos” o según la doctrina la “criminalidad informática”, ambos conceptos que pese hacer utilizados de forma generalizada por la doctrina, adolecen de una imprecisa definición o delimitación, lo que implica la necesidad de concretar estos extremos, cuando se trata de estudiar el fenómeno de los delitos informáticos y en concreto el delito de estafa informática.

Pero, así como también se encuentra la facilidad para la utilización de dichas herramientas tecnológica, para lograr realizar mayor conectividad entre sujetos y sus actividades licitas, también lo hacen aquellos seres que desean en base a sus conocimientos generar ilícitos en personas o instituciones y generar

agravios, ya sea de carácter económico o moral, es por ello que al realizar el estudio del tema de la informática y sus medios, se trata de profundizar en el porqué de esta actividad delictiva utilizando los medios informáticos.

La informática se presenta como una nueva forma de poder, que puede estar Concentrada o difuminada en una sociedad; confiada a la iniciativa del sector privado o reservada al monopolio de un Estado. Y es una forma de poder en su doble sentido: a) porque es un instrumento dirigido a facilitar el desarrollo humano casi de forma ilimitada, capaz de sustituir de modo seguro, rápido y eficaz aspectos parciales de la actividad intelectual de los seres humanos, y que coloca a quienes pueden hacer uso de ella, en base a sus desarrollos, destrezas y habilidades colocándolos en una posición ventajosa frente al resto de quienes no utilizan estas herramientas. b) porque la técnica de información a través de los medios informáticos ha significado el nacimiento de una nueva forma de energía que no es física, sino que es intelectual; de modo que la humanidad acrecienta y multiplica la posibilidad de desarrollo científico, el cual conlleva a un desarrollo social, y que como toda clase de energía, constituye una expresión de poder.

Del mismo modo que la escritura ha sido un factor condicionante para el Desarrollo de las civilizaciones, así también esta nueva clase de lenguaje electrónico, llamada informática, marca hoy la frontera entre las sociedades modernas, haciendo prevalecer a las sociedades que puedan disponer de ella; en tal sentido la informática es un factor de conocimiento y de poder que puede ser concebido como un nuevo tejido cohesionador de la sociedad civil o un instrumento de su misión universal, sobre esta alternativa del uso de la informática se juega el destino social del ser humano.

Es de esta forma como se llega al tema de la estafa informática, en la cual se

da el tipo de programas que llegan a través de un ordenador o computadora y la utilización del internet, y es que los sistemas operativos han ido mejorando, los procesadores se han ido desarrollando con mayor potencia, y con programas con mucha innovación, y es ahí donde se centra el abordaje de nuestro tema de estudio de cómo estas herramientas y conocimientos permiten la realización de conductas delictivas de algunos sujetos en contra del patrimonio de otro u otros.

CAPITULO II

SURGIMIENTO DE LA INTERVENCION JURIDICO PENAL EN LA DELINCUENCIA INFORMATICA

El presente capitulo trata sobre los Aspectos Generales sobre la Delincuencia Informática, Sociedad de Riesgo, Avance de las Tecnologías y la Expansión de los Delitos Informáticos en el Derecho Penal, Aproximación a la definición de los Delitos Informáticos, Características de los Delitos Informáticos, Bien Jurídico protegido en los Delitos Informáticos, Sujetos que intervienen en los Delitos Informáticos, perfil Criminológico del Delincuente, y la Clasificación de los Delitos Informáticos, con el propósito de conocer la delincuencia informática.

2.1 Aspectos Generales sobre la Delincuencia Informática

Hoy en día es difícil establecer solamente un tipo de delincuente, ya que a medida que se han desarrollado aspectos culturales, educativos, científicos, tecnológicos, de igual forma ha ido desarrollándose la delincuencia en muchos ámbitos como los tecnológicos, y propiamente en materia informática, y tal es así que muchos de los estudiosos del amplio mundo del derecho han realizado fenomenales esfuerzos mentales para el establecimiento de posturas en un inmenso mundo de la información a través de los medios informáticos.

El aspecto más importante de la informática radica en que la información ha

pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después[43].

Como también se puede establecer que es indispensable utilizar en cualquier ámbito laboral los ordenadores para poder obtener, intercambiar y visualizar información que requiera el individuo. Esto ha sido posible gracias a la tecnología, la cual ha contribuido a simplificar el trabajo. Sin embargo, no hay que olvidar que, cualquier alteración, modificación y/o uso indebido de la información, ya sea prensa escrita o Internet, es una violación a los derechos de autor.

Es importante destacar que las mismas autoridades competentes a nivel nacional y mundial han legislado sobre esta cuestión, pero no en forma satisfactoria, mediante convenios y tratados que se mencionarán más adelante.

2.1.1 Evolución histórica sobre el surgimiento de los Delitos Informáticos

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

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

---

[43] Claudio Paúl Magliona Markovicth y Macarena López Medel, *Delincuencia y Fraude Informático*, (Chile: Jurídica, 1999), p.23

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún." En 1983, la Organización Cooperación y Desarrollo Económico (OCDE)[44] inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal[45], durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas, que en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad". Se entiende Delito como: la "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".[46]

[44] Fundada en 1961, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) agrupa a 35 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo.

[45] La Asociación Internacional de Derecho Penal es la organización mundial más antigua que reúne a los especialistas de ciencias penales y una de las sociedades científicas más antiguas. Creada en 1924, como refundación de la Unión Internacional de Derecho Penal (1889)

[46] Pedro Torres Ruiz, *Diagnóstico y evaluación de instituciones*: programas e intervención psicológica, (Madrid: Universidad Complutense de Madrid, 2011), p. 53.

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

En esta clase de delincuencia, se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger la información.

En este punto debe hacerse notar lo siguiente:

a) No es la computadora la que atenta contra el hombre, es el hombre el

Que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir;

b) No es la computadora la que afecta nuestra vida privada, sino el mal uso que hacen ciertos individuos de los datos que ellas contienen;
c) La humanidad no está frente al peligro de la informática, sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. La protección de los sistemas informáticos puede abordarse desde distintos perspectivas, como lo son: civil, comercial o administrativa. Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

2.1.2 Expansión del Derecho Penal como origen de los Delitos

La "expansión", en mención sería la tendencia general maximalista representada por la "creación de nuevos "bienes Jurídico Penales", ampliación de los espacios de riesgos Jurídico Penalmente relevantes, flexibilización de las reglas de imputación y relativización de los principios político criminales de garantía" [47] Dicha expansión posee una "cobertura ideológica". Responde al modelo social configurado en los últimos 20 años. Responde a una constante demanda social de mayor protección. Responde a la creación de opinión pública. La sección. Ya es suficientemente claro sobre su contenido, donde en

[47] Edison Carrasco Jiménez, *La expansión del derecho penal y las críticas formuladas a ella por la doctrina penal*, (España: Universidad de Salamanca, 2009), p.32.

general trata de los fenómenos sociales, jurídicos y políticos cuyos efectos en el Derecho Penal producen como resultado su “expansión”.

El fundamento teórico más gravitante para justificar las causas de dicha “expansión” es la llamada “teoría del riesgo” de Ulrich Beck, que se divide en causas y factores: Causas del fenómeno de la expansión, y Factores del efecto multiplicador de la expansión. Causas del fenómeno de la expansión son Riesgos humanos y fallos técnicos.[48]

El punto de partida es el “riesgo” en las sociedades modernas, el “riesgo” de procedencia humana y como resultado de los avances tecnológicos, lo que hace que el grado de interrelación entre los sujetos bajo estas condiciones aumente las posibilidades de producción de riesgos y consecuencias lesivas. Dentro del anterior contexto, la delincuencia intencional y las formas tradicionales de criminalidad serían superadas cuantitativamente por la criminalidad organizada y la delincuencia no intencional. Ésta última sería aquella que procede de fallos técnicos, en los que existen acciones de control de riesgos, donde se aumenta la cadena de funciones y de su delegación y que, por consecuencia, se va perdiendo el dominio real del curso de los acontecimientos. Esto aumentaría los riesgos, los cuales podrían incidir en la generación de delitos de comisión por omisión. [49]

La crisis del modelo del Estado de bienestar otra de las causas que se puede señalar sería la crisis del modelo del Estado de bienestar. Esto provocaría problemas de “desvertebración interna” de la sociedad, lo que se reflejaría en el desempleo, la migración y la criminalidad callejera, cuestiones que

[48] Jesús María Silva Sánchez, La expansión del Derecho penal: Aspectos de la política criminal en las sociedades postindustriales, Chile, n.03 julio –sep. (1999):p.11.
[49] Ibíd. p.12.

transformarían al “otro” en un riesgo. El miedo a los riesgos una tercera causa de índole subjetiva, y que el autor Silva Sánchez refiere como la más significativa, en su obra; sería la sensación social de inseguridad o, propiamente, de miedo, entendido como superior a la existencia de riesgos objetivos, lo cual produce una desorientación cognitiva que, debido a ese malestar y para no ser sentida, se busca en cambio una orientación normativa en el Derecho Penal. De ahí que comiencen a surgir demandas de protección solicitadas al derecho penal.

Esta sensación de inseguridad, en muchos casos, se encuentra alimentada por los medios de comunicación masivos, que generan en la opinión pública no solo “percepciones inexactas”, sino también la sensación de impotencia, debido, entre otras cosas, a la reiteración de los hechos noticiosos, la exposición sesgada de la realidad y la excitación del morbo. La conformación social de sujetos pasivos una cuarta causa, sería la conformación de la sociedad en una de sujetos pasivos, “beneficiarios de la transferencia de riqueza, más que creadores de los excedentes objeto de transferencia”, pensionados, consumidores o sujetos pacientes “de los efectos nocivos del desarrollo”.

Esta presencia impulsa las políticas hacia la disminución del riesgo permitido a causa de la sensación de inseguridad y la demanda social de seguridad de estos sujetos pasivos. Pero, de otro lado, se generaría desde estos sujetos pasivos una “resistencia psicológica frente al caso fortuito, frente a la producción de resultados lesivos por azar” y una búsqueda del actuar humano como causa de dichos resultados lesivos, lo que desplaza el péndulo del caso fortuito al injusto.

Esta cuestión última se vería reforzada por el estereotipo de víctima de este

Modelo social que “no asume la posibilidad de que el hecho que ha sufrido sea debido a una ‘culpa suya’ o que, simplemente, responda al azar, se parte del axioma de que siempre ha de haber un tercero responsable al que imputar el hecho y sus consecuencias patrimoniales y/o penales”; de ahí que una de las consecuencias jurídico penal sería el incremento de los delitos de peligro, con lo que se alejan los delitos imprudentes y se acercan las legislaciones simbólicas. Una quinta causa sería la identificación social de las mayorías con la víctima del delito, prefigurada ya por la clase de sujetos pasivos y la crisis del llamado “Estado de bienestar”, lo que incide en el uso del Derecho Penal como instrumento contra la delincuencia de cuello blanco y de las empresas, considera un error de perspectiva, hasta cierto punto, la expansión sobre la criminalidad socioeconómica, ya que debido a la relativización de los principios y reglas de imputación, esto afectaría también a la criminalidad en general, sobre todo la de los “desposeídos”, que estima mayoritaria. Se encuentra un indicio de ello en la criminalidad infantil y juvenil cuando se busca hacer más duras las sanciones y rebajar la mayoría de edad penalmente responsable.

Descrédito de otras instancias de protección. Las causas anteriores explicarían por qué se busca instancias jurídicas para la solución del problema, pero no la recurrencia a instancias jurídico penales, cosa que sí explicaría el Descrédito de otras instancias de protección, que se visualiza en lo siguiente:[50]

La ausencia de una ética social que asegure la protección de bienes jurídicos. La incapacidad del derecho civil actual, basado en un “modelo del seguro”. La desconfianza en la administración por los procesos de corrupción y de burocratización que se observan en ella. De ahí que surja un depósito de

[50] Luís Gracia Martín, *Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia*, (Valencia: Tirant Lo Blanch, 2006), p.45.

confianzas en el Derecho penal como instrumento de pedagogía social y de gestión de los problemas, justamente debido a que las instancias anteriores habrían dejado de ser confiables para su solución.

Gestores atípicos de la moral es la orientación de la izquierda como “gestores atípicos de la moral”, entre los que se cuenta a la social democracia, asociaciones de reivindicación y defensas de derechos medioambientales y sexuales, entre otros los cuales contribuirían a demandar una mayor intervención del Derecho penal.

En primer término, aquellos vigorizarían la idea de la sociedad de sujetos pasivos, que en tanto titulares de bienes jurídicos individuales o colectivos, son a la vez posibles víctimas y, por ende, habría una presión sobre una demanda por mayor protección penal. Así, los movimientos sociales que antes eran renuentes al Derecho penal por la aplicación y petición de las clases más poderosas contra ellos ahora lo reclamarían en contra de estas últimas.[51]

En segundo término, la política de izquierda hoy fomenta la idea de protección del Derecho penal ante la criminalidad general, sosteniendo una política criminal con una “ideología de la ley y el orden en versión de izquierda”, basados en criterios de seguridad.

En este sentido se da un desprecio por las formas relegado a ser más bien un factor colateral, y como causa, se encuentra el desprecio por las formas, que conduce a la privatización del problema penal.

Así, se intentaría obviar principios como el de inocencia, de culpabilidad y el

[51] Silva Sánchez, “Aspectos de la Política criminal”, p.53n45.

Debido proceso, policías y delincuentes privadas de libertad ambulatoria serían, igualmente, consecuencia de esto.

Las formas que surgen del carácter público y sacramental del derecho dotan de un elemento de prevención de las reacciones punitivas que acercan el delito a lo cotidiano e informal.

Mayor demanda penal de la sociedad se expresa además como causa general del fenómeno expansivo no solo al Estado y su utilización del Derecho penal como instrumento de solución de problemas sociales, sino también a la sociedad en su conjunto, que demanda tales respuestas factores del efecto multiplicador de la expansión además se expone no solo las causas de la expansión, sino los que serían “factores del efecto multiplicador de la expansión” que acentuarían a nivel global el fenómeno expansivo de las legislaciones nacionales, a saber, la globalización y la integración supranacional.

La globalización sería fundamentalmente económica, de igual forma que la integración, lo que conduce a que ciertos hechos considerados punibles dejen de serlo por este contexto de eliminación de obstáculos a la integración. Por el contrario, hace que surjan nuevas formas de criminalidad económica, que a su vez dan origen a nuevas modalidades de delitos clásicos o propiamente a nuevos delitos, como la criminalidad organizada e internacional y la de los poderosos.

Todo lo anterior se traduce en las siguientes consecuencias:
Adopción de un carácter práctico y político para la unificación de criterios jurídicos más que de criterios científicos en la adopción de respuestas

concretas, lo cual hace olvidar la preocupación sistemática de una teoría del delito construida con fines garantistas.

Un objeto principal de la globalización a nivel jurídico-penal, el cual no es la criminalidad clásica sino la económica o criminalidad de los poderosos, ante la cual no se presenta ni existe una construcción dogmática completa, con las consecuencias de flexibilización de garantías, posibles lagunas y déficit en la ejecución de la normativa penal, lo que produce inseguridad jurídica; punitivismo y aceptación de la severidad de las penas; diversidad de tradiciones jurídicas, lo que supone adopción de las soluciones más sencillas para aunar los diversos criterios, cuestión que trae como consecuencia la adopción de criterios flexibilizados.

La Integración supranacional el carácter práctico de una legislación supranacional busca respuestas uniformes que eviten paraísos jurídicos penales. Pero dicha uniformidad no es suficiente para darse importancia a la homogeneidad en la teoría general del delito y los principios y garantías político criminales, que den sustento a una aplicación normativa supranacional, ya que la armonización legislativa sola no produce por sí sola una homogeneización.

La Administrativización del Derecho Penal como expresión de la expansión, la llamada "administrativización del Derecho Penal" tiene por expresión más visible la del contenido material de los tipos penales, donde fundamentalmente el legislador se ha inclinado por proteger el contexto o "condición previa al disfrute de bienes jurídicos individuales más clásicos" y donde se ha traducido en el cambio de dos elementos relativos a dicho contenido.

Desde el bien jurídico individual al colectivo. De los delitos de lesión a los de

Peligro, esto se ve reforzado por una tendencia contraria a la despenalización, y donde la conducta de la doctrina tradicional en relación a esta sería débil. Ejemplo de ello es el medio ambiente, el cual, si bien genuinamente presentaría un problema, resulta demasiado riesgoso que sea el Derecho Penal quien gestione el problema ecológico, sobre todo cuando la ratio legis de una legislación es el contexto, que sería para este caso el medioambiente, provocando la intervención del Derecho Penal tan pronto como se superen los estándares administrativos.

Por ello, el Derecho Penal se ha administrativizado, transformándose en un derecho de gestión de riesgos, en efecto, el Derecho Administrativo sancionador, este se preocupa fundamentalmente de la gestión de sectores de modo global, de la conducta general antes que de la individual, en cuanto afecte una globalidad de tipo estructural, una visión macro social, donde se puede decir que el daño sancionable es más bien el cumulativo, que es el que afecta por su trascendencia global. Por ello, sus criterios de actuación son más flexibles, sin necesidad de comprobar afectación a bien jurídico alguno, con lo que la lesividad no es un índice válido, ni la legalidad, por lo que los criterios de oportunidad son aceptados.

Todo este marco sería inadmisible para criterios de imputación de responsabilidad penal a un sujeto determinado, ya que las conductas se verían dirigidas a sancionar, más bien, un peligro global.

Esto puede verse reflejado en los delitos relacionados con el tráfico rodado, los delitos tributarios, los delitos medioambientales y el tráfico de estupefacientes, donde un solo hecho en sí mismo no interesa, sino que más bien es el conjunto de ellos, los cuales ponen en tela de juicio un sector social determinado, sea el tráfico rodado con el índice meramente estadístico del

alcohol en la sangre, o el número de defraudaciones en lo tributario, o la suma de vertidos tóxicos en el agua, o el modelo de gestión de salud en relación al tráfico.

Siendo así, el Derecho Penal de las sociedades postindustriales, al comportarse como instrumento de gestión de problemas sociales, asume el modo de "razonar" del Derecho Administrativo sancionador y, por lo tanto, se produce en él un proceso de "administrativización", ejemplo de lo mencionado anteriormente son los delitos acumulativos, donde un acto de forma individual no presenta un riesgo relevante sino que, más bien, es la suma de dichas conductas lo que lo produciría.

La acumulación, como manifestación delictiva llamada "culminación coherente del proceso expansivo del Derecho Penal" no sería para él admisible si lo que se quiere es la imposición de sanciones privativas de libertad asociada a la conducta. Flexibilización de principios, garantías y reglas de imputación existe como fenómeno general el que a la moderna criminalidad se asocian principios, garantías y reglas de imputaciones laxas o flexibles, ejemplo de ello son, los delitos que habrían de arrancar de una política criminal de la globalización, como lo sería el delito económico organizado, sea este empresarial o proveniente de fenómenos de macrocriminalidad tales como el terrorismo, el narcotráfico o la criminalidad organizada referida a tráfico de armas, mujeres y niños.

