UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURÍDICAS

“EL DELITO DE HURTO POR MEDIOS INFORMATICOS”

TRABAJO DE GRADO PARA OBTENER EL TITULO DE

LICENCIADO EN CIENCIAS JURIDICAS

PRESENTADO POR:

AGUIRRE DURÁN, GINO ROMANO

VELÁSQUEZ CORPEÑO, ALEJANDRA YAMILETH

VIGIL MENA, CELIA ELIZABETH

DOCENTE ASESOR:

LICENCIADO LUIS ANTONIO VILLEDA FIGUEROA.

CIUDAD UNIVERSITARIA, SAN SALVADOR, FEBRERO 2020

TRIBUNAL CALIFICADOR

DR. ARMANDO ANTONIO SERRANO.

PRESIDENTE

LICDA. LILI VERÓNICA GARCÍA ERAZO.

SECRETARIO

LIC. LUIS ANTONIO VILLEDA FIGUEROA.

VOCAL

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias Alvarado.
RECTOR

Dr. Manuel de Jesús Joya Abrego.
VICE-RECTOR ACADÉMICO

Ing. Agr. Nelson Bernabé Granados Alvarado.
VICE-RECTOR ADMINISTRATIVO

Lic. Cristóbal Hernán Ríos Benítez.
SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín.
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dr. Evelyn Beatriz Farfán Mata.
DECANA

Dr. Edgardo Herrera Medrano Pacheco.
VICE-DECANO

Msc. Digna Reina Contreras De Cornejo.
SECRETARIA

Msj. Hugo Dagoberto Pineda Argueta.
DIRECTOR DE LA ESCUELA DE CIENCIAS JURIDICAS

Msc. Diana del Carmen Merino de Sorto.
DIRECTORA DE PROCESO DE GRADUACIÓN

Msc. María Magdalena Morales.
COORDINADORA DE PROCESO DE GRADUACION DE LA ESCUELA DE CIENCIAS JURIDICAS

AGRADECIMIENTOS

A DIOS NUESTRO CREADOR, por darme la dicha de vivir y contar con salud, y por haberme guiado y proporcionado la sabiduría y fuerzas necesarias para alcanzar este logro, por permitirme estar rodeado de buenas personas que me motivan a ser mejor persona cada día. Sin ti no lo hubiese logrado y siempre te estaré infinitamente agradecido.

A MI MADRE, por tu Amor incondicional, por hacer de mi un hombre de bien, pues a pesar de todo, tus enseñanzas prevalecieron y son las que me hicieron llegar hasta aquí, por estar en las malas y en las peores pese a la distancia, por creer en mí y nunca abandonarme. Te Amo, te agradeceré el resto de mi vida.

A VERO, al amor de mi vida, mi mejor amiga, mi cómplice, por hacerme feliz y amarme como lo haces, por inspirarme y motivarme cada día, por aguantarme, pero sobre todo por apoyarme en todo momento y creer en mí; asimismo, te agradezco porque desde ya eres una excelente madre, ustedes son el motor que me impulsa cada amanecer, los amo inmensamente.

A MIS ABUELOS, por criarme con gran amor, por enseñarme tantas cosas que nunca olvidaré, fueron un gran ejemplo para mí, siempre me hicieron sentir especial y creyeron en mí, ustedes fueron parte fundamental en mi formación, siempre los recuerdo con mucho amor, les mando un abrazo hasta el cielo.

Al licenciado Luis Antonio Villeda Figueroa, porque fue de esos docentes que me ayudaron a tomarle el sentido y la pasión por la carrera, con su manera excepcional de impartir sus cátedras, y ahora como asesor logró hacer que me comprometiera y esforzara más cada semana y así sacar lo mejor de mí.

Gino Romano Aguirre Duran. –

AGRADECIMIENTOS

La presente tesis se la dedico en agradecimiento, en primer lugar, a Dios por permitirme llegar hasta este momento brindándome la sabiduría, paciencia y fuerzas necesaria para poder concluir mi carrera, ya que todo este caminar no hubiese sido igual sin el a mi lado.