Estos están normalmente asociados a menores garantías, sea por la menor gravedad de las sanciones o por ser dicha criminalidad, potencialmente peligrosa; algunos principios igualmente se ven adaptados, tratándose de la legalidad, se produce el apatía de la determinación en los tipos para la criminalidad transnacional, y procesalmente, ya que una inclinación favorable

al principio de oportunidad sobre la legalidad; tal y como lo es en materia de culpabilidad, en materia de error de prohibición, lo importante es la determinación sobre su concepto y los límites de lo evitable, pero no a la relevancia misma del error de prohibición, otra situación es que existe una admisión sobre la responsabilidad de las personas jurídicas, y las figuras donde existe presunción de culpabilidad, como lo es del caso de tradiciones de la normativa anglosajona, respecto de la proporcionalidad esta se vería comprometida en las sanciones de delitos imprudentes relativo a bienes jurídicos colectivos, como también respecto de los delitos de peligro.

Un modelo dogmático común en el Derecho internacional, en aras de un modelo dogmático común, se opta por la búsqueda y formulación de estructuras lógico-objetivas dentro de un marco político criminal valorativo flexible, abierto y siempre dispuesto a ser revisado. Respecto de esto último, no podrían formar parte en la búsqueda de una ciencia común "quienes no participaran del mismo horizonte valorativo asimismo común"; esta resistencia entre una objetividad dogmática y la relativización fuente de la política-criminal de cada país se vería equilibrada por una dogmática de tipo normativista y con participación de países pertenecientes a una misma cultura, ya que esto haría posible el carácter trasnacional valorativo de dicha política-criminal.

Un Derecho Penal funcional, para que un Derecho Penal sirva como freno a la demanda penal de la sociedad se debe pensar, en "un Derecho Penal con vocación autor restrictiva" ya que a un Derecho Penal funcional se le atribuye de forma automática el ser maximalista, cuestión que ni un Derecho Penal basado en la teoría de bienes jurídicos asegura de partida restricciones para aquel. Una teoría funcional del Derecho Penal, en cuanto estabilización de la vigencia de las normas, no obliga a prescindir del bien jurídico como contenido material de las normas, por lo cual es posible concebir, dentro del marco de lo

funcional, la introducción de elementos de “racionalidad e ilustración”, con lo que el bien jurídico cumpliría no solo una función sistemática, sino también crítica.

Dentro de este marco, es posible delimitar criterios de identidad sociales que cristalicen las “expectativas normativas esenciales”, cuestión que se los encuentra en la Constitución, donde por vía de inconstitucionalidad sería posible impugnar el aspecto formal de una norma, y de no encontrarse en esta situación, daría lugar a una política criminal defendible y no impugnable de buenas a primeras.

La Sectorización del Derecho Penal basado en la relación principios, garantías y reglas de imputación sanciones, ante el desafío de un “Derecho Penal de la globalización”, caben dos posibilidades: sectorizar las reglas de la Parte General, o bien, modificar las reglas de la delincuencia clásica en razón de la nueva criminalidad, disyuntiva a la cual ya anuncia su resolución inclinándose hacia la primera alternativa. Un sector de la doctrina aboga por la vuelta a un Derecho Penal liberal, protector de bienes jurídicos básicos los personales y el patrimonio, conservando todas las garantías del Derecho Penal. Sin embargo, esta postura la entiende Silva Sánchez como “ucrónica”, ya que el Derecho Penal liberal sería una construcción nunca realizada, debido tanto a la rígida protección del Estado actual y por la existencia de ciertos principios de organización social como también porque la rigidez de las garantías propuestas por el Derecho Penal liberal son un contrapeso al extremo rigor de las sanciones.

De ahí que la relación más importante que le es posible visualizar al autor, como resultado de las reflexiones relativas a la expansión, es la relación entre garantías de un sistema de imputación y la gravedad de las sanciones.

Tratándose del Derecho Penal general, la rigidez de las garantías junto a una dogmática igual de estricta se hayan relacionadas con el hecho de que el sistema posea sanciones graves, sean las de muerte y las corporales, y para la actualidad, fundamentalmente la privativa de libertad, el problema de la expansión, entonces, no sería tanto la expansión del Derecho Penal en sí, sino más bien la expansión de la pena privativa de libertad. “Es esta última la que debe realmente ser contenida”, después de esto es que y entendiendo que no en todo el sistema sancionatorio del Derecho Penal podrían exigirse iguales garantías, pues las consecuencias jurídicas son diversas la correlación entre garantías y sanciones podría resolverse si se tiene que a mayor disminución o flexibilización de garantías y de rigor dogmático mayor debería ser la disminución del rigor sancionatorio, cuestión que se traduciría en la aceptación de penas privativas de derechos o pecuniarias, antes que en las privativas de libertad, que son las más graves.

El uso del Derecho Penal para el logro de estos fines tiene ventajas relevantes en comparación con otros derechos: posee una mayor fuerza comunicativa y dispone de neutralidad política, a diferencia del Derecho Administrativo. Es así como sería posible la utilización de un sistema dualista de Derecho Penal, con dos niveles de garantías y principios, frente a la imposibilidad de frenar la expansión del Derecho Penal y a la imposibilidad de aplicar idéntica teoría del delito de un Derecho Penal.

2.2 Sociedad de Riesgo

La sociedad actual ha sido calificada como sociedad del riesgo, dicha sociedad se caracteriza fundamentalmente por su complejidad, transnacionalidad, dinamicidad en su economía, multiplicidad de interconexiones causales y existencia de una alta intervención de colectivos; En definitiva, una

sociedad en la que los avances científicos y tecnológicos, así como el fenómeno de la globalización, entre otros factores, favorecen la aparición de nuevos peligros ante los que el ciudadano medio se siente amenazado.

La sociedad actual ha sido calificada como sociedad del riesgo, concepto Acuñado por el sociólogo alemán Ulrich Beck[52] en 1986 en su obra La sociedad del riesgo Hacia una nueva modernidad. En su obra el profesor Mendoza Buergo[53] afirma que entre los aspectos definitorios de la sociedad del riesgo pueden destacarse los tres siguientes:

a) El primero sería el cambio en el potencial de los peligros actuales en relación con los de otros períodos, ya que a diferencia de los peligros que amenazan con desastres naturales o plagas de otras épocas, los nuevos son artificiales, en el sentido de que son producidos por la actividad del hombre y vinculados a una decisión de éste. Asimismo, presentan grandes dimensiones, lo que significa que amenazan a un número indeterminado y potencialmente enorme de personas, e incluso a la existencia de la humanidad como tal, ya que al tratarse de grandes riesgos tecnológicos, suponen posibilidades de autodestrucción colectiva.

Estos riesgos de la modernización son consecuencias secundarias del progreso tecnológico, esto es, efectos indeseados (a menudo no previstos y a veces imprevisibles) de actividades inicialmente dirigidas a fines positivamente valorados. Ante estos nuevos peligros surge el problema de la imputación y atribución de responsabilidad por las consecuencias indeseadas, tanto a las

[52] Fué un sociólogo Alemán, profesor de la Universidad de Múnich, y de la London School of Economics, Beck estudió aspectos como la modernización, los problemas ecológicos, la individualización y la globalización.
[53] Blanca Mendoza Buergo, El Derecho penal en la sociedad del riesgo, (Madrid: Civitas, 2001), p. 25.

personas singulares como a las empresas o a las autoridades administrativas implicadas, no siendo imputables según las reglas vigentes de la causalidad, la culpabilidad y la responsabilidad.

b) El segundo aspecto definitorio de la sociedad del riesgo es la complejidad organizativa de las relaciones de responsabilidad, ya que el incremento en las interconexiones causales y su desconocimiento o las dificultades en su aclaración, determina que la responsabilidad se desdibuje cada vez más.

c) El tercero y último no es otro que la creciente sensación de inseguridad subjetiva ante los nuevos peligros, que existe incluso cuando dichos peligros no sean reales. Ello hace que los ciudadanos reclamen cada vez más del Estado la prevención frente al riesgo y la provisión de seguridad, ya que la sociedad actual se mantiene en un constante temor el cual es infundido por el incumplimiento del Estado en seguridad.

Ante tales coordenadas se afirma que el Derecho penal actual es un Derecho en expansión como respuesta a dicha sociedad del riesgo, de manera que lo que viene en calificarse como expansión del Derecho penal se vincula básicamente a su utilización para defender a la sociedad moderna de esos nuevos peligros que comporta la actual era post-industrial.

Algunos de los nuevos peligros o riesgos, de los cuales deben tenerse en cuenta pueden ser dos extremos: uno, que aunque ciertamente comportan efectos negativos, resultan altamente beneficiosos tanto para las personas individualmente consideradas como para la colectividad en su conjunto; y otro, que los mismos acechan, de una parte, a bienes jurídicos de carácter supra-individual (que han nacido en el seno de esta moderna como por: ej.: mercado,

competencia y protección de los consumidores delitos relativos al mercado y a los consumidores).[54]

2.3. Avance de las Tecnologías y la Expansión de los Delitos Informáticos en el Derecho Penal

El Derecho es la principal fuente inagotable de adaptación social en la Comunidad Mundial de Naciones.

Resulta fantástico apreciar como la Humanidad ha ido insertando los adelantos científico-tecnológicos en aras de perfeccionar los principales mecanismos de comunicación y avances hacia el desarrollo. El uso imprescindible de las nuevas técnicas de la información implica además un seguimiento continuo a conductas que transgreden la voluntad política de los Estados Nacionales y, en su caso, la respuesta punitiva de quien es, junto al Estado, la más antigua y necesaria institución mundial.

La estructura orgánica del trabajo que se presenta está dividida en análisis teórico-prácticos de los principales aspectos doctrinales que avalan el amplio proceso de formación, desarrollo, proyección y protección de los delitos informáticos. Un singular esquema de referencias completan, con detallada sencillez los mecanismos internacionales que desde sus inicios buscan mancomunadamente soluciones fehacientes a las enormes problemáticas, peligros y amenazas que enfrenta la Humanidad.

Se realiza un análisis de las principales causas que generaron y condicionaron

[54] María José Jiménez Díaz, Sociedad de Riesgo e intervención Penal, Revista Electrónica de Ciencia Penal y Criminología en línea, Universidad de Ganada, (2014), p 3.

la evolución de los delitos informáticos, sus entes de referencia, clasificación, seguimiento internacional en las legislaciones de un grupo de países del mundo desarrollado y sub-desarrollado, así como los principales elementos doctrinales que la Comunidad Mundial tiene en consideración en aras de darle un tratamiento efectivo con ayuda de los organismos internacionales y el apoyo incondicional de los Estados Nacionales.

Se abunda además en el papel protagónico de América y su toma de acción en los agobiantes problemas que mueven la realidad latina de hoy, tomando como punto de conexión tres países del área, abordando sus sujetos pasivos y activos, elementos imprescindibles si se tienen en cuenta las consecuencias que traería la proliferación de esta especie jurídica.

Se realiza además, como resultado de un minucioso y exhaustivo análisis, las principales problemáticas que, a juzgar por las Naciones Unidas, deben tomarse en cuenta y ejecutarse como parte de una serie de acciones concretas, con el objetivo de hacer frente a las regulaciones específicas del uso del correo electrónico, la pornografía infantil en Internet, así como todas aquellas conductas delictivas que menoscaben los derechos de las personas que deben ser protegidas por el Estado por medio de la norma jurídica.

2.4 Aproximación a la definición de los Delitos Informáticos

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. Por lo que se refiere a las definiciones que se han intentado dar en general, cabe destacar que no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos Penales, se requiere que la expresión 'delitos informáticos' esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún, tal como lo menciona el Dr. Julio Tellez. Para Carlos Sarzana, en su obra Criminalita e Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo."[55]

El Doctor Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin", y por las segundas, "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

a) Son conductas criminales de cuello blanco, en tanto que sólo un

[55] Carlos Sarzana, "seguridad de la información", revista de la segunda cohorte del Doctorado en seguridad en seguridad estratégica, Guatemala, Universidad de (2014), p, 126, dice: que los crímenes por computadoras comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Determinado número de personas con ciertos conocimientos (en este caso técnicos en una materia en específico) pueden llegar a cometerlas;

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando;
c) Son acciones de oportunidad, ya 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 las realizan;
e) Ofrecen posibilidades 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, y todo ello debido a la misma falta de regulación por parte del Derecho;
g) Son muy sofisticados y relativamente frecuentes en el ámbito militar;
h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico;
i) En su mayoría son imprudenciales y no necesariamente se cometen con intención;
j) Ofrecen facilidades para su comisión a los menores de edad;
k) Tienden a proliferarse cada vez más, por lo que requieren una urgente regulación;
l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por otra parte, debe de mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la Computadora, tales como delitos informáticos, delitos electrónicos, delitos

Relacionados con las computadoras, crímenes por computadora, delincuencia conexa con la computadora.

En síntesis, es destacable que la delincuencia informática se apoya en el delito Instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático.

Es importante definir los que es delito e informática, para luego discutir el término de delito informático y tener bien claro lo que se quiere decir:

1. Delito: es el acto típico, antijurídico y culpable penado por la ley;

2. Informática: Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento informático de la información por medio de ordenadores.

Por su parte, el delito informático se explica como la acción de un individuo

capaz de obtener, almacenar, modificar, distribuir, intercambiar, utilizar y transmitir la información a través de ordenadores, ya sea por medio de dispositivos externos (impresoras, discos flexibles, discos compactos, USB, entre otros), software e incluso firmware (un registro almacenado en la Memoria de sólo lectura del ordenador) quebrantando la ley. En los países ricos se cuenta con leyes que hablan sobre los delitos informáticos, los cuales están sancionados por penas que van desde los seis meses hasta dos años de cárcel, y con una multa variada que en ocasiones no alcanza derecho a fianza. En algunos países con menores recursos, existen solamente unos cuantos apartados dentro de sus respectivas Constituciones, mientras que otros ni siquiera lo tienen contemplado como un delito. Los delitos informáticos que se conocen están caracterizados de distintas maneras y he aquí algunos ejemplos:

1. Acceso en forma abusiva a la información 2. Introducción y ejecución de virus informáticos 3. Intercepción abusiva 4. Espionaje y falsificación 5. Violencia sobre bienes informáticos 6. Abuso de la detentación y difusión de códigos de acceso 7. Violación de correspondencia electrónica 8. Ultraje de información 9. Pornografía.

Esta serie de delitos va acompañada de un concepto llamado ingeniería social, el cual se refiere a una serie de mecanismos de captación de información con el fin de acceder a ordenadores y realizar las actividades ilícitas antes mencionadas, como por ejemplo: los malware (software maliciosos, del cual, surgen los virus y los spyware) los ataques a servidores, el phishing (falsificación de identidad), y el spam (correo no deseado), principalmente, es importante destacar que hasta hace poco tiempo, a través de la criptografía se podía clasificar mensajes de manera pública o privada, por ejemplo, mandar un mensaje a un destinatario para que, éste a su vez, lo pudiera encriptar y

codificar a través de una clave que el mismo destinatario poseía, siempre y cuando esto se llevara a cabo bajo un diseño y canal de comunicación seguros tanto del navegador como del servidor del que se trate.

Sin embargo, en la actualidad, esto ya se volvió arcaico, debido a que los hackers y crackers han implementado nuevas formas más sofisticadas de sabotear los sistemas informáticos. En este contexto, es necesario definir y explicar claramente el papel de hacker y cracker. Esto es importante dada la confusión existente respecto a las actividades que cada uno de ellos realiza, siendo estigmatizados ambos como “terroristas” por la sociedad.

Es fundamental también para entender el porqué de los delitos informáticos que se cometen a diario. Primero, tenemos al hacker que es un individuo que se introduce y modifica los sistemas de información de cualquier empresa, institución nacional o extranjera e incluso de individuos, siendo una persona hábil que cuenta con un código de ética como son: difundir la información obtenida por él mismo pero sin obtener nada a cambio, no dañar algo de manera intencional, modificar el acceso y evitar ser identificado y sobretodo, realizar acciones en servidores ajenos para no ser rastreado de forma inmediata en puntos alámbricos e inalámbricos cercanos. Incluso, esta figura ha sido contratada por empresas de distintas ramas para salvaguardar los sistemas computacionales, combatiendo los virus y a los creadores de los mismos.

Por otro lado, el cracker se enfoca particularmente al diseño de virus informáticos que él mismo introduce con el fin de alterar información, esto sí, para fines propios y de manera intencional y sin ningún código de ética, como son: la defraudación, la burla, o el terrorismo entre otros. Otro actor que participa paralelamente con el cracker es el pirata informático, cuyo trabajo es

la sustracción de información para la comercialización ilegal de copias de software legales con fines de lucro, adueñándose de los derechos de autor, así como el uso de técnicas para desproteger los programas y su utilización en forma ilegal, en este sentido se dice entonces que a cada momento que se dan avances tecnológicos de igual manera existen algunos sujetos que están cada día incursionando en nuevas formas de generar desmejora en el patrimonio así como en los datos de los sujetos pasivos.

2.5 Características de los Delitos Informáticos

En lo que respecta a las características se podrá observar el modo de operar De estos ilícitos:

a) Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas;
b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando;
c) Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico;
d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan;
e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse;
f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho;
g) Son muy sofisticados y relativamente frecuentes en el ámbito militar;

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico;
i) En su mayoría son imprudenciales y no necesariamente se cometen con intención;
j) Ofrecen facilidades para su comisión a los mentores de edad;
k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación;
l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Luego de todo lo mencionado se puede indicar de forma concreto de las características enunciadas que es importante señalar que se debe de actuar de la manera más eficaz para evitar este tipo de delitos y que no se sigan cometiendo con tanta impunidad, se debe de legislar de una manera seria y honesta, recurriendo a las diferentes personalidades que tiene el conocimiento, tanto técnico en materia de computación, como en lo legal (el Derecho), ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular

Según la doctrina, existen tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos: Acceso no autorizado, actos dañinos o circulación de material dañino e intercepción no autorizada.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos han tipificado y penado y penalizado estos tres tipos de comportamiento, ilícito. Muchos autores han abordado el tema con singular pasión, clasificando a los delitos informáticos sobre la base de

dos criterios: como instrumento o medio, o como fin u objetivo, los cuales son:

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

Como fin u objetivo: En ésta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Otros sin embargo advierten una clasificación sui géneris, "delitos electrónicos" diciendo que existen tres categorías, a saber:

Los que utilizan la tecnología electrónica como método (Conductas Criminógenas en donde los individuos utilizan métodos electrónicos para Llegar a un resultado ilícito); los que utilizan la tecnología electrónica como medio (Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo) y los que utilizan la tecnología electrónica como fin (conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla), Ahora bien puede realizarse un análisis objetivo de estas clasificaciones a los delitos informáticos: como instrumento o medio, o como fin u objetivo:

1. Como instrumento o medio: se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito;

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

3. Los que utilizan la tecnología electrónica como método;

4. Los que utilizan la tecnología electrónica como medio,

5. los que utilizan la tecnología electrónica como fin;

6. Como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito;

7. Como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo;

8. Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.6 Bien jurídico protegido en los delitos informáticos

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

2.6.1 Los Bienes Jurídicos Protegidos en los Delitos Informáticos

Dentro de los delitos informáticos, es por ello que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha

Agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección**,** esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede a criterio de Pablo Palazzi ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de “dañosidad” o “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de Beccaria “Los Delitos y las Penas” (1738 -1794).