A mis papas por apoyarme en todo momento de forma incondicional durante todos los años de mi vida y estudio, por procurar siempre mi bienestar, por sus esfuerzos y sacrificios ya que sin estos no hubiese sido posible concluir mis estudios universitarios, por su dedicación, comprensión y paciencia para tratar de hacer de mí una mujer de bien con valores y principios, por ser esos ejemplos a seguir y pilares fundamentales en mi vida, por siempre brindarme ánimos para seguir adelante sin importar las adversidades que se presenten en el camino. A mis abuelitos por orar y cuidar siempre de mí, sobre todo a mi abuelita Lupita que está en el cielo, porque este logro es de ambas.

A mi hermana, por todo su amor y apoyo a cada momento, por siempre creer en mí, sobre todo por animarme a seguir adelante para alcanzar mis metas, por enseñarme que todo se aprende y que todo esfuerzo es al final recompensado.

Al Licenciado Villeda, quien fue nuestro asesor de tesis y guía para la elaboración de la misma durante todo este proceso, por su tiempo, dedicación, accesibilidad y conocimientos brindados.

Alejandra Yamileth Velásquez Corpeño. -

AGRADECIMIENTOS

Este trabajo de grado es dedicado en agradecimiento a:

A mi Dios todo Poderoso, que atreves de su misericordia y bondad me ha permitido llegar hasta esta etapa de mi vida, permitiéndome formarme como persona y como futura profesional, enseñándome durante 25 años que el éxito y la prosperidad solo la puedo encontrar permaneciendo siempre en sus caminos. Gracias Jesús

Manuel Enrique Vigil Rodríguez, quien fue mi padre durante 23 años y mi mentor durante 5 años universitarios, quien me alentaba a ser diferente y sobresalir para enorgullecer a mi DIOS, quien me enseño que todo lo que haga en la vida sea siempre para glorificar a mi señor JESUS, atreves de la Humildad, Honestidad y Aplicación de los valores morales y principios básicos de una vida cristiana los cuales me fueron inculcados en casa. ¡Por todo esto y más… Gracias papa!

A mi hermosa madre Dinora Elizabeth Mena, quien fue, es y será siempre mi confidente en cada paso que di, que estoy dando y que en un futuro daré, quien ha sido mi apoyo incondicional en cada etapa de mi vida, gracias por tus sacrificios y amor incondicional, por creer siempre en mí. Por todo esto y mucho más… GRACIAS MAMA

A mi novio Harold Jean Carlos Guevara, quien ha sabido apoyarme en estos 5 años universitarios, quien me ha alentado a no rendirme y siempre dar lo mejor de mí, a pesar de cada circunstancia negativa, por haber sido también un apoyo económico en mis primeros años de mi carrera, por su paciencia y amor …. Gracias amor mío.

Celia Elizabeth Vigil Mena. -

INDICE **Pág.**

RESUMEN

Es innegable que las tecnologías de la información y la comunicación han adquirido relevancia, a través del desarrollo y modernización de los sistemas computarizados de gestión, almacenamiento y transmisión de información, permitiendo su masiva difusión e innovación, sin embargo, no se puede perder de vista el riesgo del cometimiento de nuevas modalidades delictivas, como lo es el delito de hurto por medios Informáticos.

Al ver ambas caras de esta nueva realidad, se advierte que, pese a los beneficios de la tecnología en la actualidad, su inserción en el marco jurídico regulatorio no ha sido lo suficientemente veloz, generando vacíos legales, que colocan dichas actividades en un entorno de inseguridad jurídica. La complejidad de los medios empleados para la comisión del delito de hurto por medios informáticos, dificulta la obtención y producción de la prueba, afectando con ello la apreciación de los hechos y circunstancias que son objeto del proceso por parte del Juzgador, disminuyendo con ello la posibilidad de una sentencia de carácter condenatoria.

El presente estudio recae sobre el delito de Hurto por medios Informáticos y la labor probatoria pericial, su obtención, las medidas de seguridad que se requieren y su valoración en el proceso penal, considerando necesario establecer la naturaleza jurídica y científica de la labor pericial en el ámbito de conocimiento e intervención del perito informático forense dentro del proceso penal; esto complementado con el desarrollo tecnológico investigativo, pues para hacer frente a esta realidad se necesita apoyo de personal técnico informático capacitado, el cual debe estar dotado de nuevos y modernos medios probatorios, sustentados en soportes técnicos.