Se define como un bien vital, “bona vitae”, estado social valioso, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma.
En conclusión se puede decir que el bien jurídico protegido en general es la

Información, pero está considerada en diferentes formas, ya sea como un valor económico, o como valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

a) El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar;

b) La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos;

c) La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos;

d) El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por lo que el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere, para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos,[56] es decir “que se caracterizan porque simultáneamente protege

[56] Alfonso Reyes Echandía**,** *La Tipicidad,* (Colombia: Universidad de Externado de Colombia, 1981), p.32.

varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo".

En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos, esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macro social), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macro social vinculado al funcionamiento delos sistemas informáticos"

El nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes(intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. En tal razón puede considerarse que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar se puede decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona al ver que su información personal es vista

por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro un bien colectivo que conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

2.7. Sujetos que intervienen en los Delitos Informáticos, perfil Criminológico del Delincuente

Se trata de abordar la calidad de los sujetos que intervienen en los delitos Informáticos, tanto la calidad del sujeto activo como también el sujeto pasivo, con ello se diferencia cuáles son las cualidades de cada uno de ellos, la actuación de los mismos.

2.7.1. Sujeto Activo en los Delitos Informáticos

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes.

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos

Informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente Informático es tema de controversia ya que para algún dicho nivel no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros". Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no están de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete.

Entre las características en común que poseen ambos delitos tenemos que: el

Sujeto activo del delito es una persona de cierto 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. Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Se considera que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objetos de un estudio más profundo. El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos teóricos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

2.7.2. Sujeto Pasivo en los Delitos Informáticos

En primer término puede distinguirse que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto

activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Es importante puntualizar que ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

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

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos, pero sobre todo es el mismo usuario de los servicios por medios de internet el que debe generarse una educación en cuanto al uso de los medios informáticos, ya que en muchas ocasiones la ingenuidad de parte de quien hace uso de la tecnología informática facilita el hecho delictivo.

2.8 Clasificación de los Delitos Informáticos

Los delitos informáticos abarcan una variedad de modalidades como se mencionan en la web de la INTERPOL, los cuales se exponen a continuación:

a) Ataques contra sistemas y datos informáticos;
b) Usurpación de la identidad;
c) Distribución de imágenes de agresiones sexuales contra menores;

d) Estafas a través de Internet;
e) Intrusión en servicios financieros en línea;
f) Difusión de virus;
g) *Botnets* (redes de equipos infectados controlados por usuarios remotos);
h) *Phishing* (adquisición fraudulenta de información personal confidencial).

Sin embargo no son los únicos, también existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información tales como:

a) Acceso a material inadecuado (ilícito, violento, pornográfico, etc.);
b) Adicción - Procrastinación (distracciones para los usuarios);
c) Problemas de socialización;
d) Robos de identidad;
e) Acoso (pérdida de intimidad);
f) Sexting (manejo de contenido erótico);
g) *Ciberbullying* (acoso entre menores por diversos medios: móvil, Internet, videojuegos, etc.);
h) Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat).

CAPITULO III

REGULACION JURIDICA SOBRE LOS DELITOS INFORMATICOS

El propósito en el presente capitulo es la de realizar un abordaje sobre los diferentes Convenios Internacionales existentes en materia de Delitos informáticos, así como en la Legislación Nacional en materia de los delitos Informáticos, y en el marco comparativo en la Legislación en otros Países relacionada con los Delitos Informáticos.

Se debe de hacer mención que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones políticas jurídicas de los problemas derivados, de la falta de seguridad al momento de utilizar los diferentes medios electrónicos, lo cual ha dado lugar a que, en algunos casos, se modifiquen las leyes como los códigos penales nacionales.

En un primer término, debe considerarse que en 1983, la OCDE[57] inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: Análisis de la Normativa Jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido

[57] Es la Organización para la Cooperación y el Desarrollo Económico.

que los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

El GATT[58], se transformó en lo que hoy es conocido como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes.

En el Art. 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

3.1 Convenios Internacionales

3.1.1 El convenio de Berna y su incidencia en la protección de los derechos de autor

Adoptado en 1886, el Convenio de Berna fue revisado en París (1896), y en Berlín (1908), completado en Berna en 1914 y revisado nuevamente en Roma (1928), en Bruselas (1948), en Estocolmo (1967) y en París (1971), y por último, fue objeto de enmienda en 1979.

[58] General Agreement on Tariffs and Trade, que traducido en español es conocido como Acuerdo General sobre Comercio y Aranceles, que se trata de un convenio que fue ideado en el marco de la Conferencia de La Habana que se llevó a cabo en el año 1947 y que fue firmado un año después por 23 países, con el objetivo de fijar un conjunto de pautas de alcance comercial y concesiones arancelarias.

El Convenio de Berna trata de la protección de las obras y los derechos de los Autores, los cuales se fundan en tres principios básicos y contiene una serie de disposiciones que determinan la protección mínima que ha de conferirse, así como las disposiciones especiales para los países en desarrollo que quieran valerse de ellas.

Los principios básicos son los siguientes:

a) Las obras originarias de uno de los Estados Contratantes es decir, las obras cuyo autor es nacional de ese Estado o que se publicaron por primera vez en él, deberán ser objeto, en todos y cada uno de los demás Estados Contratantes, de la misma protección que conceden a las obras de sus propios nacionales el principio del "trato nacional";
b) La protección no deberá estar subordinada al cumplimiento de formalidad alguna principio de la protección "automática";
c) La protección es independiente de la existencia de protección en el país de origen de la obra (principio de la "independencia" de la protección). Empero, si en un Estado Contratante se prevé un plazo más largo de protección que el mínimo prescrito por el Convenio, y cesa la protección de la obra en el país de origen, la protección podrá negarse en cuanto haya cesado en el país de origen.

Las condiciones mínimas de protección se refieren a las obras y los derechos que han de protegerse, y a la duración de la protección:

a) En lo que hace a las obras, la protección deberá extenderse a "todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión" (párrafo 1 del artículo 2 del Convenio);
b) Con sujeción a ciertas reservas, limitaciones o excepciones permitidas,

los siguientes son algunos de los derechos que deberán reconocerse como derechos exclusivos de autorización: el derecho a traducir, el derecho de realizar adaptaciones y arreglos de la obra, el derecho de representar y ejecutar en público las obras dramáticas, dramático musicales y musicales, el derecho de recitar en público las obras literarias, el derecho de transmitir al público la representación o ejecución de dichas obras, el derecho de radiodifundir los Estados Contratantes cuentan con la posibilidad de prever un simple derecho a una remuneración equitativa, en lugar de un derecho de autorización, el derecho de realizar una reproducción por cualquier procedimiento y bajo cualquier forma (los Estados Contratantes podrán permitir, en determinados casos especiales, la reproducción sin autorización, con tal que esa reproducción no atente contra la explotación normal de la obra ni cause un perjuicio injustificado a los intereses legítimos del autor y, en el caso de grabaciones sonoras de obras musicales, los Estados Contratantes podrán prever el derecho a una remuneración equitativa, el derecho de utilizar la obra como base para una obra audiovisual y el derecho de reproducir, distribuir, interpretar o ejecutar en público o comunicar al público esa obra audiovisual asimismo, el Convenio prevé "derechos morales", es decir, el derecho de reivindicar la paternidad de la obra y de oponerse a cualquier deformación, mutilación u otra modificación de la misma o a cualquier atentado a la misma que cause perjuicio al honor o la reputación del autor;

c) Por lo que respecta a la duración de la protección, el principio general es que deberá concederse la protección por el plazo de los 50 años posteriores a la muerte del autor. Sin embargo, existen excepciones a ese principio general. En el caso de obras anónimas o seudónimas, el plazo de protección expirará 50 años después de que la obra haya sido lícitamente hecha accesible al público, excepto cuando el seudónimo no deja dudas sobre la identidad del autor o si el autor revela su identidad durante ese período; en

este último caso, se aplicará el principio general. En el caso de las obras audiovisuales cinematográficas, el plazo mínimo de protección es de 50 años después de que la obra haya sido hecha accesible al público "exhibida" o, si tal hecho no ocurre, desde la realización de la obra. En el caso de las obras de artes aplicadas y las obras fotográficas, el plazo mínimo es de 25 años contados desde la realización de la obra.

El Convenio de Berna permite ciertas limitaciones y excepciones en materia de derechos económicos, es decir, los casos en que las obras protegidas podrán utilizarse sin autorización del propietario del derecho de autor y sin abonar una compensación. Generalmente se utiliza el término "libre utilización" de obras protegidas para referirse a esas limitaciones, y figuran en el párrafo 2) del artículo 9 reproducción en determinados casos especiales, el artículo 10 citas y uso de obras a título de ilustración de la enseñanza, el artículo 10 *bis* reproducción de artículos de periódicos o artículos similares y el uso de obras con fines de información sobre acontecimientos actuales y el párrafo 3 del artículo 11 bis grabaciones efímeras con fines de radiodifusión.

3.1.2 La convención sobre la propiedad intelectual de Estocolmo

El Convenio de la OMPI, el instrumento constitutivo de la Organización Mundial de la Propiedad Intelectual (OMPI), fue firmado en Estocolmo el 14 de julio de 1967, entró en vigor en 1970 y fue enmendado en 1979. La OMPI es una organización intergubernamental que en 1974 pasó a ser uno de los organismos especializados del sistema de organizaciones de las Naciones Unidas.

Los orígenes de la OMPI se remontan a 1883 y a 1886, cuando se adoptaron, respectivamente, el Convenio de París para la Protección de la Propiedad

Industrial y el Convenio de Berna para la Protección de las Obras Literarias y Artísticas. Ambos Convenios preveían el establecimiento de sendas "Oficinas Internacionales".

Las dos Oficinas se unieron en 1893 y en 1970 fueron sustituidas por la Organización Mundial de la Propiedad Intelectual, establecida en virtud del Convenio de la OMPI.

La OMPI tiene dos objetivos principales, el primero de ellos es fomentar la protección de la propiedad intelectual en todo el mundo.

El segundo es asegurar la cooperación administrativa entre las Uniones que entienden en materia de propiedad intelectual y que han sido establecidas en virtud de los tratados administrados por la OMPI, con el fin de alcanzar esos objetivos, la OMPI, además de encargarse de las tareas administrativas de las Uniones, lleva a cabo diversas actividades que incluyen:

a) actividades normativas, es decir, la creación de reglas y normas para la protección y la observancia de los derechos de propiedad intelectual mediante la concertación de tratados internacionales;
b) actividades programáticas, que comprenden la prestación de asistencia técnica y jurídica a los Estados en el ámbito de la propiedad intelectual;
c) actividades de normalización y de clasificación internacionales, que incluyen la cooperación entre las oficinas de propiedad industrial en lo que respecta a la documentación relativa a las patentes, las marcas y los dibujos y modelos industriales;
d) actividades de registro y presentación de solicitudes, que comprenden la prestación de servicios relacionados con las solicitudes internacionales de patentes de invención y el registro de marcas.

3.1.3 La convención para la protección y producción de fonogramas de 1971

El Convenio de Ginebra o Convenio Fonogramas establece la obligación de los Estados Contratantes de proteger a los productores de fonogramas que son nacionales de otro Estado Contratante contra la producción de copias sin el consentimiento del productor, contra la importación de dichas copias, cuando la producción o la importación se haga con miras a la distribución al público, y contra la distribución de esas copias al público.

Se entenderá por "fonograma" la fijación exclusivamente sonora por lo que no incluye, por ejemplo, las bandas sonoras de películas o de cintas de video, cualquiera que sea su forma disco, cinta, etc.

La protección puede otorgarse mediante la legislación sobre derecho de autor, una legislación *sui generis* derechos conexos, la legislación sobre competencia desleal o el derecho penal.

La protección debe tener una duración mínima de 20 años contados desde la fecha de la primera fijación o la primera publicación del fonograma, sin embargo, las legislaciones nacionales prevén cada vez con mayor frecuencia un plazo de protección de 50 años.

El Convenio permite las mismas limitaciones que las previstas en relación con la protección de los autores. Permite licencias no voluntarias si la reproducción tiene por único objeto la enseñanza o la investigación científica, limitadas al territorio del Estado cuyas autoridades conceden la licencia, y si se abona una remuneración equitativa artículo 6.

3.1.4 Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidos por satélite de 1974

El Convenio de Bruselas o Convenio Satélites establece la obligación de los Estados Contratantes de tomar medidas adecuadas para impedir que, en su territorio o desde él, se distribuyan sin autorización señales portadoras de programas transmitidas por satélite. Se considera que una distribución carece de autorización si no ha sido autorizada por el organismo por lo general, un organismo de radiodifusión que ha decidido el contenido del programa. La obligación rige respecto de los organismos que son "nacionales" del Estado Contratante.

El Convenio permite ciertas limitaciones a la protección. Se permite la distribución de señales portadoras de programas por personas no autorizadas si esas señales son portadoras de breves fragmentos que contengan informaciones sobre acontecimientos de actualidad o, cuando se trate de citas, breves fragmentos del programa que portan las señalas emitidas o, en el caso de los países en desarrollo, si el programa del que son portadoras las señales emitidas se distribuye con fines educativos exclusivamente, incluida la enseñanza de adultos y la investigación científica. En el Convenio no se establece un plazo de protección y se deja esta cuestión al arbitrio de la legislación nacional. Sin embargo, no se aplican las disposiciones del Convenio cuando la distribución de señales se efectúa desde satélites de radiodifusión directa.

3.1.5 Convenio sobre la ciberdelincuencia o convenio de Budapest

El día 23 de noviembre del año 2001, los Estados miembros del Consejo de Europa formalizó la Convención sobre la Ciberdelincuencia, también conocida

Como Convenio de Budapest. Las conductas ilícitas, reguladas en el Convenio de Budapest, son: el acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia de sistema, uso erróneo de dispositivos, falsificación del ordenador, fraude del ordenador, pornografía infantil. También se establecen disposiciones de índole procesal para la preservación de datos almacenados, y todo lo relacionado a los actos procesales para producir prueba y aislar todo acto de cibercrimen.

El Convenio de Budapest fue celebrado a nivel del Consejo de Europa, no existe ningún impedimento legal para que otros países, como es el caso de El Salvador que ha podido adherirse a dicha normativa. Al contrario, tanto para Europa como para los países de América Latina y todos los países del mundo, la normativa se convierte en derecho positivo cuanto mayor sea el número de países que se adhieran a la misma.

El convenio establece en parte de su preámbulo "Convencidos de que el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable" [59] por lo que se puede mencionar que desde hace algunos años se está realizando esfuerzos en materia penal y en específico a la delincuencia informática.

[59] Convenio sobre la Ciberdelincuencia, 2001, párrafo noveno del preámbulo.

3.1.6 Congreso de las Naciones Unidas sobre prevención del delito y justicia penal

También organismos intergubernamentales han procurado realizar algunos aportes importantes en materia de criminalidad informática como es el caso del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal fue patrocinada por el Gobierno de Brasil y tuvo lugar en Salvador de Bahía, del 12 al 19 de abril de 2010, los congresos de las Naciones Unidas sobre Prevención del Delito se han venido celebrando cada cinco años, desde 1955, en distintas partes del mundo y en torno a una amplia variedad de temas.

Los congresos han tenido una considerable repercusión en la esfera de la prevención del delito y la justicia penal a escala internacional y han influido en las políticas y prácticas profesionales de los países. Como plataforma mundial, los congresos posibilitan el intercambio de información y de mejores prácticas entre los Estados y profesionales que trabajan en este sector. Su objetivo global es el de promover políticas de prevención del delito y medidas de justicia penal más eficaces en todo el mundo.

En dicho congreso se lograron acuerdos como determinar nuevas formas de delincuencia que planteen una amenaza a las sociedades de todo el mundo y analizar los medios para prevenirlas y controlarlas.

3.1.7 Grupo de trabajo en delito informático de la organización de Estados Americanos

Se menciona que este convenio que se llevó a cabo en el continente Americano, ha sido uno de los más principales en cuanto a su importancia ya

Es el principal foro hemisférico establecido desde 1999 por las REMJA[60] para Fortalecer la cooperación internacional en la investigación y persecución del delito cibernético, facilitar el intercambio de información y de experiencias entre sus integrantes y formular las recomendaciones que sean necesarias para mejorar y garantizar el combate contra este delito, que está integrado Los expertos gubernamentales de los Estados miembros de la OEA con responsabilidades en materia de delito cibernético o en cooperación internacional en su investigación y persecución. Dentro de sus funciones que tiene este equipo de trabajo están:

a) Considerar e implementar los mandatos que reciba de las REMJA;
b) Informar a las REMJA sobre los avances dados en el desarrollo de sus mandatos;
c) Facilitar el intercambio de información y de experiencias;
d) Fortalecer la cooperación entre las autoridades que participan en el mismo;
e) Formular recomendaciones para mejorar y fortalecer la cooperación entre los Estados miembros de la OEA y con otras organizaciones o mecanismos internacionales.

La difusión de la informática ha llegado a todos los ámbitos de la actividad humana.

La reglamentación que busca una forma de convivencia más armónica dentro de las sociedades, tratando de prevenir o castigar las conductas que riñen con el bienestar de la mayoría, no está exenta de los efectos de este nuevo medio.

[60] Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas.

Algunos países han venido legislando sobre temas relativos a la comisión de delitos vinculados a la informática, ya sea porque utilizan herramientas informáticas para realizarlos, o porque el blanco de la infracción es de índole informática.

3.2 Legislación Nacional sobre los delitos informáticos

En este apartado trata de enfocarse en la normativa que comprende el Estado de El Salvador, en materia Informática Penal.

3.2.1 Ley especial contra los delitos informáticos y conexos

En el caso de El Salvador se ha implementado respecto a los delitos informáticos una Ley Especial donde se regula el accionar de aquellas conductas ilícitas de quienes utilizan el conocimiento informático para hacerse valer de la información de otras personas y afectar así su patrimonio, esta ley tiene dentro de esa regulación el delito de La Estafa Informática regulada en el Art. 10 de la Ley Especial Contra los Delitos Informáticos y Conexos el cual menciona “El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años. Se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos:

a) En perjuicio de propiedades del Estado;
b) Contra sistemas bancarios y entidades financieras; y
c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos."

Se sabe que estos no son los únicos delitos informáticos que establece la ley en comento, pero se trata de enfocarse en el tema de estudio, es decir propiamente lo relacionado a la estafa informática.

3.2.2. **Código penal Salvadoreño**

Hasta la modificación del Código Penal, las estafas en el ámbito informático tenían que ser analizadas bajo la regulación tradicional y, por ello, la identificación de los supuestos debía hacerse mediante analogía con la estafa incluso con la apropiación indebida, dando lugar a condenas relativamente bajas.

Actualmente y con la evolución a la que se hace referencia, la persecución de las estafas informáticas ha sido recogida en el Código Penal, y supone junto a otras medidas de carácter policial. De esta forma, el primero de los apartados del artículo 216 numeral 5 castiga a quienes se valgan de medios informáticos para conseguir bienes de la víctima.