LISTA DE SIGLAS Y ABREVIATURAS

ABREVIATURAS

Cn. Constitución de la República

CP. Código Penal

CPP. Código Procesal Penal

Art. / Arts. Artículo / Artículos

Inc. Inciso

Lit. Literal

Ord. Ordinal

Núm. Numeral

Etc. Etcétera

SIGLAS

TIC Tecnologías de la Información y Comunicación

WWW World Wide Web (Red Informática Mundial)

CSJ Corte Suprema de Justicia

FGR Fiscalía General de la República

CCD. Convenio contra la Ciberdelincuencia

LECDIC. Ley Especial contra Delitos Informáticos y Conexos

INTRODUCCION

La Ley Especial Contra Delitos Informáticos y Conexos como legislación aplicable a la investigación del Delito de Hurto por Medios Informáticos, manifiesta la falta de regulación expresa en la investigación de este tipo de delitos, dando paso a la búsqueda de una solución alterna, por lo que se pretende brindar un panorama más amplio sobre la necesidad que existe en El Salvador de crear una normativa penal vigente que regule la forma de proceder ante un delito de este tipo, pues en la actualidad, unicamente se cuenta con el tipo penal, pero no se cuenta con una parte procedimental ni probatoria, lo cual representa un obstáculo para la investigación de los mismos, debido al constante progreso tecnológico que estos presentan y la evolución en las formas de delinquir, dando lugar a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos, razón por la que, la presente investigación gira en torno a este tipo de delitos.

En El Salvador se cuenta con la Ley Especial Contra Delitos Informáticos y Conexos, pero esta Ley, no es suficiente para dar tratamiento a estas conductas delictivas, es por ello que la presentación de los temas a desarrollar requieren el análisis de diferentes aspectos, que permitan el cumplimiento de los objetivos que han sido trazados, mediante la utilización de las siguientes metodologías: Exploratoria, nos permitirá explorar más acerca del delito de Hurto por medios Informáticos, por ser un tema poco investigado e innovador; Explicativa, para determinar el origen de los delitos informáticos y la importancia de una regulación especial para los mismos, así como establecer el medio de prueba pertinente para demostrarlos; Pura o Básica, permite acrecentar los conocimientos teóricos, enfocados en establecer la naturaleza científica y jurídica de la labor pericial, en el ámbito del conocimiento e intervención del perito informático forense dentro del proceso penal; Además

se utilizara la metodología Bibliográfica-Documental que permite recolectar, seleccionar y analizar información que sirve de sustento a la investigación; asimismo, será una investigación Empírica o de Campo, ya que proporcionará datos y conocimientos de primera mano, a través de entrevistas a actores claves en materia de delitos informáticos; y por último, la Hermenéutica, que permite interpretar aquellos textos poco claros para efectuar una adecuada interpretación de las normas jurídicas, para que los profesionales o estudiantes interesados den lectura y puedan establecer un juicio sobre la problemática que en general se tiene al encontrarse en presencia de un delito informático.

El contenido del capítulo uno se expone a partir de las consideraciones previas que relatan la evolución histórica de la Informática e internet, la aparición de los delitos informáticos y del delito de hurto por medios informáticos a nivel internacional y en El Salvador para determinar su evolución tecnológica.

El capítulo dos consiste en las bases doctrinarias de los delitos informáticos y el delito de hurto por medios informáticos, desarrollando el significado o definición de los mismos, sus características principales, los sujetos procesales, el bien jurídico protegido por cada uno de ellos, los tipos de delitos informáticos de acuerdo a la conducta realizada por el sujeto activo, sea una conducta lesiva a la confidencialidad de los datos, una conducta lesiva a la integridad de los datos o una conducta lesiva a la disponibilidad de los mismos.

El capítulo tres esta denominado como: “La legislación nacional e internacional relacionada con el delito de hurto por medios informáticos”, el cual es un pre-ambulo para desembocar en lo que es el centro de nuestra investigación; el delito de hurto por medios informáticos, en la legislación actual no representa un avance significativo para dar cumplimiento a la investigación de los mismos, ni el procedimiento a seguir al estar frente a un delito de este tipo, lo cual representa un desafío en El Salvador para dar tratamiento a los mismos, es

importante determinar la necesidad de la suscripción a tratados y convenios que permitan reforzar la normativa penal vigente.

El cuarto capítulo consiste en el régimen probatorio pericial, el cual es la parte medular de nuestra investigación puesto que es de interés identificar el medio de prueba pertinente para demostrar el delito de hurto por medios informáticos como conducta punible, ya que es indispensable que las partes se valgan de los medios de prueba pertinentes para la investigación de este delito.

CAPITULO I

EVOLUCION HISTORICA DE LA INFORMATICA, DELITOS INFORMATICOS Y EL DELITO DE HURTO

El presente capitulo tiene como propósito establecer el desarrollo histórico de la informática y los delitos informáticos de forma general para lograr con ello determinar los avances que se han venido dando con el pasar de los años; a su vez se desarrollara la evolución histórica del delito de hurto a nivel internacional en las diferentes épocas hasta la actualidad en donde además se tocara la evolución que dicho delito ha tenido en El Salvador, haciendo un breve análisis de los diversos códigos penales que han surgido hasta la actualidad y por último el avance tecnológico del delito de hurto para estudiarlo desde el punto de vista informático.

1. Evolución Histórica de la Informática e Internet

Uno de los primeros dispositivos mecánicos para contar fue el ábaco, cuya historia se remonta a la antigua civilización griega y romana, este dispositivo representa y almacena los datos, sin embargo, es importante establecer que a este dispositivo no se le puede denominar aun como computadora porque carece del elemento fundamental llamado programa[1].

La primera computadora fue la máquina analítica creada por Charles Babbage, profesor matemático de la Universidad de Cambridge en el siglo XIX[2], la idea que tuvo sobre un computador nació debido a que la elaboración de las tablas matemáticas era un proceso tedioso y propenso a errores, por eso en 1823 el gobierno Británico lo apoyo para crear el proyecto de una máquina de

[1] José Alberto Jaén, Raquel Martínez y Ángel García Beltrán. División de Informática: Breve Historia de la Informática Industrial (Madrid: Universidad Politécnica, 2006), p. 22
[2] Philips Bretón, Historia y Crítica de la Informática, (Madrid: Cátedra, 1989), p.35.

diferencias, que era un dispositivo mecánico para efectuar sumas repetidas, por su parte Charles Jacquard, que era un fabricante de tejidos francés, creo un telar que podía reproducir automáticamente patrones de tejidos leyendo la información codificada en patrones de agujeros perforados en tarjetas de papel rígido, al enterarse de este método Babbage abandonó la máquina de diferencias y se dedicó al proyecto de la máquina analítica, para que se pudiera programar con tarjetas perforadas y así efectuar cualquier cálculo con una precisión de 20 dígitos aunque la tecnología de la época no bastaba para hacer realidad sus ideas.

En 1944 en la Universidad de Harvard, se construyó la Mark I, diseñada por un equipo encabezado por Howard Aiken, aunque esta máquina no está considerada como computadora electrónica debido a que no era de propósito general y su funcionamiento estaba basado en dispositivos electromecánicos llamados relevadores, posteriormente en 1947 se construyó en la Universidad de Pennsylvania la ENIAC (Electronic Numerical Integrator And Calculator) que fue la primera computadora electrónica, luego se creó la EDVAC (Electronic Discret Variable Automatic Computer), la idea fundamental de Von Neumann en esto fue permitir que en la memoria coexistan datos con instrucciones, para que entonces la computadora pueda ser programada en un lenguaje, y no por medio de alambres que eléctricamente interconectaban varias secciones de control.

Durante toda esta época había un gran desconocimiento de las capacidades de las computadoras, ya que se realizó un estudio que determinó que con veinte computadoras se saturaría el mercado de los Estados Unidos en el campo de procesamiento de datos, toda esta época abarco los años cincuenta, conociéndosele como la primera generación, cuyas máquinas estaban construidas por medio de tubos de vacío, eran programadas en

lenguaje de máquina, eran grandes y costosas, sus unidades de entrada utilizaban tarjetas perforadas, retomadas por Herman Hollerith quien además fundó la compañía llamada IBM (International Bussines Machines).