Este supuesto incluye todos los casos en los que los delincuentes utilizan software mal intencionado para hacerse con los datos de la víctima como los famosos troyanos y otros programas espías, todas las modalidades de estafas

directas mediante engaños a la hora de facilitar datos en la red, como es el caso de las denominadas cartas nigerianas, en las que el delincuente promete una cantidad económica a la víctima a cambio de un adelanto o de ciertos datos personales. También son muy comunes en la red las ofertas o sorteos que asaltan al usuario cuando entra en una web y que prometen suculentos premios a cambio de ciertas cantidades de dinero.

En el caso que establece el código penal, de acuerdo a lo establecido en el artículo en comento se realiza la conducta típica de la Estafa agravada cuando realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos, y tal como se señala en dicha obra con esta descripción se engloba todos los casos en los que se realiza una transferencia no consentida de activos patrimoniales en perjuicio de terceros, la difusión de la informática ha llegado a todos los ámbitos de la actividad humana.

La reglamentación que busca una forma de convivencia más armónica dentro de las sociedades, tratando de prevenir o castigar las conductas que riñen con el bienestar de la mayoría, no está exenta de los efectos de este nuevo medio.

Algunos países han venido legislando sobre temas relativos a la comisión de delitos vinculados a la informática, ya sea porque utilizan herramientas informáticas para realizarlos, o porque el blanco de la infracción es de índole informática. Venezuela es uno de los países que se encuentra en este momento presentando y discutiendo una ley acerca de este tipo de delitos.

La ley tipifica los delitos informáticos, contempla en la categoría de delitos contra los sistemas que utilizan tecnologías de información los siguientes: el Acceso indebido; el Sabotaje o daño a sistemas; el Sabotaje o daño culposos, es decir, el mismo anterior, pero cometido por imprudencia, negligencia,

impericia o inobservancia de las normas establecidas; el Acceso indebido o sabotaje a sistemas protegidos; la Posesión de equipos o prestación de servicios de sabotaje; el Espionaje informático; y la Falsificación de documentos.

En la categoría de delitos contra la propiedad, se incluyen: el Hurto; el Fraude; la Obtención indebida de bienes o servicios; el Manejo fraudulento de tarjetas inteligentes o instrumentos análogos; la Apropiación de tarjetas inteligentes o instrumentos análogos; la Provisión indebida de bienes o servicios; y la Posesión de equipo para falsificaciones.

Entre los delitos contra la privacidad de las personas y de las comunicaciones, se hallan: la Violación de la privacidad de la data o información de carácter personal; la Violación de la privacidad de las comunicaciones; y la Revelación indebida de data o información de carácter personal, en la clase de los delitos contra niños o adolescentes, se incluyen: la Difusión o exhibición de material pornográfico; y la Exhibición pornográfica de niños o adolescentes.

Finalmente, en cuanto a los delitos contra el orden económico, se consideran como tales: la Apropiación de propiedad intelectual; y la Oferta engañosa, la ley contempla las penas que se aplicarán en cada uno de los delitos incluidos, así como los agravantes que pueden suceder en estos delitos, más temprano que tarde, nuestro país necesitará contar con legislaciones similares.

Primeramente el delito de Amenazas que atentaren contra la seguridad de la persona y su familia a través de medios electrónicos o que pudiesen ser anónimos. Por ejemplo: amenazas de muerte a profesores universitarios a través de correo electrónico, dicho delito de Amenazas se encuentra regulado en el Art. 154, El que amenazare a otro con producirle a él o a su familia, un

daño que constituyere delito, en sus personas, libertad, libertad sexual, honor o en su patrimonio, será sancionado con prisión de uno a tres años.

La Agravación Especial regulada en el Art. 155, en los casos de los artículos anteriores se considerarán agravantes especiales que el hecho fuere cometido con arma o por dos o más personas reunidas o si las amenazas fueren anónimas o condicionales. En estos casos la sanción se aumentará hasta en una tercera parte de su máximo.

Los Delitos de Promoción de pornografía infantil, exhibiciones obscenas a través de internet y correo electrónico. Por ejemplo: promoción de pornografía a través de páginas web, así como el envío de imágenes por medio de electrónico. Inducción, promoción, favorecimiento y determinación de la prostitución a través de internet y correo electrónico. Por ejemplo: el envío de correos electrónicos a distintas personas para que accedan a un sitio pornográfico.

EL Art. 169 establece: El que indujere, facilitare, promoviere o favoreciere la prostitución de persona menor de dieciocho años, será sancionado con prisión de dos a cuatro años.
Cuando cualquiera de estas modalidades se ejecutare prevaliéndose de la superioridad originada por cualquier relación, se impondrá además una multa de cincuenta y cien días multa.

También se puede mencionar la determinación a la prostitución regulada en el Art. 170 menciona: El que determinare coactivamente o abusando de una situación de necesidad, a una persona para que ejerciere la prostitución o se mantuviere en ella, será sancionado con prisión de uno a tres años, cuando cualquiera de estas modalidades fuere ejecutada prevaliéndose de la

superioridad originada por cualquier relación, se impondrá junto con la pena correspondiente una multa de cincuenta a cien días multa; la pena de prisión será de dos a cuatro años, cuando la víctima fuere menor de dieciocho años de edad.

Otro delito en mención es el de Exhibiciones obscenas regulado en el Art. 171, que dice “El que ejecutare o hiciere ejecutar a otros actos lúbricos o de exhibición obscena ante menores de dieciocho años de edad o deficientes mentales, será sancionado con prisión de seis meses a dos años”.

La Pornografía regulada en el Art.172 hace mención: “El que por cualquier medio directo, difundiere, vendiere o exhibiere material pornográfico entre menores de dieciocho años de edad o deficientes mentales, será sancionada con prisión de seis meses a dos años.”

La utilización de menores con fines pornográficos y exhibicionistas regulada en el Art. 173 establece que “El que utilizare a un menor de dieciocho años, con fines o en espectáculos exhibicionistas o pornográficos, será sancionado con prisión de seis meses a dos años y multa de treinta a sesenta días multa”, Intercepción de mensajes electrónicos y otra información, por ejemplo: a través de la red se pueden interceptar correos electrónicos, obtención de claves de acceso y/o información electrónica, un ejemplo es: el uso de programas para monitorear el uso de computadoras, a través de los cuales se pueden obtener las claves y/o información.

Divulgación de secretos profesionales, se menciona como ejemplo: la publicación a través del internet y correo electrónico (un foro, chat, etc.), Sobre los secretos administrativo de una empresa.

También se puede hacer mención los Artículos que pueden ser empleados en la regulación de penal de Violación de comunicaciones privadas esto regulado en el Art. 184: El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivos o registro público o privado, será sancionado con multa de cincuenta a cien días multa, Si difundiere o revelare a terceros los datos revelados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa, y el tercero a quien se revelare el secreto y lo divulgare ha sabiendo de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa, violación agravada de comunicaciones.

También es de suma importancia el hablar sobre Captación de comunicaciones regulado en el Art. 186 “El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artículos técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa”, Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

Otra regulación relacionada al tema en curso producto de la presente es la Revelación De Secreto Profesional regulada en el Art. 187 El que revelare un secreto del que se ha impuesto en razón de su profesión u oficio, será sancionado con prisión de seis meses a dos años e inhabilitación especial de

profesión u oficio de uno a dos años, menciona que el tercero a quien revelare el secreto y lo divulgare, a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

Otros delitos relacionados a los Delitos informáticos es el Delito Robo de hardware; Robo de títulos valores a través de transacciones electrónicas; por ejemplo: el robo de un domino. Robo de capital por medio de infiltración electrónica a cuentas varias, personales, comerciales y estatal. Por ejemplo: alterar una cuenta del banco Cuscatlán a través de su sitio en el internet. Estafa electrónica para beneficio propio y terceros. Por ejemplo: los empleados pueden modificar los balances de las cuentas bancarias para su beneficio.

Los Artículos que pueden ser empleados es el que regula el Hurto Art. 207, el cual menciona que el que con ánimo de lucro para sí o para un tercero, se apoderare de una cosa mueble, total o parcialmente ajena, sustrayéndola de quien la tuviere en su poder, será sancionado con prisión de dos a cinco años, si el valor de la cosa hurtada fuere mayor de quinientos colones.

El Hurto Agravado regulado en Art. 208, cuya sanción será de cinco a ocho años de prisión, si el hurto fuere cometido con cualquiera de las circunstancias siguientes:

a) Empleando violencia sobre las cosas;
b) Usando la llave verdadera que hubiere sido sustraída, hallada o retenida; llave falsa o cualquier otro instrumento que no fuere la llave utilizada por el ofendido. Para los efectos del presente numeral se considerarán llaves las tarjetas magnéticas o perforadas y los mandos o instrumentos de apertura de contacto o a distancia;
c) Aprovechando estrago o calamidad pública o una situación de desgracia particular del ofendido;

d) Con escalamiento;
e) Arrebatando las cosas del cuerpo de las personas;
f) Por dos o más personas;
g) Usando disfraz;
h) Engañado;
i) En vehículos de motor;
j) Sobre objetos que formaren parte de la instalación de un servicio público o cuando se tratare de objetos de valor científico o cultural.

Estafa Agravada (De Los 5 Literales, Solo Son Aplicables El 1, 2, 4 Y 5), Ya entrando más de lleno a la discusión en mención sobre los delitos informáticos podemos mencionar lo regulado en el artículo Art. 216 menciona que: El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

1) Si recayere sobre artículos de primera necesidad, viviendas o terrenos destinados a la construcción de viviendas;
2) Cuando se colocare a la víctima o su familia en grave situación económica, o se realizare con abuso de las condiciones personales de la víctima o aprovechándose el autor de su credibilidad empresarial o profesional;
3) Cuando se obrare con el propósito de lograr para sí o para otro el cobro indebido de un seguro; y
4) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

El inciso número 2 del Art. 222 del Código penal, menciona que si el daño se realizare mediante manipulación informática; los delitos que se mencionan son: la reproducción de software, con fines de lucro, la reproducción de música

y video con fines de lucro, por ejemplo: la grabación de música (de archivos mp3 a cinta o CD de audio), para luego ser vendida; comercialización de sistemas sin autorización previa del programador, por ejemplo: si una farmacia le vende a otra su programa sin previo aviso al programador.

Adjudicarse una obra electrónica, ejemplo de esto es: adquirir un libro de la red, y luego cambiarle el nombre del autor; también se da la violación de distintivos que puede ser aquella en que se: realiza una venta, utilizando el distintivo de una empresa sin autorización de esta; violación de derechos de autor y derechos conexos.

El Art. 226. Dice que: “El que reprodujere, plagiare, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística, científica o técnica o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de uno a tres años.”

En la misma sanción incurrirá quien no depositare en el Registro de Comercio, importare, exportare o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

La estafa informática tiene su regulación de manera especial en el Art. 10 de la ley especial contra los delitos informáticos y conexos el cual regula: “El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio

tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años, se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos:

a) En perjuicio de propiedades del Estado;

b) Contra sistemas bancarios y entidades financieras; y,

c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos."

3.2.3 Ley especial contra Actos de Terrorismo

Establece en su artículo 12 el delito informático en el que menciona que será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades

Nacionales, internacionales o de otro país;

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a, de este artículo.

Tal y como lo establece en su considerando IV en el que menciona que actualmente el terrorismo constituye una grave amenaza para la seguridad del país, la paz pública y la armonía de los Estados, afectando directa e indirectamente a sus nacionales en su integridad física y moral, así como en la propiedad, posesión y conservación de sus derechos, lo que hace necesario la creación de una ley especial para prevenir, investigar, sancionar y erradicar las actividades terroristas respondiendo a las circunstancias actuales y excepcionales que afectan a la comunidad internacional, y en este sentido para estar en armonía con las normas internacionales en la lucha en contra del accionar delincuencial con utilización de medios informáticos.

3.2.4 Ley Especial para sancionar Infracciones Aduaneras

En la actualidad, se cuenta con la Ley especial para sancionar infracciones aduaneras, en la sección quinta la ley hace mención de las infracciones aduaneras penales, en su artículo 24 el cual establece que los delitos informáticos serán sancionados con prisión de tres a cinco años, quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por la Dirección General;
b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases

de datos, que de manera exclusiva y en el ejercicio de sus controles y servicios utilizare la Dirección General;

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra personal;

d) facilite el uso del código y la clave de acceso, asignados para ingresar en los sistemas informáticos. La pena será de uno a tres años si el empleo se facilita culposamente; y

e) Manipule el sistema informático o de comunicaciones a fin de imposibilitar cualquier control que con base en dicho sistema exista la posibilidad de realizar.

Como se puede mencionar en cuanto a la regulación de las manipulaciones informáticas sin consentimiento del sujeto pasivo, se han realizado muchos esfuerzos para poder establecer en las normas jurídica, y que se pueda por medio de la regulación proteger a los sujetos que sufren de los abuso de parte del sujeto activo que en base a su conocimiento manipula para sí o para tercero los sistemas informáticos, y con ello desmejorar el patrimonio del sujeto pasivo el cual se ve desmejorado por la conducta delictiva del actor del delito, es entonces que el legislador hace un esfuerzo por garantizar por medio de las normas jurídicas la protección del bien jurídico del sujeto pasivo, el cual está siendo víctima y ve desmejora en su patrimonio, es de esta forma como nace la protección que garantice al sujeto pasivo el poder acudir al juzgado en caso de ser víctima en esta nueva forma de delincuencia.

3.3 Legislación en otros países relacionada con los delitos informáticos

En este apartado se realiza un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

Costa Rica

Los primeros tipos penales informáticos en Costa Rica datan del año 2001 cuando se crearon e incluyeron en el Código Penal los delitos de violación de comunicaciones electrónicas en su artículo 196 bis, el fraude electrónico regulado en el artículo 217 bis, y alteración de datos y sabotaje informático establecido en el artículo 229 bis, los cuales fueron modificados con la nueva ley que es conocida como Ley 9048, esta ley Reforma varios artículos y modifico la sección VIII denominada delitos informáticos y conexos, del título VII del Código Penal.

Costa Rica, A partir de la reforma del Código Penal, en el 2012, en materia de Delitos Informáticos, Costa Rica incorporó en su normativa un aspecto muy novedoso en materia penal, en su artículo 232 inciso “e”, señala la Instalación o propagación de programas informáticos maliciosos, será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.[61]

De esta manera, se estableció como delito lo que tradicionalmente conocemos como SPAM, que para los efectos lo podemos comprender cómo: todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Esta conducta es particularmente grave cuando se realiza en forma masiva.
Resulta importante señalar que bajo esta comprensión, el SPAM no es solo por correo electrónico, actualmente existe un sinfín de maneras para realizarlo, pensemos en aplicaciones como WhatsApp Líne, mensajes de texto, etc., las cuales ofrece la posibilidad de que se realice este envío masivo de comunicaciones no solicitadas.

Es importante resaltar que la persecución penal, según lo establece el delito, va a actuar contra las personas que *ofrezca, contrate o brinde servicio* de envío de comunicaciones masivas no solicitadas, actualmente es muy común encontrar en Internet este tipo de ofrecimientos que por un pago permite a una persona o empresa el envío de información no solicitada, por correo, voz, fax, etc., y no se conoce la manera cómo consiguieron las bases de datos con las que trabajan, y si las personas autorizaron que se les envíe ese tipo de información; es común escuchar a muchos ciudadanos relatar que reciben

[61] Código Penal, Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII (Costa Rica: Procuraduría General de la Republica, 2012) artículo 3.

correos de ofertas, llamadas telefónicas para ofrecerles tarjetas u otros productos, y las personas se preguntan ¿cómo saben mis datos y mi teléfono?; es claro que están usando nuestros datos al margen de la ley, y en muchas de las ocasiones es el mismo usurario el que lo permite sin enterarse, como cuando activa señal de wife fuera de su zona de seguridad, ya que cuando su aparato activa esta señal pueden estar siendo interferidos sus archivos.

Chile

En el año 1993 se promulgo la ley 19223 “ley de delitos informáticos”. Esta que constaba de cuatro artículos fue la primera ley en Latinoamérica en establecer reglas para el uso de la informática, La ley 19223 que tipifica figuras penales relativas a la informática o “ley de delitos informáticos”, fue promulgada el 28 De mayo de 1993 y publicada el 07 de junio 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. Asimismo, dentro de esas consideraciones se encuentran los virus.

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

Aunque ésta ha sido la primera ley en América Latina concerniente a los delitos informáticos, hoy en día ha sufrido mucha crítica de arte de la comunidad jurídica chilena, ya que se le considera desfasada respecto a los

avances tecnológicos sufridos desde la fecha de promulgación hasta la actualidad ya que en aquel momento no existía la delincuencia cibernética que existe hoy. Pero con todo y ello se resalta la importancia que ha tenido por ser uno de los primeros esfuerzos a nivel continental en la protección de carácter informático.

CAPITULO IV

ESTAFA TRADICIONAL REGULADA EN EL ARTÍCULO 215 Y 216, DEL CODIGO DE PENAL, ESTAFA INFORMATICA SEGÚN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS, Y LOS ELEMENTOS DIFERENCIADORES

El propósito en el presente capitulo es tratar de establecer las generalidades de las estafa convencional, para luego poder realizar una mención los elementos básicos de la misma, con el propósito de comprender de una forma más sencilla que elementos son los que se diferencian entre la estafa convencional y la estafa informática.

4.1 Delito de estafa básica o convencional

En el presente apartado se trata de establecer los elementos de la estafa convencional, y la estafa informática, con el objetivo de poder establecer cuáles de ellos son los diferenciadores entre tipo de estafas.

El delito de estafa surgió como tal, a mediados del Siglo XIX; desde entonces, se ha tratado de construir una concepción genérica que abarque todas las consideraciones que influyen en esta conducta y la distingan del fraude civil como de otros comportamientos típicos similares, es así que se establecerá con base doctrinaria cual es la definición que se adecua a la normativa penal salvadoreña, pero antes de realizar una definición, es necesario poder conocer de manera general algunas regulaciones tanto a nivel constitucional así como en tratados internacionales, que estos se convierten en leyes una vez aprobados por los países que los suscriben.

El artículo 2 inciso primero de la Constitución de la República de El Salvador, Sostiene como derecho fundamental de todas las personas, el Derecho de Propiedad y Posesión “Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos.

Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se establece la indemnización, conforme a la ley, por daños de carácter moral”, por su parte la Declaración Americana de los Derechos y Deberes del Hombre (1948) reconoce el derecho a la propiedad en su Art. 23: “Toda persona tiene derecho a la propiedad privada correspondiente a las necesidades esenciales de una vida decorosa, que contribuya a mantener la dignidad de la persona y del hogar”.

También lo contempla la Declaración Universal de Derechos Humanos de adoptada el 10 de diciembre en Paris, Francia en el año de 1948 en su Artículo 17, que establece:

a) Toda persona tiene derecho a la propiedad, individual y colectivamente;
b) Nadie será privado arbitrariamente de su propiedad.

El artículo en comento menciona el derecho a la propiedad individual y colectiva, así como, del derecho que tiene toda persona a no ser privada arbitrariamente de su propiedad.

La Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica de 1969, lo regula en su Art. 21 Derecho a la Propiedad Privada:

1) Toda persona tiene derecho al uso y goce de sus bienes, la ley puede subordinar tal uso y goce al interés social;

2) Ninguna persona puede ser privada de sus bienes, excepto mediante El pago de indemnización justa, por razones de utilidad pública o de interés social y en los casos y según las formas establecidas por la ley;

3) Tanto la usura como cualquier otra forma de explotación del hombre por el hombre, deben ser prohibidas por la ley"´

A nivel de legislación secundaria, el Artículo 215 del Código Penal de El Salvador, salvaguarda este bien jurídico de la siguiente manera: "El que obtuviere para sí o para otro un provecho injusto en perjuicio ajeno, mediante ardid o cualquier otro medio de engañar ò sorprender la buena fe, será sancionado con prisión de dos a cinco años, si la defraudación fuere mayor de doscientos colones.

Para la fijación de la sanción el Juez tomará en cuenta la cuantía del perjuicio, la habilidad o astucia con que el agente hubiere procedido y si el perjuicio hubiere recaído en persona que por su falta de cultura ò preparación fuera fácilmente en ganable".

El art. 216 del Código Penal, le brinda protección a este Derecho; a través de la regulación de conductas que puedan poner en peligro o concreta lesión el bien jurídico en comento, en sus agravantes: " El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

a) Si recayere sobre artículos de primera necesidad, viviendas o terrenos destinados a la construcción de viviendas;

b) Cuando se colocare a la víctima o su familia en grave situación económica, o se realizare con abuso de las condiciones personales de

la víctima o aprovechándose el autor de su credibilidad empresarial o profesional;

c) Cuando se realizare mediante cheque, medios cambiarios o con abuso de firma en blanco;

d) Cuando se obrare con el propósito de lograr para sí o para otro el cobro indebido de un seguro; y

e) cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

Así también muchas otras legislaciones por ejemplo la Civil y la Mercantil entre otras, le dan un ámbito de protección a este derecho, claro está que en un sentido diferente a la protección que emerge del ámbito Penal, el cual lleva imbíbito perse el carácter de Ultima ratio.

Como el propósito de este apartado no es el realizar un exhaustivo estudio sobre el delito de estafa convencional sino más bien el poder sentar algunas bases que luego servirán como parámetro para poder establecer los elementos que diferencian a esta clase de estafa del delito de estafa informática, se realizar un pequeño desarrollo de los elementos propios de la estafa tradicional.

4.2 Definición del delito Estafa

La estafa consiste en la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que determinando un error en una o varias personas las induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su

Patrimonio o en el de un tercero. La definición refleja claramente los elementos exigidos por el tipo de estafa: engaño, error, acto de disposición patrimonial, perjuicio y ánimo de lucro, dichos elementos no pueden aparecer en forma aislada, sino que deben estar relacionados de manera especial.

4.3 Naturaleza del delito de Estafa

La estafa es un delito de resultado que requiere la existencia de perjuicio evaluable económicamente, consumado o en grado de tentativa, muchos autores han considerado que la existencia del delito de estafa, se debe a la tutela de la buena fe en los negocios jurídicos.

Se ha determinado que la naturaleza es la protección que el legislador dirige a las personas defraudadas patrimonialmente, tomando al patrimonio como una universalidad, cuya afectación es comprobable a través de la disminución del mismo en su sentido económico, que están conformados por todos aquellos derechos reales o personales, bienes muebles e inmuebles etc., diferenciándolo del hurto y el robo que conllevan un perjuicio patrimonial, donde se considera de manera aislada.

4.4 Elementos del delito de Estafa

Se trata de establecer los elementos que componen el delito de estafa convencional.

4.4.1. El Ardid o Engaño

El engaño es el elemento más importante y esencial de la estafa; es decir, la conducta engañosa que realiza el sujeto activo, es el componente

característico que permite diferenciarlo con otros tipos penales como el hurto, apropiación indebida, etc.

En términos comunes se entiende al ardid como los artificios o mañas, siendo el elemento primordial de la estafa, hacer creer algo que es falso; entendiendo por engaño, la falta de verdad en lo que se dice o hace, la simulación u ocultamiento de lo que realmente existe, por ello sería una falsa apreciación de la realidad.

Existen modalidades en que el engaño puede manifestarse aunque en la doctrina son muy discutidos: como lo son el engaño expreso y el engaño a través de actos concluyentes, el primero se refiere a la conducta que realiza el sujeto activo mediante una declaración de voluntad que la ejecuta de forma verbal o escrita, reuniendo todas las características propias del engaño que es la simulación de hechos que van dirigidos a provocar un error, también es conocido como engaño o misivo, y el segundo es aquella acción que está implícita la aceptación falsa de un hecho, por ejemplo: el ingresar a un restaurante y pedir el servicio de la comida, alojarse en un hotel, alquilar un coche, el abordar un transporte público constituyen acciones positivas; pero, para hacer uso de estos servicios se requiere solvencia económica, para el pago por la prestación de ellos.

El problema surge cuando por medio de ese acto, se hace creer que se posee esa posibilidad de pagar y realmente carece de ella; entonces allí existe un engaño, que induce al error del sujeto pasivo.[62]

En este sentido el ardid es la supresión de verdad en lo que se dice o hace

[62] José Manuel Valle Muñiz, El Delito de Estafa, (Barcelona: Bosch, 1992), p.177.

Con ánimo de lograr un objetivo pasando por perjudicar a otro, es toda astucia o maquinación que alguien emplea contra legítimos derechos, ya hablando u obrando con mentira o artificio, ya callando maliciosamente lo que se debía manifestar pero con un propósito que va más allá del simple silencio u omisión, del ardid debe, inexorablemente, producirse el error en el sujeto pasivo, es decir, concurre una relación de imputación necesaria entre ardid y error, por lo cual éste consiste en un estado psicológico provocado por el autor del delito mediante ardid y que inducirá a la víctima a la realización de una disposición patrimonial perjudicial, en lo anterior radica la conducta antisocial y con relevancia penal que califica un fraude en el sentido de Estafa.[63]

4.4.2. El Dolo

En cuanto al dolo, éste debe comprender la representación y voluntad de la realización del tipo penal objetivo, porque este elemento subjetivo se proyecta sobre la conducta engañosa, en el error del engañado, en la disposición patrimonial y en el perjuicio económico que es imprescindible para la obtención del lucro deseado. Así el agente es consciente y quiere engañar por medio de manifestaciones falsas, representándose el producto inevitable de su conducta, es decir, la inducción al desprendimiento patrimonial; esto implica, el dominio en la provocación del resultado en condiciones de imputación objetiva; ello significa que el ardid y su despliegue debe ser querido por el sujeto activo que lo realiza.[64]

Se concibe como la conciencia y voluntad del sujeto de realizar el hecho tipificado objetivamente en el supuesto de hecho, es decir el conocer y querer

[63] Sentencia del Recurso de Apelación, Referencia INC-74-14 (El Salvador, cámara tercera de lo penal de la primera sección del centro, San Salvador, Corte Suprema de Justicia, 2014).
[64] Ibíd.

realizar los elementos objetivos del tipo, de este concepto es donde se determinan los elementos del dolo vinculando al ilícito en estudio que son el elemento cognoscitivo y el volitivo.

4.4.3. Ánimo de Lucro

Sobre el ánimo de lucro, debe decirse, que determinados delitos dolosos no agotan el contenido del injusto personal con la presencia del dolo, pues junto a éste y de manera imprescindible para afirmar la tipicidad, como en la estafa, es necesario, por imperativo del principio de legalidad penal, establecer que el autor, no solo debe conocer y querer la realización de un perjuicio patrimonial ajeno mediante el despliegue de una conducta engañosa, sino que es preciso que todo ello lo acometa con ánimo de lucro, porque la finalidad del beneficio se configura como resultado que el agente debe tener presente en la realización típica, pues el ánimo de lucro es esencial en la Estafa para afirmar su tipicidad, y por tanto, su ausencia, conlleva a la atipicidad de la conducta.[65]

4.4.4. El Error

El error es entendido comúnmente como la apreciación equivocada de la realidad y en el delito de estafa es considerado doctrinariamente como un elemento esencial, se presenta dentro del mismo una doble función, en primer lugar nos indica la efectividad del engaño y hace que sea posible la disposición patrimonial por parte del sujeto pasivo y así la consumación del ilícito penal.

En el delito de Estafa, los actos de disposición son medios de disposición para

[65] Recurso de Apelación, CSJ, Ref. INC-74-14, (2014).n112.

el engaño las acciones y omisiones que impliquen un desplazamiento patrimonial, ya sea entregando, cediendo o prestando la cosa, sean estas fungibles, tal es el caso del dinero en efectivo; o no fungibles, así como, derechos o servicios; además, que la defraudación sea mayor de doscientos colones,[66] que hace la diferencia de este delito con otros naturales del patrimonio como el hurto o el robo en que no se emplea violencia.

Esta definición del acto de disposición hace posible incluir dentro del estudio jurídico, los casos en los cuales el acto es realizado por un servidor que no es el sujeto tenedor del bien jurídico, en otras palabras, que el error puede provocarse sobre el sujeto que realiza la disposición patrimonial o el desplazamiento patrimonial pero no es ella quien recibe un perjuicio sobre su patrimonio sino un tercero que es el caso conocido doctrinariamente como la estafa en triangulo.[67]

4.4.5. La Disposición Patrimonial

Requisito necesario es que el engaño que es capaz de producir un error en la víctima, genere en ésta por su propia voluntad una disposición patrimonial perjudicial, lo que caracteriza a la estafa precisamente como un delito de autolesión, este concepto marca un importante distingo respecto de otros delitos contra la propiedad, como el hurto o el robo, en que hay desplazamiento de la cosa desde la víctima al sujeto activo, pero a través de la clandestinidad en el actuar de este último, tratándose de la estafa, es la propia víctima quien voluntariamente realiza un acto de disposición, con el sujeto activo.

---

[66] Así lo establece el artículo 216 del Código Penal Salvadoreño.

[67] La Estafa en triángulo, es aquella en la que dentro de la relación de causalidad intervienen tres sujetos uno que es el agente activo o “estafador” que realiza la conducta engañosa; el segundo, el sujeto pasivo en el cual recae el error realizando la disposición patrimonial y el tercero, que interviene es la persona sobre la que recae el perjuicio o “perjudicado”.

4.4.6. El Nexo Causal

Un elemento muy importante dentro del tipo objetivo, lo constituye el nexo causal,[68] el cual implica la unión entre la acción y el resultado, puesto que el resultado debe haber sido producido causalmente por la acción del autor. Significa entonces, que a cualquier sujeto podrá imputársele un hecho ilícito, siempre y cuando medie una relación causal, verificable.

El denominado nexo causal, es necesario aclarar que siempre debe generarse bajo las circunstancias anteriormente descritas, para efecto de determinar si verdaderamente el resultado se adecua al comportamiento descrito en el Art. 215 del Código Penal; dicho proceso, para la determinación o individualización de las responsabilidades, usualmente se realizara bajo la perspectiva de la causalidad natural o causalidad adecuada, pero, cuando esta mera verificación no sea suficiente se utilizara la teoría de la imputación objetiva para la atribución del resultado, en cuanto, comprobada la causalidad natural, se requiere además verificar que la acción ha creado un peligro jurídicamente desaprobado para la producción del resultado; y que este sea la realización del mismo peligro creado por la acción, y en cualquier caso, que se trate de uno de los resultados que quiere evitar la norma penal. En consecuencia, el primer nivel de la imputación objetiva es la creación de un riesgo típicamente relevante.

El comportamiento ha de ser entonces, peligroso, esto es, crear un determinado grado de probabilidad, requiere incluir las circunstancias conocidas o reconocibles por un hombre prudente en el momento de la acción,

[68] El nexo causal entre el error y engaño, o sea la relación que debe de concurrir entre todos los elementos de la comisión del delito, desde la fase de la ideación en la mente del sujeto activo hasta la comisión del mismo.

mas todas las circunstancias conocidas o reconocibles por el autor en base a sus conocimientos excepcionales o al azar. En todos los casos además, el riesgo creado no debe ser un riesgo permitido que los incrementos de peligro para el bien jurídico que se deriven de acciones socialmente permitidas en el ámbito en que se produce la estafa, no deben considerarse anti - normativas, eso es, contrarias al fin de la norma y comprendidas, por consiguiente, en el del tipo.

4.4.7. El resultado

En el mundo exterior todo comportamiento humano genera efectos de tipo físico e incluso psíquico, es decir un resultado; y cuando la consecuencia coincide con ciertos elementos valorados negativamente por el codificador, dicho resultado se vuelve jurídicamente relevante.

Nexo causal o relación de causalidad entre el engaño provocado y el perjuicio experimentado, ofreciéndose éste como resultado del primero, lo que implica que el dolo del agente tiene que anteceder o ser concurrente en la dinámica defraudadora, no valorándose penalmente, en cuanto al tipo de estafa se refiere, el “dolo subsequens”, es decir, sobrevenido y no anterior a la celebración del negocio de que se trate; aquel dolo característico de la estafa supone la representación por el sujeto activo, consciente de su maquinación engañosa, de las consecuencias de su conducta, esto es, la inducción que alienta al desprendimiento patrimonial como correlato del error provocado y el consiguiente perjuicio suscitado en el patrimonio del sujeto víctima, secundado de la correspondiente voluntad realizadora. Por ello la determinación del resultado, es importante a efectos de poder realizar el análisis del tipo (juicio de desvalor de la acción) y comprobar de esa manera la compatibilidad de aquel con lo descrito en la norma.

El resultado requerido en la estafa, es el perjuicio patrimonial, significando ello que sin perjuicio no existe estafa perfecta o consumada.[69]

4.5 Sujetos del delito de Estafa

Se establece la clase de los sujetos que intervienen en el delito de estafa, se Hace mención del delito que realiza la acción, así como el sujeto a quien se le desmejora parte de su patrimonio, de igual forma se hacen algunas diferenciaciones entre cada uno de los sujetos que intervienen en este tipo de delito, ya que la intervención de los sujetos en este delito son distintos a los que intervienen en delito de estafa tradicional.

4.5.1 Sujeto Activo

Para que se ejecute una acción es necesario que una persona la realice y quien lleva a cabo la conducta tipificada en la ley es llamado: Agente, autor o sujeto activo Bajo esta perspectiva las prohibiciones jurídico - penales tiene funciones tanto de carácter general como especiales, van dirigidas a toda la población; en relación al ilícito de estafa regulada en el Art. 215 del Código Penal, establece “el que”… La conducta engañosa, puede ser ejecutada por cualquier persona natural; por ser este un delito común, significa que el agente no requiere de cualidades especiales, siempre que vaya dirigida a realizar la conducta engañosa, con la finalidad de obtener un provecho injusto para sí o para un tercero, tal y como lo es en el delito de estafa informática que requiere de algún tipo de conocimiento para la realización de la conducta delictiva.

[69] José Francisco Leyton Jiménez, *Los Elementos típicos del delito de estafa en la doctrina y jurisprudencia contemporáneas*, (Santiago: Ministerio Público de Chile, 1999), p.138.

4.5.2. Sujeto Pasivo

Como consecuencias de las acciones del sujeto activo recaen sobre otros, a quienes se denominan sujetos pasivos; siendo éste el titular del bien jurídico protegido en el caso concreto y que puede resultar o no perjudicado con la conducta del sujeto activo.[70] Partiendo de esta definición se analizaran diversos criterios, para que el error y la disposición patrimonial en que incurre el sujeto pasivo a causa de la conducta engañosa, sean típicas del delito de estafa. La víctima objeto del engaño puede ser cualquier persona, ya sea naturales o jurídicas.[71] Por ello se llega a la conclusión que el sujeto engañado son indeterminados; es decir, pueden ser una o varias personas, pero siempre y cuando haga uso de los medios informáticos, ya que con la utilización de estas herramientas el sujeto pasivo cuando utiliza medios informáticos se vuelve vulnerable ante la actitud delictiva del sujeto activo, que lo que busca es el poderse apropiar de los bienes del sujeto pasivo que se ve afectado.

4.6 Bien Jurídico protegido en el Delito de Estafa

No hay duda de que la estafa, como tal, debe estar entre los delitos contra la propiedad, ya que no se castiga el engaño, sino el daño patrimonial que ocasiona, aunque el medio utilizado pueda causar daño a otro bien jurídico, y éste ha sido el criterio de las legislaciones más conocidas en todas ellas el bien jurídico es la propiedad.

---

[70] Fernando Velásquez Velásquez, *Derecho Penal, Parte General*, (Bogotá: Temis, 1994), p.32.

[71] El Art. 52 del Código Civil establece que las personas son naturales o jurídicas, son personas naturales todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición. Son personas jurídicas las personas ficticias capaces de ejercer derechos y contraer obligaciones y ser representadas judicial o extrajudicialmente".

4.7 Agravantes del Delito de Estafa

Además de la modalidad simple ubicada en el Artículo 215 de la legislación penal vigente, también posee una forma agravada de comisión la cual se constituye bajo cualquiera de los supuestos siguientes:

a) Si recayere sobre artículos de primera necesidad, viviendas o terrenos destinados a la construcción de viviendas;
b) Cuando se colocare a la víctima o su familia en grave situación económica, o se realizare con abuso de las condiciones personales de la víctima o aprovechándose el autor de su credibilidad empresarial o profesional;
c) Cuando se realizare mediante cheque, medios cambiarios o con abuso de firma en blanco;
d) Cuando se obrare con el propósito de lograr para sí o para otro el cobro indebido de un seguro; y
e) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

Por lo que se puede decir entonces que dichos subtipos se encuentran dentro del Art. 216 Penal y constituyen un plus de la forma básica; es decir que, para determinar si existe o no un delito de Estafa Agravada, es necesario que concurran todos los elementos propios de la Estafa ente ellos el engaño, error, disposiciones patrimoniales y perjuicio patrimonial, así como deben presentarse de forma adicional cualquiera de las situaciones antes planteadas.

La conducta de la manipulación, en este caso no abarcan las maniobras físicas sobre aparatos automáticos (cabinas telefónicas, máquinas expendedoras), bien porque se manipule para obtener un objeto material, o una persona realice manipulaciones para que la máquina reciba el dinero y no expenda el

producto. En ambos casos no se comprende la agravación en comento, porque la primera supondría un apoderamiento y el segundo sí sería estafa, pero del tipo básico.

La manipulación tiene que ir dirigida a lograr interferir, en el sentido de alterar el resultado de un procesamiento o transmisión informática de datos, de tal modo que se atribuyan indebidamente ingresos, bienes o servicios; o se anulen incorrectamente débitos o gastos, equivaliendo dicha interferencia al acto de disposición y al perjuicio del comportamiento que se realizara.

En los tiempos actuales las nuevas tecnologías, en general, y la informática, en particular, introducen incansablemente no sólo nuevas formas de realizar tareas conocidas, sino también nuevas actividades, muchas de las cuales se manifiestan como antisociales y reprobables, en razón de interferir en la Pacífica convivencia de los ciudadanos.

Tal y como lo menciona el Doctor Gustavo Arocena[72] "la informática no sólo importa una técnica destinada a hacer lo mismo, aunque mejor y más rápido, por medio de la ayuda electrónica y del soporte magnético, por el contrario, ella supone también una fértil fuente de nuevos estados de cosas, que pueden colocar en jaque a los sistemas jurídicos, cuando los muestran impotentes para contemplar las nuevas realidades".