Cerca de la década de 1960, las computadoras seguían evolucionando, se reducía su tamaño, crecía su capacidad de procesamiento y también en esta época se empezó a definir la forma de comunicarse por medio de las ellas, que recibía el nombre de programación de sistemas, estaban construidas con circuitos de transistores, se programaban en nuevos lenguajes llamados lenguajes de alto nivel, algunas de estas se programaban con cintas perforadas y otras más por medio de cableado en un tablero, los programas eran hechos a la medida por un equipo de expertos analistas, diseñadores, programadores y operadores, para resolver los problemas y cálculos solicitados por la administración, el usuario de la información no tenía contacto directo con las computadoras, pues se requería saberlas "programar" para obtener resultados, aparecen también los programas procesadores de palabras como el célebre Word Star, la impresionante hoja de cálculo Visicalc y otros más, el software empieza a tratar de alcanzar el paso del hardware, pero aquí aparece un nuevo elemento: el usuario.

Durante esta misma época al terminar la II Guerra Mundial, las dos superpotencias, Estados Unidos y la Unión soviética, dejaron de ser aliadas y se enzarzaron en la llamada guerra fría, ambos ejércitos tenían claro que si se producía una escalada bélica entre ellos, el inicio del ataque vendría marcado por un masivo lanzamientos de misiles, por lo que era necesario detectar esos misiles al nada más ser lanzados y preparar el contra ataque que permitiese destruirlos en pleno vuelo en cuestión de minutos, siendo, la única forma fiable de intentar detener el ataque con misiles, el dejar que los ordenadores actuasen y, para ello, debían estar interconectados, comunicándose entre sí,

por eso en 1964 la RAND corporation propuso una red que no disponía de una autoridad central, sugiriendo así un diseño que desde el principio estaba preparado para trabajar de forma fragmentada, ya que todos sus nodos deberían tener un status parecido pero a la vez tener autonomía y poder suficiente para generar, transmitir y recibir mensajes que a su vez pudieran ser enviados por separado, a finales de 1966, Roberts Lawrence, se trasladó a la Agencia de Proyectos de Investigación Avanzada (ARPA), para desarrollar el concepto de red de ordenadores, confeccionando así el plan para ARPANET, la velocidad propuesta para ser usada en el diseño de esta fue aumentando desde 2,4 Kbps hasta 50 Kbps, considerándosele la primera red sin nodos centrales que se convirtió en Internet y se basó en la idea de que habría múltiples redes independientes con un diseño bastante arbitrario, siendo esta, la red pionera.

Con los progresos de la electrónica y los avances de comunicación que se producían por medio de las computadoras, a finales de esta década, surge la tercera generación de computadoras, cuya fabricación electrónica estaba basada en circuitos integrados y su manejo era por medio de los lenguajes de control de los sistemas operativos.

En 1970, Vition Cerf escribe por primera vez la palabra internet, en 1971 ARPANET, había crecido hasta 15 nodos con 23 ordenadores centrales, un año después, es decir en 1972 se diseñó el primer programa creado específicamente para el email, remitiéndose así el primer correo electrónico, usándose como símbolo la @, que se utilizaría para separar el nombre del usuario con el de la máquina , a mediados de esta década, para ser más exactos en 1976, aparecen en el mercado las computadoras de tamaño micro, que fueron inventadas por Steve Jobs, que no son tan costosas como las grandes, pero disponen de gran capacidad de procesamiento, siendo un gran adelanto de la microelectrónica, más tarde Steve Jobs forma la compañía

conocida como Apple que fue la segunda compañía más grande del mundo, antecedida tan solo por IBM.

En 1981 se vendieron 80,000 computadoras personales, al siguiente año subió a 14 millones, entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no queda duda que su impacto y penetración han sido enormes, de igual forma con el surgimiento de las computadoras personales el software y los sistemas que con ellas se manejan, han tenido un considerable avance, porque han hecho más interactiva la comunicación con el usuario, lo que hizo que surgieran otras aplicaciones como los procesadores de palabra, las hojas electrónicas de cálculo, paquetes gráficos, entre otros, haciendo a su vez que las industrias del Software de las computadoras personales crecieran con gran rapidez.

Con la extensión de los navegadores personales, en 1991, se puso en marcha el primer navegador de la web, que posteriormente en 1993 le dio paso al primer visualizador grafico de páginas web, denominado www Mosaic, el cual se desarrolló en el national center for super computing.