Por ello se puede hacer mención que la estafa informática es un fenómeno delictivo que en los últimos años está tomando mayor magnitud y relevancia en el ámbito de la criminalidad informática, siendo éste la base principal del

[72] Juez de Ejecución Penal, Ciudad de Córdoba, Profesor de Derecho Penal y Procesal Penal, Facultad de Derecho de la Universidad Nacional de Córdoba, Argentina. (UNC)

delito informático sobre el que gira la ciber - delincuencia, y que es te fenómeno ha ido tomando un mayor relevancia en todos los ámbitos de la vida cotidiana que desarrolla el ser humano, es así que el derecho ha tenido un nuevo desafío en cuanto a la tipificación de estas conductas en sus ordenamientos penales.

Entonces se puede decir que el Derecho penal como conjunto normativo, no deja de ser sino un instrumento de control social, que tiene como función primordial la de mantener y proteger un determinado sistema de convivencia, lo que conlleva que solo puede ser comprendido en y desde el sistema.[73]

Luego de haber hecho un breve análisis y plantear las ideas esenciales sobre la Estafa Tradicional regulada en el artículo 215 y 216 del Código Penal, a continuación se desarrollara lo referente a la Estafa Informática regulada en el artículo 10 de la Ley Especial contra los Delitos Informáticos y Conexos.

4.8. Antecedentes Históricos o evolución de la Estafa Informática

Como ya se ha hecho mención en los anteriores capítulos, se ha tratado de hacer el abordaje de manera general de los delitos informáticos y la evolución que han tenido en las distintas épocas del desarrollo humano. Pero es necesario que de forma particular se aborde la evolución del delito de estafa informática.

En la sociedad actual de la información la denominada “cibercriminalidad” se presenta en la cotidianeidad de las personas bajo las más variadas formas, expresivas de una amplia heterogeneidad de nuevos fenómenos delictivos y

[73] Francisco Muñoz Conde, Derecho Penal Parte General, 5ª ed. (Valencia: Tirant lo Blach, 2002), p.56.

renovadas modalidades de comisión de los delitos tradicionales, especialmente, a través de sistemas o redes informáticas de transmisión e intercambio de datos por Internet, cuya complejidad operativa dificulta su persecución y, consecuentemente, incrementa los niveles de impunidad.

Aunque en realidad, no exista una definición de "cirbercriminalidad" unánimemente aceptado, podríamos decir que se trata de un término que hace referencia a un conjunto de actividades ilícitas cometidas al amparo del uso y el abuso de las tecnologías de la información y la comunicación también llamados Tics, poniendo en peligro o lesionando intereses o bienes jurídicos de naturaleza individual, o bien, amenazando la seguridad de los sistemas sociales, dentro de este contexto, se destaca el particular interés que suscita en la actualidad la estafa cometida a través de Internet; la cual se trata de ataques a la integridad y confidencialidad de los datos personales, y también, al patrimonio del sujeto pasivo de este tipo de delito informático.

Con la evolución tecnológica los ataques al patrimonio se han desarrollado de formas que difícilmente podrían tener cabida en esa definición, por lo que la intervención del legislador ha tenido que ser reiterada para respetar los principios de seguridad jurídica y legalidad penal, es así que en el año de 1994, el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos destacó que el fraude por manipulación informática, la falsificación informática, los daños o modificaciones a datos o programas informáticos, el acceso no autorizado a sistemas y servicios informáticos, y la reproducción no autorizada de programas informáticos protegidos legalmente eran tipos comunes de delitos informáticos.[74]

[74] Naciones Unidas, Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos, 1994, p.23.

Aunque dichos actos a menudo eran considerados delitos locales que involucraban sistemas independientes o cerrados, la dimensión internacional del delito informático y la legislación penal correspondiente ya habían sido reconocidas desde 1979, en una presentación sobre fraude informático en el Tercer Simposio de la INTERPOL sobre Fraude Internacional, realizado del 11 al 13 de diciembre de 1979, se destacó que "la naturaleza del delito informático es internacional, debido al estable crecimiento de las comunicaciones por teléfono, satélite, etc., entre los distintos países." El concepto central del delito cibernético actual sigue siendo exactamente ese, la idea de que la tecnología de información y comunicación globalizada convergente puede ser utilizada para cometer actos delictivos con un alcance transnacional, tal y como sucede con el delito de estafa informática que ha avanzado a un ritmo vertiginoso, y de igual forma los sujetos activos de este tipo delito han elaborado un mejoramiento en el uso de las técnicas especializadas para la realización del fenómeno delictivo.

El papel de los factores socioeconómicos en el delito de la estafa informática no se limita únicamente a países industrializados, más bien se aplica por igual en el contexto de los países en vías de desarrollo, ya que en algunos países de África Occidental, por ejemplo, los estudios sobre las características sociodemográficas de los yahooboys[75] muestran que muchos son estudiantes universitarios que consideran el fraude en línea como un sostén económico.

El desempleo, en particular, es identificado como un factor crucial que acerca a los jóvenes a la actividad del yahooboyismo.

[75] La subcultura de los 'yahooboys' describe a jóvenes Nigerianos recién graduados de la Universidad, que hacen uso de las aplicaciones de yahoo, para relacionarse y que comenzaron sus actuaciones a partir del año 2000, usan Internet para actos de fraude informático y phishing.

Los estudios en otro país de África destacan de manera similar que los "Sakawa"[76] que están frecuentemente involucrados en fraudes de Internet justifican sus actividades como la única manera en que pueden sobrevivir a falta de empleo, es de esta forma cómo ha evolucionado el delito de estafa informática a lo largo de los años, de tal forma que se ha vuelto más dificultoso el poder establecer una alerta temprana para el sujeto pasivo de este delito, ya que, quien se encuentra realizando dicho acto delictivo, cada vez tiene mayor nivel de eficacia y mejor conociendo en la materia por la utilización de nuevos sistemas operativos que hacen que sea menos detectable, y el grado de complejidad en la utilización de software de avanzada, hacen caer al sujeto pasivo del delito en una mayor vulnerabilidad al momento de estar frente a este tan complicado delito de estafa informática.

Es en este apartado en que se han tratado de establecer algunos aspectos que han logrado construir algunos antecedentes de manera muy general, ya que como se ha determinado anteriormente en donde se hace el abordaje con mayor profundidad del proceso evolutivo de los delitos informáticos, entre ellos el de estafa informática, y para no ser monótono su desarrollo, se hace un planteamiento de forma suscinta, sentando las bases para la fácil comprensión del tipo penal en estudio.

Por lo que se hace el abordaje desde la definición y los elementos que lo diferencian, y así poder comprender y diferenciar lo relacionado a los delitos de estafa informática del delito de estafa tradicional que se desarrolla en el presente trabajo.

[76] Los Sakawa es una nueva versión de la estafa nigeriana, ahora estos jóvenes visitan sitios de citas en Internet donde crean perfiles falsos con fotos de hermosas mujeres que buscan pareja. Una vez que son contactados desarrollan una relación amorosa ficticia y ya teniendo la confianza de un hombre o en ocasiones una mujer, inventan una historia trágica en la cual necesitan dinero para poder salir del yugo donde se encuentran e ir al encuentro de su amor.

4.9. Definición del delito de Estafa Informática

La estafa informática o más concretamente la estafa por computación, Constituye una parte del computercrime, el cual "consistente en una defraudación por medios informáticos".

Esto se refiere a la utilización del sistema informático como medio para la transferencia patrimonial a favor del autor.[77] Entonces, se dice que un delito es una acción antijurídica realizada por un ser humano, tipificada, culpable y sancionada con una pena; entonces si la estafa informática es: "la apropiación ilícita de fondos o dineros ajenos", también es un delito que se realiza con la utilización de un ordenador o computador y quien lo realiza no es un delincuente común, sino que es una persona con un alto grado de conocimiento, tanto informático como jurídico que sabe cómo eludir la ley por la falta de tipificación de este delito. Dicho de otra forma "el delito informático es toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio, sin que necesariamente se beneficie directamente".[78]

La Doctora Gutiérrez Francés, señala que con el vocablo "fraude" y sus derivados, en lenguaje común, con frecuencia suele identificarse con la idea de engaño, aunque aclara que no es fraude cualquier engaño. Por otro lado para el tratadista ecuatoriano Jorge Zavala Baquerizo el fraude es "un modo de actuar dentro de la vida, una conducta que se manifiesta, unas veces mediante el engaño y, en otras mediante el abuso de confianza.[79]"

---

[77] José Antonio Choclan Montalvo, *Internet y Derecho Penal*, (Madrid: consejo general del poder judicial, 2000), p. 321-322.

[78] María Barrera Gloria. *Los delitos de estafa informática*: "según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana", (Quito: Universidad central del Ecuador, 2014), p. 33

[79] Jorge Zavala Baquerizo, *Delitos Contra la Propiedad*, Tomo 2, (Ecuador: Edina, 1998), p.38.

Por tanto se puede afirmar que, cuando se habla de estafa se está aludiendo al "modus operandi, a la dinámica intelectiva ideal, que caracteriza un determinado comportamiento, el cual implica la presencia dominante de un montaje o artimaña ideal que desencadena determinada modalidad de acción. Lo informático del fraude está en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera; o sea, el carácter informático del fraude alude al instrumento con cuyo auxilio se efectúa la defraudación. Para que se configure la defraudación informática esta debe tener las notas características y configuradoras de una defraudación, es decir que debe existir un perjuicio económico, irrogado mediante un comportamiento engañoso, astuto, artero, o sea un medio fraudulento que en este caso sería la propia manipulación informática.

Para los autores Magliona y López, esto es muy importante ya que "ayuda a Distinguir el fraude informático de otros hechos delictivos, que no obstante ser realizados por medios informáticos, no constituye defraudaciones, por ejemplo, atentados contra la intimidad cometidos por medio de manipulaciones informática.[80] Al respecto Marcelo Huerta y Claudio Líbano señalan que "la finalidad perseguida por el sujeto activo, es la que condiciona el tipo de delito que se produce,"[81] ya que para ellos las manipulaciones informáticas se aplican a todos los delitos informáticos.

Con estos elementos podemos mencionar entonces, que se puede comprender por estafa informática "la utilización de un medio informático, para el cometimiento del delito, mediante la manipulación fraudulenta; con la

[80] Magliona y López, *Delincuencia y Fraude Informático*, p. 40.n
[81] Marcelo Huerta Miranda y Claudio Líbano Manzur, *Los Delitos Informáticos*, (Chile: Edi. Jurídica Cono Sur, 1996), p. 41.

finalidad de causar un perjuicio económico, y que conlleva ánimo de lucro, para sí o un tercero."

En este sentido un delito es: un acto antijurídico realizado por un ser humano, Tipificado, culpable y sancionado con una pena; entonces si el fraude informático es la apropiación ilícita de fondos o dineros ajenos, tiene la particularidad de ser un delito que se realiza utilizando un ordenador o computador, y quien lo realiza no es un delincuente común, sino que es una persona con un alto grado de conocimiento informático que puede eludir la ley por la falta de tipificación de este delito.

4.10. Naturaleza jurídica del delito de Estafa Informática

Para un sector doctrinal el delito informático es únicamente una forma de realización de distintos tipos delictivos, en consecuencia el bien jurídico protegido en el delito informático será aquél protegido en el delito que presuntamente se ha realizado: patrimonio, Hacienda Pública, etc. otra concepción de la criminalidad informática le concede autonomía entendiendo que con el fraude informático se protege un bien jurídico con naturaleza propia: "la confianza en el funcionamiento de los sistemas informatizados", como interés de carácter supraindividual o colectivo; Se parte de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días, porque de ello depende que no se colapsen las actividades del mundo bancario, bursátil, de seguros, transportes, gestión tributaria, Seguridad Social, sanitario, etc.

Esta segunda posibilidad es la admitida en muchas legislaciones Estatales en Los Estados Unidos, que tipifican de forma autónoma, conductas de acceso

Ilegal a un sistema informático, su uso sin autorización y la manipulación ilícita y modificación de datos informatizados, siguiendo una construcción análoga a la de las falsedades. Según esta regulación, si como consecuencia de una de estas manipulaciones se obtiene una subvención ilícita o se comete un delito fiscal estaríamos frente a un concurso ideal o real de delitos, en el mismo sentido que en la actualidad se suscita entre falsedades y delito fiscal o entre delito fiscal y contable. Con estas previsiones se trata de adelantar las barreras de protección en atención a la especial peligrosidad que suponen estos nuevos instrumentos de comisión de delitos.

La determinación de los hechos que alcanzan relevancia penal entre los múltiples comportamientos irregulares que permiten las nuevas tecnologías es fundamental; es decir, se debe especificar la zona punible. Para ello es necesaria la selección de hechos que van surgiendo en el desarrollo de la vida moderna, vinculados con la informática, y que van a resultar relevantes para la adecuación de los tipos penales ya existentes a las nuevas situaciones relacionadas con el uso de los sistemas informáticos.

Un diverso problema lo constituye la individualización de la responsabilidad criminal en el ámbito de los hechos punibles cometidos en Internet. No resultará fácil la determinación de la responsabilidad de los diversos sujetos que aparecen en el contexto general de la red, sea como operadores o como usuarios. Para ello es necesario distinguir entre hechos propios y ajenos, y determinar también la posible responsabilidad de quienes, como intermediarios de servicios facilitan o impiden ilegalmente el acceso y transmisión de información a través de la red.

Por otra parte, las posibilidades técnicas de las nuevas tecnologías obligan a abandonar la concepción del Derecho penal como cuerpo legislativo vigente

para un determinado y exclusivo territorio, ya que se hacen patentes las limitaciones para la persecución de este tipo de hechos, derivadas de la aplicación puramente territorial de la ley penal.

De la problemática anterior se desprende la necesidad de armonizar y concertar legislaciones y mecanismos efectivos de cooperación internacional, a fin de evitar la fragmentación y aplicación territorial del derecho en una materia que se caracteriza por la transnacionalidad de sus efectos, atravesando fronteras como una de sus notas distintivas.

Al igual que en la estafa genérica, la estafa informática es un delito de resultado que requiere la existencia de perjuicio evaluable económicamente, consumado o en grado de tentativa.
Los bienes jurídicos que se lesionan por las conductas ilegales denominadas como estafa informática, es necesario que revisemos brevemente las doctrinas de los tratadistas del Derecho Penal para entender de forma amplia el concepto de bienes jurídicos.

En este sentido el tratadista Von Liszt respecto a los bienes jurídicos en general menciona que son: “intereses vitales, interés del individuo o de la comunidad. No es el ordenamiento jurídico lo que genera el interés, sino la vida; pero la protección jurídica eleva el interés vital a bien jurídico. Los intereses vitales deben ser indispensables para la convivencia comunitaria luego de lo cual y como consecuencia de ello serán protegidos normativamente bajo juicios de valor positivo.” [82]

[82] Franz Von Liszt, *Tratado de Derecho penal*, 20 ed., T.II, (Madrid: Reus, traducción de Luis Jiménez de Asúa, 1916), p. 6.

Los bienes jurídicos en el Derecho Penal son muy importantes puesto que determinan cuales son los intereses que la sociedad considera imprescindibles proteger, para esto el legislador a través de la norma penal otorga la protección jurídica a los bienes referidos, por medio de las normas que traerán la amenaza y la imposición de la pena para el sujeto activo que se atreva a dañarlos con su conducta delictual.

El bien jurídico puede presentarse como objeto de protección de la ley o como objeto de ataque contra el que se dirige el delito y no debe confundirse con el objeto de la acción que pertenece al mundo de lo sensible.

Siguiendo el ejemplo más común: en el hurto el objeto de la acción es la cosa sustraída; el objeto de la protección, la propiedad.

Una vez que sabemos que el bien jurídico a proteger no es otra cosa que "la Protección que se le da a los intereses de la comunidad", corresponde entonces revisar qué tipo de bienes jurídicos se lesionan por el desarrollo de las ciencias informáticas y las Nuevas Tecnologías.

Todo lo anterior parte del hecho de que el bien jurídico es aquel que se ve amenazado o se lesiona por la conducta delictiva del sujeto activo, constituyéndose en la razón de ser del delito. Es común que en el campo de los delitos informáticos, la atención de los bienes jurídicos, se haga desde la perspectiva de los delitos tradicionales, por lo que se reinterpretan los tipos penales que ya existen con la finalidad de aplicarlos o adaptarlos a los distintos tipos de delitos como por ejemplo la estafa informática.

Pero debido a la creciente influencia del enfoque de la sociedad de la información y el conocimiento, se ha visto necesario la introducción de valores

inmateriales, siendo la información uno de estos bienes intangibles a ser protegidos. La información y otros intangibles son bienes protegidos constitucionalmente, aunque su valoración económica es muy diferente a la de los bienes corporales.

En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macro social), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macro social vinculado al funcionamiento de los sistemas informáticos".

Se debe tomar en cuenta que para recabar en forma adecuada la evidencia que compruebe la comisión de los delitos informáticos y en especial el de la estafa informática, es necesario que se tenga bien claro cuál es el bien jurídico Que se tutela en este tipo de delitos, un aspecto importante a tener en cuenta es que dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una reinterpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos reinterpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Parte de la doctrina, ya se han pronunciado frente a los cambios necesarios en la realidad jurídica de los Estados que permiten tipificar los delitos informáticos teniendo en cuenta su naturaleza, que aunque no es nueva en el mundo, su comisión si es objeto de estudio de forma muy reciente en relación

a los delitos tradicionales, lo que conlleva a la creación y discusión de nuevas teorías jurídicas.

Una de las grandes dificultades en este aspecto la viven los países de tradición jurídica Romano Germánica, donde procedimentalmente no es viable la adecuación de la Ley al mismo ritmo que avanza, cambia y se desarrolla la tecnología fuente de la comisión de delitos informáticos.

El fenómeno de los delitos de alta tecnología y relacionados con las redes informáticas requiere la tipificación de delitos totalmente nuevos y la modificación de los tipos de delitos existentes para garantizar que se apliquen a la utilización abusiva de las nuevas tecnologías. “Es de remarcar el positivo avance que constituye contar con normas específicas que tipifiquen las acciones que, hasta su sanción, estaban exclusivamente bajo la interpretación de los jueces para cada caso particular que se les presentaba

En el ámbito Constitucional en nuestro país ampara en el artículo 2 el derecho, la protección, la conservación y defensa de la propiedad y posesión, así mismo como la intimidad personal desde este enfoque podemos mencionar que en ello lleva y crea un ámbito de privacidad del individuo.

Según sentencia emitida por la Sala de lo Constitucional con número de referencia 36 – 2004 se estableció que "si bien en el ordenamiento jurídico salvadoreño no aparece la figura del habeas data como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa, como manifestación del derecho a la intimidad, ello no significa que tal derecho quede totalmente desprotegido, pues partiendo de lo que establece el inc. 1º del art. 2 Constitución, que "toda persona tiene derecho a ser protegida en la conservación y defensa de los mismos" y asimismo el art. 247 de la misma

Carta Primaria, también en su primer inciso sostiene: "Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución"; se infiere que los derechos reconocidos expresa como implícitamente, deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio.

De manera que, aunque no se disponga de una ley que prescriba los presupuestos procesales para materializar tal figura, se puede decir que la protección del derecho en mención puede ser efectuada a través del proceso constitucional de amparo, no importando la naturaleza de la empresa o ente a Quien se le atribuya la vulneración de dicho derecho, en ese orden de ideas la Sala estableció, como conclusión se puede considerar que el proceso de amparo es un mecanismo suficiente para la tutela del derecho a la autodeterminación informativa, y por tanto no existe ningún elemento que evidencie que la aplicación de dicho proceso resulte inoperante en materia de protección de datos, y aunque no se encuentre regulado de manera textual la figura del habeas data como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa, como manifestación del derecho a la intimidad, ello no significa que tal derecho quede totalmente desprotegido, ya que existe una protección de forma explícita.

El fundamento de esta nueva institución denominada Habeas Data, en una clara analogía con el Habeas Corpus, no es otro que el de la intimidad o privacidad de estos datos que se pretenden conocer por ser relativos al requirente. Esta garantía constitucional no tiene otro fundamento que el considerar aquel espacio de protección incluyendo el espacio informático, aunque en su esfuerzo el legislador de la época de conformación de la carta

magna de 1983, no los considero como tal ya que fue después que han surgido según el avance tecnológico estas garantías proteccionistas de los datos de los ciudadanos, por ello podemos mencionar que este tipo de protección es un nuevo ámbito de la propiedad privada.

4.11 Elementos típicos del delito de Estafa Informática

Antes de entrar en el estudio de los elementos propios de este tipo de estafa, se deben sentar las bases de lo que conocemos como estafa tradicional o propia, que es aquélla en la que un sujeto, movido por el ánimo de lucro y mediante un engaño, induce a error a otra persona llevándola a realizar una disposición patrimonial que le causa un perjuicio propio o a un tercero.[83]

Ya sobre esta base podemos decir que "comete estafa informática quien, con ánimo de lucro, se valga de alguna manipulación informática para conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro", como se ve, dos son las notas que la diferencian de la estafa tradicional.

En primer lugar, la sustitución del engaño por el uso de una manipulación informática o artificio semejante se entiende así que el hecho de llevar a cabo esta conducta, que está orientada a producir engaño y, en segundo lugar, que ya no se exige que el tercero lleve a cabo una disposición patrimonial, sino que se produzca una transferencia no consentida de cualquier activo patrimonial, algo distinto y más acotado, establecido lo anterior se puede mencionar que, los elementos típicos que integran el delito de estafa informática son:

a) La manipulación informática y artificio semejante: El concepto de

[83]Muñoz, *Derecho penal*, p. 234n121.

manipulación informática puede definirse como la introducción, alteración, borrado o supresión indebida de datos informáticos, especialmente datos de identidad, y la interferencia ilegítima en el funcionamiento de un programa o sistemas informáticos, cuyo resultado sea la transferencia no consentida de un activo patrimonial en perjuicio de tercero.

Es por ello queda incluido en el término la introducción de datos falsos, la introducción indebida de datos reales, la manipulación de los datos contenidos en el sistema, así como las interferencias que afectan al propio sistema.

El concepto de manipulación informática corresponde con la conducta de alterar, modificar u ocultar datos que informáticos de manera que, se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener.

De esta forma un sujeto puede introducir instrucciones incorrectas en un programa de contabilidad de manera que no anote cargos a su cuenta corriente por ejemplo, o que desplace a su cuenta bancaria todos los ingresos efectuados un determinado día a las cuentas cuyos números terminen en determinado número, etc.;

b) transferencia patrimonial no consentida por el titular del mismo: La transferencia de un activo patrimonial consiste en el traspaso fáctico de un activo; esto es, una operación de transferencia de un elemento patrimonial valorable económicamente que pasa del patrimonio originario a otro, no teniendo necesariamente que producirse por medios electrónicos o telemáticos;

c) ánimo de lucro: El ánimo de lucro es elemento subjetivo del injusto que consiste en el propósito o intención del delincuente de conseguir un beneficio o ventaja económica, el ánimo de lucro ha de ser entendido como la intención de obtener un enriquecimiento patrimonial correlativo al perjuicio ocasionado, este ánimo de lucro constituye un elemento subjetivo del tipo, y su ausencia hace que la conducta realizada sea atípica, y por tanto impune.

Para que se dé la estafa ha de haber una transferencia no consentida de un activo patrimonial, en forma de entrega, cesión o prestación de la cosa, derecho a servicio;

d) perjuicio en tercero: El actor de la estafa informática deberá actuar en perjuicio de tercero, el cuál sufre un daño en su activo patrimonial, dando así lugar a la consumación del delito, Está referida al cambio de una partida económica de un lugar a otro, es decir, desplazamiento del dinero como puede ser de la cuenta bancaria de la víctima a la cuenta del autor del delito.

4.12 Sujetos del delito de Estafa Informática

Es en este apartado que se desarrolla los sujetos que intervienen en el delito de estafa informática, con el objetivo de poder establecer cuál podría ser la diferencia con los sujetos que intervienen en el delito de estafa convencional regulado en el Código penal.

4.12.1 Sujeto Activo

En general, el sujeto activo o agente de un delito, es la persona natural que lo perpetra. En el caso de la estafa informática, es la persona física que utiliza como herramienta dual, tanto a las computadoras como a los programas de

computación para manipular las distintas etapas de procesamiento y tratamiento informático desde el simple retiro o modificación del texto sobre información de los productos o servicios hasta la burla de los cortafuegos o firewalls,[84] debe perturbarse la uniforme combinación de alguno de estos elementos, la programación, las bases de datos, los distintos métodos de pago y las reglas de negocios.

Es por ello que se menciona que las personas que cometen delitos informáticos difieren de los delincuentes comunes, ya que requieren habilidades para el manejo de sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o son hábiles en el uso de sistemas informatizados. Los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico.

4.12.2 Sujeto Pasivo

El sujeto pasivo dentro del delito de estafa informática, es la víctima que se ve Afectado por la conducta realizada por el sujeto activo, es decir por el proceso de apropiación ilícita del bien apropiado por el sujeto activo. Si vemos este delito de forma más amplia podemos afirmar que para el caso de los delitos informáticos los sujetos pasivos bien pueden ser individuos, instituciones financieras y no financieras, gobiernos, etc., que utilizan sistemas automatizados, que generalmente están enlazados en una intranet, extranet o Internet.

[84] Un cortafuego o firewall es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Dicho lo anterior se puede mencionar que el sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo y en el caso de los “delitos informáticos” mediante él puede conocerse los distintos ilícitos que cometen los delincuentes informáticos, es imposible conocer la magnitud de los delitos informáticos ya que la mayoría no son descubiertos o no son denunciados por autoridades responsables, porque deja ver la vulnerabilidad de los distintos sistemas, lo que implica que por ejemplo en el caso de empresas un desprestigio, y en caso de entes gubernamentales pude generar una crisis en el país de que se trate. Esto lleva a que no se tenga una cifra exacta de damnificados o víctimas de este tipo de delito.

4.13 Bien jurídico Protegido

La cuestión relativa al bien jurídico protegido plantea uno de los problemas que más dudas suscitan en los delitos de daños en general, y en los delitos de daños informáticos en particular. El derecho penal, como conjunto normativo, no deja de ser sino un instrumento de control social, que tiene como función primordial la de mantener y proteger un determinado sistema de convivencia, lo que conlleva que solo pueda ser comprendido en y desde tal sistema.[85]

Inevitablemente este instrumento de control social no podía permanecer ajeno a los problemas de convivencia e interacción, que se venían suscitando como Consecuencia de la creciente y masiva utilización de los modernos sistemas informáticos en ámbitos sociales que tradicionalmente habían gozado de su tutela; siendo la creación del delito de estafa informática, precisamente, una muestra evidente de la preocupación del legislador penal por el mantenimiento

[85] Muñoz, *Derecho Penal parte General*, p.56nn121-134.

de las normas básicas de convivencia en este nuevo campo de interacción social[86] como lo es la era informática.

Parte de la doctrina establece que el delito de estafa informática, no Solo tiene Como misión proteger el patrimonio de un sujeto en particular, sino que también ha creado la protección de otro bien jurídico, que es de naturaleza supraindividual o colectiva, que viene a delimitar el interés social que se tiene en la seguridad del tráfico de activos representados por medios informáticos.

El daño que puede padecer una persona sobre un bien no solo radica en un deterioro sustancial como lo puede ser una lesión, sino también en su puesta en peligro y en la privación de la posibilidad de disponerlo. Ese tipo de afectación se encuentra íntimamente vinculada con la relación jurídicamente garantizada existente entre el bien y su titular, cuya esfera de libertad el derecho penal debe proteger, ya que señala el margen de maniobra que le es jurídicamente adjudicado al particular para la libre organización de su vida.[87] Sobre la base de ello, habría tres categorías de menoscabo al bien jurídico:

a) Lesión, que es el efectivo menoscabo a la integridad del bien;
b) Puesta en peligro concreto, donde, desde la perspectiva del bien, resulta probable una lesión que no se puede impedir de manera programada, lo que implica una grave desprotección de este, dicho de otro modo, existe una situación próxima a la lesión del bien jurídico;
c) Puesta en peligro abstracto, que es la merma de las condiciones de seguridad necesarias para el uso tranquilo del bien.

[86] Alfonzo Galán Muñoz. *El fraude y la estafa mediante sistemas informáticos*, (Valencia: Tirant lo Blanch, 2005), p. 183.
[87] Urs Kindhäuser, "Cuestiones fundamentales del derecho penal económico", Argentina, Derecho Penal y Procesal Penal, Universidad Astral, n. 5, (2012): p. 12.

Existe un menoscabo en los estándares típicos de seguridad, no pudiéndose disponer tranquilamente del bien[88]. Desde otra óptica, cuando existe una peligrosidad general para algún bien con la mera presencia de la acción del sujeto.

Dentro de esta última categoría, se puede hallar a los delitos de peligro abstracto puramente formales (vulnerados por la mera infracción a la prohibición y sin que el injusto penal incorpore restricción típica alguna) y los genuinos delitos de peligro abstracto, que son aquellos delitos de peligro real para los bienes jurídico con un contenido material de injusto que rebasa la mera ilicitud extrapenal.[89]

Incluso también parte de la doctrina agrega otra categoría entre los delitos de peligro abstracto o los delitos de peligro concreto, cuya utilización es cada vez más frecuente en el derecho penal económico, tratándose de los delitos de aptitud o de peligro potencial o peligro hipotético, la que incorpora elementos típicos normativos de aptitud, elementos de valoración sobre la potencialidad lesiva de la acción del agente, cuya concurrencia habrá de ser constatada por el juez.[90]

La importancia de la idea del peligro abstracto en el derecho penal económico radica en que está presente en la tipificación de aquellos delitos económicos en sentido estricto que tutelan bienes jurídicos inmateriales, institucionalizados o espiritualizados, porque afectan estructuras básicas del sistema económico

---

[88] Fabián Balcarce, Derecho Penal Parte especial, tomo I, *Delitos contra la propiedad consistentes en defraudaciones*: "Abusos de situación, Apoderamiento de inmuebles y daños", (Córdoba, Lerner, 2007), p.447.
[89] Ibíd.
[90]Carlos Martínez Buján Pérez. *Derecho Penal:* "Parte General", (Valencia: Tirant lo Blanch, 1998), p.111.

y como así también en aquellos delitos socioeconómicos de carácter supraindividual, sean institucionalizados o sean difusos, que se orientan a la protección de bienes individuales o suficientemente individualizables o determinables.[91]

4.13.1 Bienes Jurídicos Colectivos o Supraindividuales

Por un lado, los conflictos propios de la evolución social, el desarrollo cultural y tecnológico, las transformaciones materiales de las relaciones sociales en la sociedad moderna, no pueden ser abarcados por el Estado liberal,[92] y por otro, esa evolución ha propiciado el brote de condiciones con un cierto potencial para una realización efectiva de la libertad, de la igualdad y de la justicia sustanciales que solo un nuevo Estado de carácter social y democrático está en condiciones de llevar a cabo.

Es que el moderno derecho ha abandonado la protección exclusiva a bienes personales para abarcar una esfera aun mayor del ciudadano: se trata de bienes jurídicos colectivos y supraindividuales.

Esto es parte de lo que muchos han denominado el «expansionismo del derecho penal, es así como, en este marco, no solo se han criminalizado nuevas conductas, sino que también, en algunos casos, se produjo un adelantamiento punitivo a actos carentes de un principio de ejecución.

Se legitimó la prohibición de acciones bajo amenaza de pena ante la existencia

[91]Balcarce, Derecho Penal, p.133n.140

[92] José Luis Díez Ripollés, La contextualización del bien jurídico protegido en un derecho penal garantista: “En Teorías Actuales en el Derecho Penal”, (Buenos Aires, Ad Hoc, 1998), p. 452 - 453.

de un daño social concretado a través de una lesión o una puesta en peligro aquellos bienes jurídicos que exceden los intereses individuales.

La legitimidad de los bienes jurídicos colectivos deriva de la potencialidad de sus substratos para maximizar las posibilidades de uso y consumo de los bienes individuales, para la satisfacción de necesidades e intereses legítimos, y para la autorrealización personal, a todos por igual. Este potencial de los substratos colectivos los hace ciertamente funcionales para los bienes jurídicos individuales en la realidad social, en la medida en que prestan a estos utilidades con virtualidad de posibilitar el libre desarrollo personal y la satisfacción de necesidades e intereses legítimos y, por esto, tienen que ser pensados como antepuestos a los individuales, en el sentido de que los envuelven y complementan.[93]

Las estafas tradicionales son figuras pluriofensivas: protegen el patrimonio como bien jurídico preponderante y el discernimiento en concreto o intención, como manifestación de la voluntad de la persona, en el carácter de bien jurídico complementario. En algunos casos puede proteger otro bien jurídico complementario como es la administración pública.

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

[93] Luis Gracia Martín, Contribución al esclarecimiento de los fundamentos de legitimidad de la protección penal de bienes jurídicos colectivos por el Estado social y democrático de Derecho, Derecho Penal y Procesal Penal, Argentina, n. 3 (2012): p. 34.

Los bienes jurídicos protegidos en general son los siguientes:

a) El Patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da lugar;

b) La Reserva, la Intimidad y Confidencialidad de los Datos, en caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos;

c) La Seguridad y Fiabilidad del Tráfico Jurídico y Probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos;

d) El Derecho de Propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el denominado terrorismo informático.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan por que simultáneamente protegen varios intereses jurídicos, sin perjuicio de que tales están independientemente tutelados por otro tipo.[94]" En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

4.14 El Sabotaje

Con el avance de la tecnología, la informática se ha convertido en un instrumento que proporciona infinitas posibilidades de desarrollo y progreso.

[94] Echandía, *La Tipicidad*, p. 76n70.

Sin embargo, se ha dado lugar a una nueva forma de delincuencia, la delincuencia informática; ya que esta tecnología pone a disposición del delincuente un abanico de nuevas técnicas y métodos para alcanzar sus propósitos criminales."[95] Los autores chilenos Magliona y López, mencionan que el fraude informático es uno de los fenómenos más importantes dentro de la delincuencia informática, dado el creciente aumento de las manipulaciones fraudulentas, y es por tanto la zona más inexplorada y la que mayores problemas enfrente en cuanto a su prevención, detección y represión.

Con la incursión de la informática en el sistema financiero, se ha remplazado muchos de los documentos tradicionales en soporte papel en los que constan las operaciones y saldos de cada uno de los clientes, por anotaciones en cuenta, o registros lógicos realizados en los sistemas informáticos, sin un soporte en papel o con reflejos en papel meramente informativos o secundarios. De ahí que, la doctrina haya centrado el estudio del problema desde el enfoque de las manipulaciones de datos informativos.
Se ha sostenido que estas manipulaciones constituyen la forma más frecuente de comisión de delitos por medios informáticos: cuando se tuvo conocimiento de los primeros casos de fraude informático, estos fueron vinculados al delito de estafa.

Así se trató de encajar esta nueva figura dentro de los moldes estrechos de dicho tipo clásico, lo que a la postre supuso una dificultad para su encuadre, ya que los mismos elementos que configuraban a la estafa no lo permitían. Es así como nacieron en la doctrina extranjera las discusiones acerca de la imposibilidad de engañar a una máquina, o de la existencia de un error psicológico por parte de la computadora que lo lleva a la lesiva disposición.

[95]Magliona y López, *Delincuencia y Fraude Informático*, p.78n126.

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

Gutiérrez Francés, señala que el vocablo fraude y sus derivados, en lenguaje común, con frecuencia suelen identificarse con la idea de engaño, aunque percibe que no es fraude cualquier engaño. Por otro lado para el tratadista ecuatoriano Jorge Zavala Baquerizo el fraude es "un modo de actuar dentro de la vida, una conducta que se manifiesta, unas veces mediante el engaño y, en otras mediante el abuso de confianza"[96]

Por lo que se puede establecer que este se da 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.

Luego de mencionado lo anterior se establece que sabotaje informático, es aquel daño mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc), se realiza en contra de los datos protegidos de una persona o institución, pero que es interrumpido por aquel sujeto que con malicia destruye las barreras protectoras para atacar y poder causar daño en algunos sistemas.

[96] Zavala, *Delitos Contra la Propiedad*, p.202n125.

4.15. Elementos diferenciadores del delito de estafa convencional con el delito de Estafa Informática

Parte de la doctrina establece que la estafa cualquiera que sea su modalidad Persigue un fin, que es el desfavorecimiento del patrimonio del sujeto pasivo, sin embargo en la presente investigación bibliográfica se ha tratado de establecer los elementos que se diferencian entre las estafas convencional o tradicional con la estafa informática, en ese sentido tratamos de realizar algunos de esos elementos que únicamente se encuentran en una de las modalidades que en este caso es el de la estafa informática, los cuales se desarrollan a continuación.

4.15.1 La Manipulación

La manipulación informática o artificio semejante puede definirse como la acción consistente en alterar los elementos físicos que afectan los programas de la informática. Modalidades hay varias y ya citamos los más importantes supuestos. Hacerse pasar por un usuario autorizado para operar en su nombre obteniendo un beneficio, o la introducción de datos maliciosos para apropiarse de otros datos sensibles son casos típicos.

Por ello se establece que la manipulación informática o artificio semejante que procuran la transferencia inconsentida de activos en perjuicio de terceros admite diversas modalidades, como la creación de órdenes de pago o transferencias, o las manipulaciones de entrada o salida de datos, en virtud de las que la máquina actúa en su función mecánica propia solo que en el sentido patrimonial no deseado por inconsentido, generador del perjuicio en tercer.

El término manipular no puede aplicarse en estos casos atendiendo a la

definición dada por la Real Academia Española, el Diccionario define la acción de la siguiente manera; “Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares”. Dicha definición es incompleta para este estudio ya que es demasiado amplia, pudiendo emplearse para todo tipo de intervención, ya sea autorizada o no. Debemos precisar esta definición; profundizando en la primera descripción podríamos ampliarla, de este modo manipulación informática sería cualquier acción que suponga una intervención en el sistema informático; alterando, modificando u ocultando los datos que deban ser tratados automáticamente, o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial.