En el año de 1995 habían más de cinco millones de servidores conectados a internet, ya para el año 2000 internet estaba formado, no solamente por restos del ARPANET original, sino también incluye redes como AARNET (Academia Australiana de Investigación de redes), la NASA Science Internet (NSI), la red académica de investigación suiza (SWITCH), entre otras.

A lo largo de la Historia de la Informática se han creado grandes cosas, que al pasar de los años se han ido modificando y estudiado para su perfeccionamiento y a través de eso se ha dado lo que es su evolución progresiva, los servidores de Internet hasta el día de ahora han crecido exponencialmente, ya que la cantidad de computadoras conectadas a Internet

durante estas décadas han ido aumentando de una forma dramática, hasta los comienzos de la red.

En la actualidad, Internet conecta millones de computadoras directamente, y millones más tienen acceso a Internet a través de esquemas de direcciones privadas, tanto la Historia de la Informática y el internet durante su evolución se han convertido en un fenómeno global que a través del tiempo se ha hecho más viral, las personas han pasado a depender de esta red de una forma drástica, además, en la actualidad podemos hablar de la Historia de la Nube Informática, la cual es una entrega de servicios informáticos, entre ellos tenemos el almacenamiento, bases de datos, redes, software, etc., los cuales son almacenados en internet a través de la nube, su uso es totalmente en línea y es tanto para crear aplicaciones y servicios, almacenar datos, hacer streaming de audios y videos, entre otras funciones. La nube en la actualidad es uno de los servicios más populares y más usados, siendo uno de los avances tecnológicos más destacados de hace algunos 10 años para acá.

Existen dos tipos de nubes informáticas, la privada la cual es un servicio pagado dependiendo del almacenamiento necesitado y la nube pública, la cual es un servicio contratado por la compañía en la cual se vaya a usar, además es restringida debido a que cuenta con una capacidad básica de espacio.

1.1 Evolución Histórica de los Delitos Informáticos

La creación de nuevas tecnologías que intermedian la comunicación entre las personas trae aparejadas nuevas posibilidades para el aprovechamiento indebido e ilícito. Desde la creación del telégrafo y la posterior incorporación del teléfono a la vida cotidiana de las personas, así como la irrupción de la computadora personal, la posterior expansión de Internet y la World Wide Web; la capacidad de procesamiento de los datos e información y el acceso a miles de personas a un medio interactivo de características globales, amplió

las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales “amigables” y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto así como las posibilidades de anonimato en las comunicaciones.

El origen de los delitos informáticos puede rastrearse a partir de los años sesenta, por el temor infundido por la literatura de la época en relación a la recolección y almacenamiento de datos personales en computadoras, como referencia se encuentra la obra “1984” de George Orwell, donde se controlaba y vigilaba la vida de las personas a través del uso de las tecnologías, tras la publicación de artículos periodísticos sobre algunos de los casos, apareció por primera vez, el término *delitos informáticos* o *delincuencia relacionada con computadoras***,** retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como “ciberpunk”.

Durante los años sesenta, diferentes programadores o especialistas en informática intentaban boicotear el financiamiento gubernamental durante la guerra de Vietnam mediante el uso gratuito del servicio telefónico; el activismo político hippie de la época tuvo su costado informático a través de los phreakers (neologismo proveniente de las palabras en inglés freak, de rareza; phone, de teléfono; y free, gratis) donde a través de las llamadas blue box cajas azules establecían comunicaciones en forma gratuita simulando los tonos de llamadas utilizadas por la Bell Corporation y la ATT, básicamente para comunicaciones de larga distancia.

Con el correr del tiempo, estas técnicas de Hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables, en cuanto a la utilización de

computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales.

Durante la década de mil novecientos setenta, se comienzan a registrar una serie de casos que arrojan pérdidas cuantiosas para los sectores privados, a partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión, el objetivo de dichos delitos eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas[3], en relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial, en cuanto al sabotaje y extorsión informática, eran los delitos que más preocupaban a las administraciones gubernamentales y empresas por la alta concentración de datos electrónicos almacenados, pues el objetivo de estos eran tanto bienes tangibles (dispositivos físicos), como intangibles (datos e información), afectando tanto hardware como de software de los dispositivos, durante esta época aún no se conoce con precisión cifras estadísticas acerca de las afectaciones producidas con esta forma de criminalidad, pues apenas algunos casos han sido conocidos.