En cuanto a la manipulación, se puede decir que puede darse manipulación actuando sobre la introducción de datos, sobre su tratamiento o su salida, intervención sobre el software, etc. Pero la manipulación no exige un contacto directo con el ordenador que contiene los datos de interés, otro ejemplo más del modo en que avanza la tecnología y con ella la casuística son los casos en donde existen sistemas de tratamiento de datos que operan a distancia, pudiendo acceder a ellos a través de mecanismos como la red de telefonía, mediante un terminal que opera a distancia. Es algo evidente que hoy en día quien quiera perpetrar un fraude no necesita acceder físicamente al ordenador objeto de ataque, ya sea mediante internet o mediante otro tipo de redes. Las principales vías por las que el sujeto activo consigue un movimiento contable a su favor, que se la transfieran fondos o se le cancele una deuda son tres: 1. Introducción de datos falsos, 2. Manipulaciones en el programa, y 3. Manipulaciones en el sistema de salida de datos u output.

Manipulaciones en el programa: Se da en la fase de tratamiento, y aquí si

Encuentra ante una manipulación informática en todo el sentido de la palabra. Se modifican los protocolos del programa para que beneficie al autor. Las variantes y posibilidades son enormes; podemos englobar lo dicho en los apartados anteriores sobre el spyware. Casos como los troyanos son los más típicos, en donde un programa malicioso accede al sistema haciéndose pasar por un programa aparentemente inofensivo y seguro. Por citar otra técnica curiosa señalaría la llamada salami technique, mediante esta técnica se dan instrucciones para que el programa que lleva las cuentas de alguna entidad redondee los céntimos, de este modo el sujeto activo obtiene un gran beneficio con pequeñas estafas.[97]

Caso contrario en la estafa tradicional no es necesario que exista una manipulación del medio informático para que esta pueda consumarse ya que únicamente necesita el sujeto activo del delito hace que el sujeto pasivo le pueda entregar un bien patrimonial, por medio del engaño; es decir, haciendo creer la existencia de algo que en realidad no existe. Y es ahí que al momento del incumplimiento se perfecciona dicho delito.

4.15.2 Transferencia del Activo Patrimonial

Una vez que el afectado ha caído en el error se produce un acto de disposición patrimonial en beneficio del sujeto activo y en perjuicio de la víctima. Pero es la propia víctima quien lo realiza; esto es muy importante y lo que diferencia el delito de estafa de otros tipos penales. Si fuese el agente estaríamos ante otro delito como podría ser administración desleal. Por acto de disposición patrimonial podemos tomar la definición del Doctor Mata y Martín, en la

[97] María Luz Gutiérrez Francés. *Fraude Informático y Estafa*, (Madrid: Ministerio de Justicia, Centro de Publicaciones, 1991), p.5.

menciona que sería “en la entrega de una cosa (material o dineraria), en la realización de un acto documental con transcendencia económica (gravamen de un bien) o en la presentación de cualquier tipo de servicio, todo ello siempre cuantificable económicamente”. Lo fundamental es que sea cuantificable económicamente, para determinar si realmente podemos englobarlo dentro del delito de estafa.[98]

Es fundamental que sea el propio perjudicado quien realiza el acto de disposición patrimonial. En caso contrario podríamos estar ante supuestos de administración desleal. Este elemento es muy similar al delito de estafa tradicional o convencional ya que existe una desmejora en el patrimonio del sujeto pasivo, sin embargo en la estafa convencional únicamente dicha afectación es de carácter económico, y por lo general de dinero, en cuanto a afectación en el delito de estafa informática esta se da además de la parte propiamente económica puede afectar en la sustracción de datos, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, tal y como lo menciona el artículo 10 de la ley especial contra los delitos informáticos y conexos.

4.15.3 El Perjuicio

Los efectos del engaño y el acto de disposición patrimonial se traducen en un Perjuicio causado a una víctima, que puede ser el sujeto objeto del engaño o

[98] Ricardo Manuel Mata Y Martin, Algunas consideraciones sobre informática y Derecho penal: “El caso de la estafa informática, en Documentos Penales y Criminológicos”, vol. 1, (Madrid: Edisofer, 2001), p. 48.

Un tercero, por tanto el perjuicio puede ser propio o ajeno, lo fundamental es que el perjuicio debe ser cuantificable económicamente.

Para entender la existencia del perjuicio no podemos fijarnos únicamente en el balance negativo del patrimonio del afectado, sino que el perjuicio debe ser real, efectivo y evaluable económicamente; son las notas esenciales que se deben tener en cuenta, es de esa forma que se puede decir que el perjuicio en el delito de estafa no se contrae sólo a la determinación comparativa del patrimonio con anterioridad y posterioridad al hecho delictivo, sino que se hace preciso atender al acto dispositivo concretamente realizado y al aspecto patrimonial afectado en el hecho, de manera que el perjuicio debe ser real, efectivo y evaluable económicamente, esto es una disminución patrimonial lesiva al perjudicado.[99]

En el caso de la estafa informática además se da la afectación de siguientes bienes jurídicos: la información que garantice y proteja el ejercicio de derechos, fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros, por lo que se puede hacer notar que el perjuicio a diferencia de la estafa tradicional es más que lo económico. Tal y como lo menciona la ley especial contra los delitos informáticos y conexos en su artículo 3 literal “b”.

4.15.4 Calidad del Sujeto Activo

Como se ha mencionado en apartados anteriores, se he descrito el sujeto

[99] Javier Gustavo Fernández Teruelo, *Cibercrimen*: “Los delitos cometidos a través de Internet”, (Oviedo: Constitutio Criminalis Carolina, 2007), p. 44.

activo en materia de estafa informática, y se ha mencionado que el perfil de las personas que cometen delitos informáticos, especialmente el delitos de estafa informática, ya que si bien es cierto que por un lado se cree que los sujetos activos poseen habilidades diferenciadoras para el manejo de sistemas informáticos y generalmente su lugar de trabajo permite una posición estratégica de acceso a información sensible, por otro también se contempla la posibilidad de que no necesariamente estos sujetos activos posean una situación laboral en la cual puedan favorecer el cometimiento de este tipo de delitos, Según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, el noventa por ciento de los delitos que utilizaron una computadora, fueron cometidos por trabajadores de la propia organización afectada (Insiders). De la misma forma de acuerdo con su estudio realizado en América del Norte y Europa interiores y solo de veintitrés por ciento provinieron de actividades externas (Outsiders).

Así el sujeto activo de un delito informático tiene diferentes caras, y se Desplaza desde aquel que es un experto con las computadoras, hasta alguien que no labora en esta materia y tienen conocimientos básicos de informática. Esto se observa con los llamados “niños genios”,[100] tal es el caso de un niño ingles[101] personas como éstas logran que desarrollar su conocimiento en la informática y el ciber espacio de forma acelerada y finalmente por su propia cuenta son capaces de intervenir con éxito en operaciones de alto grado de dificultad técnica, entendiéndose por tal que es quien realiza toda o una parte de la acción descrita por el tipo penal fraude financiero informático.

[100] La ciencia considera un niño prodigio a un joven menor de 15 años que demuestra una habilidad propia de adultos, en una determinada disciplina.
[101] Como el caso del niño prodigio británico Aarón Bond, de 14 años, el cual fue expulsado del King Edward VI College por hacer realidad el sueño prohibido de muchos pre-adolescentes: 'hackear' el sistema informático de su escuela.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleador del sector financiero o de procesamiento de datos.

En cuanto a la conducta que realiza el sujeto activo del delito de estafa convencional el código penal en su artículo 215…dice “el que”, por tanto podemos determinar que el pronombre personal en tercera persona (el que), no determina una especialidad o conocimiento avanzada en una rama o materia en específico del sujeto activo, sino más bien deja muy amplia la posibilidad de que este sujeto pueda ser cualquier persona que con el afán de perjudicar a otra realice esta conducta delictiva, únicamente que se lleve a cabo cualquiera de los verbos rectores que establece como los son engañar, sorprender, únicamente basta en ganar la confianza del sujeto pasivo, para llevar a cabo el cometimiento del acto delictivo.

4.15.5 Calidad del Sujeto Pasivo

El sujeto pasivo dentro del fraude financiero informático, es la víctima que se ve afectado por la conducta realizada por el sujeto activo, es decir por el proceso de apropiación ilícita del dinero depositado en la entidad financiera. Si vemos este delito de forma más amplia podemos afirmar que para el caso de los delitos informáticos los sujetos pasivos bien pueden ser individuos, instituciones financieras y no financieras, gobiernos, etc., que utilizan sistemas automatizados, que generalmente están enlazados en una intranet, extranet o Internet. Como se puede observar la diferencia entre este sujeto pasivo con el del delito de estafa tradicional, es que necesariamente debe tener acceso al

uso del internet y de realizar a través del mismo actividades económicas como lo son las compras, transacciones, etc. Ya que en la estafa tradicional esta calidad no es necesaria porque puede ser sujeto pasivo de este delito en esta modalidad cualquier tipo de persona, sin que necesite realizar alguna actividad en específica en materia informática, únicamente debe de contar con patrimonio el cual le pueda ser desmejorado con la acción del sujeto activo.

CONCLUSION

Se puede concluir que la naturaleza virtual de los delitos informáticos dificulta la tipificación de las distintas conductas que se puedan ir desarrollando, ya que la tecnología está en continuo cambio y progreso. No tiene ningún sentido escribir leyes específicas para la tecnología. La estafa es Estafa, cualquiera sea el medio que se utilice para ejecutarlo. Las leyes deben independizarse de la tecnología, ya que ésta avanza demasiado rápido para que la legislación pueda hacer lo mismo. Por ello considero que la legislación relativa a delitos informáticos tal como se implementó en nuestro país, en base a las figuras existentes, es lo más acertado modificando sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible. En tal sentido cabe mencionar que para que la problemática jurídica de los sistemas informáticos no quede desfasada del contexto al cual debe aplicarse, debe considerarse a la tecnología de la información en su conjunto.

También es muy difícil la actividad probatoria en este sentido deben contarse con personas expertas a fin de poder reunirla, ya que se corre el riesgo concreto de perderla si no se sabe cómo manipular los distintos sistemas o equipos. Se debe tener en cuenta que en este tipo de situaciones el tiempo apremia y el agravante en este tipo de delitos es que el autor generalmente es un experto. La actividad informática tiene un gran potencial como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

El otro inconveniente que presenta este tipo de delitos es el tema de la Jurisdicción Territorial. La ONU señala que cuando el problema se eleva a la

escena internacional, se magnifican los inconvenientes y los delitos informáticos se constituyen en una forma de crimen transnacional. En este sentido habrá que recurrir a aquellos tratados internacionales de los que nuestro país es parte y que, en virtud del Artículo 144 de la Constitución de 1983, establece que los tratados internacionales celebrados por El Salvador con otros estados u organismos internacionales, tienen rango constitucional. La Organización de Naciones Unidas resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos;
b) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos;
c) No armonización entre las diferentes leyes procesales nacionales en la faz investigativa de los delitos informáticos;
d) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras;
e) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática. Por lo que se debe tener en cuenta que la persona que se siente afectada por estos delitos recurre a la autoridad más cercana, quien deberá iniciar la investigación disponiendo lo necesario para poder como ya expresáramos fijar la prueba. Por lo tanto

sería importante contar con un equipo profesional experto en estos temas, ligado directamente al poder judicial, de manera de poder facilitar el desarrollo del procedimiento investigativo, a cargo de la Fiscalía General de Republica, la cual por mandato constitucional en al artículo 193 de la ley máxima antes citada.

Sin embargo se están realizando algunos esfuerzos importantes para poder contrarrestar esta actividad delictiva, bajo la modalidad de la informática, tal es así que bajo el nombre de Ley Especial de Delitos Informáticos y Conexos, fue aprobada el pasado 4 de febrero del año 2016, esta normativa busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador.

Se puede decir entonces que estos esfuerzos son muy importantes ya que La Era Digital y la Sociedad de la Información han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio – económica, provocando una reestructura de los negocios e industria. La Informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la vida humana, desde los más importantes a los más triviales. Sin la informática las sociedades actuales colapsarían, pues es un instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual. Por lo que se puede decir que paralelamente al avance tecnológico, hay un avance más desarrollado en el delincuente, ya que este, tiene que tener un amplio conocimiento de estos avances tecnológicos, los cuales, no los ocupan en realizar el bien sino para delinquir; y que debido a la falta de una correcto conocimiento en los operadores de justicia como lo son los policías, fiscales, jueces así como todos aquellos que están involucrados en el que hacer en desarrollo de los procesos judiciales, y que son los encargados de que este

tipo actividades delincuenciales puedan ser ventilados en los tribunales y con ello se logre una protección a todas aquellas personas que hacen uso de las estas herramientas tecnológicas.

Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática. Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores. Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países como el nuestro que tiene una demanda muy grande en cuanto al uso de las redes sociales y con ello existe con mayor

posibilidad que el delincuente informático haga uso de estas para poder realizar el acto delictivo, ya que este uso de redes sociales conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Por ello se menciona que los grandes avances en las tecnologías informáticas, han permitido que así mimos la delincuencia tenga ese avance en los nuevos métodos del cometimiento de los delitos como lo son los delitos informáticos y en particular el delito de estafa informática.

BIBLIOGRAFIA

LIBROS

Abascal Gutiérrez, José Breve. Historia de la Informática: Madrid, 2006.

Barrera, Gloria María. Los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana. Universidad central del Ecuador, Quito, 2014.

Choclan Montalvo, José Antonio. El Delito de Estafa, Barcelona: Ed. Bosch, 2000.

Díez Ripollés, José Luis. La contextualización del bien jurídico protegido en un derecho penal garantista, en Teorías Actuales en el Derecho Penal, Buenos Aires: Ad Hoc, 1.a ed., 1998.

Fernández Teruelo, Javier Gustavo. Cibercrimen: "Los delitos cometidos a través de Internet", Oviedo, España: Edi. Constitutio Criminalis Carolina, 2007.

Galán Muñoz, Alfonzo. El fraude y la estafa mediante sistemas informáticos, Valencia: Ed. Tirant lo Blanch, 2005.

Garrido López, Carlos Alberto. Historia de la Computación, Universidad de San Carlos República de Guatemala.

Gracia Martín, Luís. Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia, Valencia: Ed. Tirant Lo Blanch, Alternativa, 2006.

Gutiérrez Francés, María Luz. Fraude Informático y Estafa, Ministerio de Justicia, Madrid: Centro de Publicaciones, 1991.

Islas Gutiérrez, Fernando Octavio. Internet: El medio inteligente, México: CECSA, 2000.

Leyton Jiménez, José Francisco. Los Elementos típicos del delito de estafa en la doctrina y jurisprudencia contemporáneas, Santiago, Chile: Ministerio Público.

Magliona Markovicth, Claudio Paúl y López Medel, Macarena, Delincuencia y Fraude Informático, Chile: Editorial Jurídica, 1999.

Muñoz Conde, Francisco. Derecho Penal Parte General, 5ª, Valencia: Edit.Tirant lo Blach, 2002.

Pekka, Himacen. La ética del hacker y el espíritu de la era de la información, Ed. Planeta, 2001.

Reyes Echandía, Alfonso**.** La Tipicidad, Universidad de Externado de Colombia, 1981.

Silva Sánchez, Jesús María. La expansión del Derecho penal: Aspectos de la Política criminal en las sociedades postindustriales." Montevideo: 2ª Ed. Editorial B de F. 2006.

Téllez Valdés, Julio. Derecho Informático, 3ª edición, México, Editorial McGraw Hill, Serie Jurídica.

Valle Muñiz, José Manuel. El Delito de Estafa, Barcelona: Ed. Bosch, 1992.

Valle Fonrouge, Marcelo. Introducción a la Informática Jurídica: El Derecho Informático y Otras disciplinas." LL, Argentina, 1979.

Velásquez Velásquez, Fernando. Derecho Penal, Parte General, Bogotá, Colombia: Ed. Temis, 1994.

Winer, Norbert Cibernética. Cibernética: El control y la Comunicación Barcelona, 1998.

Zavala Baquerizo, Jorge. Delitos Contra la Propiedad, Tomo 2, Ecuador: Editorial Edina, 1998.

TESIS

Garrido López, Carlos Alberto. “Historia de la Computación”, tesis de maestría en docencia universitaria, Universidad San Carlos de Guatemala, 2008.

FUENTES LEGISLATIVAS

Constitución de la República De El Salvador, 1983, decreto Constituyente N°38, fecha de emisión 15 de diciembre de 1983, publicado en el D.O. N° 234, Tomo N°281.

Código Civil de El Salvador, Nº: S/N Fecha: 23/08/1859, Decreto Ejecutivo de fecha 10 de abril de 1860, el día 1 de mayo del mismo año como fecha oficial para su publicación en cada uno de los pueblos, villas y ciudades de El Salvador, según consta en la Gaceta Oficial número 85, tomo 8, de fecha 14 de abril de 1860.

Ley especial contra los delitos informáticos y conexos, de El Salvador, decreto Legislativo Nº 260 de fecha de emisión 04 de febrero de 2016, publicado en el D.O. Nº 40, Tomo 410 de fecha 26 de febrero de 2016.

Código penal de El Salvador, decreto Legislativo Nº 1030 de fecha 26 de abril de 1997, publicado en el D.O. Nº 105, Tomo Nº 335 de fecha 10 de junio de 1997.

Ley especial contra actos de terrorismo, decreto Legislativo Nº 108 de fecha 21 de septiembre de 2006, publicado en el D.O. Nº 193, Tomo Nº 373 de fecha 17 de octubre de 2006

Ley especial para sancionar infracciones aduaneras, decreto Legislativo Nº 551 de fecha 20 de septiembre de 2001, publicado en el D.O. Nº 204, Tomo Nº 353 de fecha 29 de octubre de 2001.

FUENTES JURISPRUDENCIALES

Nacional

Sentencia de la cámara tercera de lo penal de la primera sección del centro, San Salvador, de fecha once de junio de dos mil catorce, Ref. INC-74-14.

REVISTAS

Escuela Judicial Consejo General del Poder Judicial, “internet y Derecho” 2001.

Londoño Sepúlveda, Néstor Raúl, El uso de las TIC en el proceso judicial: una propuesta de justicia en línea, Revista Facultad de Derecho y Ciencias Políticas, Volumen 40, N°112, Medellín, Colombia, 2010.

Gracia Martín, Luis, Contribución al esclarecimiento de los fundamentos de legitimidad de la protección penal de bienes jurídicos colectivos por el Estado social y democrático de Derecho, en Revista Argentina de Derecho Penal y Procesal Penal, N.° 3, junio de 2012

Kindhäuser, Urs. Cuestiones fundamentales del derecho penal económico, en Revista Argentina de Derecho Penal y Procesal Penal, Universidad Astral, N.° 5, octubre de 2012.

DICCIONARIOS

Cabanellas de Torres, Guillermo. 2006. Diccionario Jurídico Elemental, 18ª ed. Buenos Aires: Editorial Heleista.

FUENTES ELECTRÓNICAS

Jiménez Díaz, María José, 2014, Revista Electrónica de Ciencia Penal y Criminología, Universidad de Ganada,

www.Secretaria de Programación y Presupuesto, 2016, La Informática y el Derecho, INEGI, México.

Estrada Garavilla, Miguel, 2015, Delitos Informáticos, Universidad Abierta http://www.universidadabierta.edu.mx