A partir de los primeros años de la década de1980, los delitos informáticos adquieren una importante notoriedad por el aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales, para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación del uso de las tarjetas de débito en los cajeros automáticos,

[3] Julio Mazuelos Coello, Modelos de Imputación en el Derecho Penal Informático (Alemania, editorial AKAL, 2002), 3. Acceso el 1 de junio de 2019.https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwj4gtXfzvbkAhVH1VkKHZU5AkEQFjAAeQIARAB&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F3313826.pdf&usg=AOvVaw3wlUk6IidOsuy18yBc5QjG.

fundamentalmente a través de la vulneración de las bandas magnéticas, esto motivó la utilización por parte de las empresas la adopción de chips en los plásticos como medida de seguridad, fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados unidos en1988, la cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial, a finales de 1990, los temas más discutidos giraron en torno a la problemática de la difusión de contenidos antijurídicos en internet para determinar si estos podían ser considerados dentro del concepto de delitos informáticos.

En la década del año 2000 en adelante pero sobre todo en el contexto latinoamericano, para el año 2015, la empresa de seguridad informática ESET, expreso en su informe titulado “ESET Security Report Latinoamérica 2015”, que solo en ocho de catorce países latinoamericanos, siendo estos México, Honduras, Nicaragua, Panamá, Ecuador, Perú, Chile y Uruguay, más del cincuenta por ciento de las empresas encuestadas reportaban “accesos indebidos a la información”, lo que suponía la pérdida y exposición de información confidencial para todas estas empresas.

Por su parte, en el informe titulado “Tendencias de seguridad Cibernética en América latina y el Caribe”, la empresa de seguridad informática Symantec, con el auspicio de la Organización de los Estados Americanos, estimaba que en dicha región los costos por la realización de delitos informáticos “ascendían por lo menos a 113 millones de dólares de los Estados Unidos de América. La misma empresa catalogó el año como el “año de las grandes violaciones a la seguridad cibernética”, manifestando que: “En la proliferación de violaciones de seguridad cibernética con fines financieros, los hackers se infiltraron en

decenas de empresas y gobiernos, incluidas muchas instituciones de América Latina y el Caribe, para lograr acceso a la información confidencial. Se produjeron 253 violaciones de datos a gran escala durante el año 2013, lo que representó un aumento del 62 % respecto del años 2012, ocho de estas violaciones de datos expusieron 10 millones de identidades o más, lo cual obligó a diversos comerciantes minoristas, empresas financieras de seguros y personas físicas, a invertir una gran cantidad de tiempo y recursos financieros para responder y recuperarse de esos ataques e implementar mecanismos de protección adicionales".

Frente a este panorama, en nuestro país se exhibió un escenario propio, en este contexto especifico, ya que el ciberdelito no es frecuente en tribunales, ni variado en su forma de realización, lo que parece desprenderse de las mismas estadísticas de la Fiscalía General de la República, según las cuales desde el año 2016 a febrero del 2018 habían ingresado un total de 568 casos, de los cuales el 70% de los mismos se canalizaban a través de los mismos tipos penales como Revelación de datos o información, Hurto de identidad, Utilización de datos personales, Acoso a través de TICS y comportamientos relativos a la pornografía. En otros términos, delitos que se relacionan con la intimidad o la libertad y la indemnidad sexual un dato que es confirmado en las entrevistas practicadas dentro de la presente investigación por un representante de la institución policial.

Resulta, entonces, llamativa la ausencia estadística de comportamientos de daños a sistemas o acceso sin consentimiento de los mismos, esto a pesar que la compañía de seguridad ESET para el año 2015 reportaba que en el territorio de El Salvador un 34% de las empresas encuestadas por dicho estudio habían sido objeto de ataques a través de malware, las razones de estas ausencias no se han medido con precisión en el presente estudio, sin embargo, expertos entrevistados sospechan que puede tratarse de una suerte

de “cifra negra” de delitos no denunciados, ya sea por la percepción que no se trata de delitos, o bien por el desinterés de realizar el aviso una vez la intrusión o el daño ha sido contenido o reparado.

1.2 Evolución Histórica del Delito de Hurto

1.2.1 A nivel internacional

En tiempo de los hebreos, el trato hacia los ladrones fue piadoso; los hurtos eran sancionados con pena de multa o indemnizaciones, porque se entiende que los bienes fueron entregados al pueblo por Dios para su administración, esta visión social de la propiedad, es la que determina el tratamiento clemente de quienes hurtan o roban por estimar que ello sucedía a consecuencia de necesidades insatisfechas cuya responsabilidad era de la comunidad[4]. Desde entonces se hace una distinción entre el hurto y el robo sobre las mismas bases actuales, es decir, el primero se perpetraba sin violencia, imponiendo en ambos casos a sus autores la restitución del objeto sustraído más una multa, salvo que no pudiera hacerse cargo de la indemnización, circunstancia que lo hacía verse privado de su libertad.

En el derecho penal romano, se denominaba furtum a la apropiación de la propiedad ajena, puesto que, como enseña Mommsen[5], literalmente fur significa “el que lleva algo” y furtum, “la sustracción y lo sustraído”, conceptualmente, este delito consiste en la apropiación de una cosa mueble ajena, con el fin de lograr un enriquecimiento patrimonial propio y con perjuicio de un tercero, el hurto de cosas privadas se reprimía con la pena capital (pena de muerte), en épocas del derecho de guerra de la República, pero con la ley de las Doce Tablas (donde aparecen las primeras disposiciones que lo regulan), se manifestaron sus primeros elementos, el ánimo de lucro recaía en

[4] Martín Schwab, Manual de derecho penal hebreo, editorial Jurídica (Buenos Aires, 2014), 264, 267. Acceso el 1 de junio de 2019 http://www.casi.com.ar/sites/default/files/10953.PDF.
[5] Theodor Mommsen, Derecho penal romano (Madrid: La España Moderna, 1905), 457.

cosa ajena, aunque en este antiguo Derecho no se distinguía sobre el apoderamiento violento de la cosa ajena y el realizado sin ella, con el tiempo se lograron distinguir ambas figuras, denominándole al primero como Rapiña castigándosele con mayor dureza y al segundo se le denomino como ya se había dicho anteriormente Furtum, esta distinción romana modernamente es conocida como Robo y Hurto, caracterizándose el hurto por la aprehensión clandestina de la cosa mueble ajena con ánimo de lucro, mientras que el robo era la aprehensión violenta y manifiesta de la cosa ajena con el mismo ánimo de lucro, para estos el hurto se constituía mediante dos actos: uno moral que consistía en la resolución de apoderarse de la cosa ajena llamado dolo malo, y otro físico, que consistía en poner la mano sobre el objeto apetecido que era llamado contrectatio.

En el derecho español, el Fuero Real hacia una distinción del hurto, pues este lo clasificaba en dos sentidos, el primero era según el lugar de comisión del mismo, ya que este podía ser cometido en el camino, en la iglesia o casa.[6] En el caso del hurto cometido en casa o en una iglesia podía llegar a castigarse con la pena de muerte, mientras que el cometido en el camino por asaltante reincidente solo se le aplicaba una multa arbitraria. En segundo lugar, el Hurto era clasificado también de acuerdo con el valor de lo sustraído, ya que, si este era mayor o menor a cuarenta maravedíes, usualmente a quien cometiera el hurto se le multaba o se le castigaba con azotes, pero la multa impaga se castigaba con la pérdida de una oreja o de un puño.

Durante las partidas se estableció otra de las distinciones de hurto pues este se clasificaba entre *furtum manifestum* o flagrante, que era cuando el ladrón

[6] Abelardo Levaggi, Historia del Derecho Penal Argentino (Buenos Aires: Perrot, 1939), 94. Acceso el 1 de junio de 2019. http://www.derecho.uba.ar/investigacion/documentos/lecciones-de-historia-juridica-v-1978-levaggi-historia-del-derecho-penal-argentino.pdf.

era sorprendido en el momento de cometer el delito o cuando se le encontraba llevando consigo el objeto hurtado, y *furtum nec manifestum* u oculto; siendo esta la manera en cómo se siguió reconociendo el hurto en muchas legislaciones hasta llegar a nuestros días.

1.2.2 En El Salvador

En El Salvador se pueden identificar seis códigos penales, el primer código fue decretado el día 13 de abril de 1826[7], que constaba de ochocientos cuarenta artículos, el cual tomó de modelo el Código Español de 1822, ya que al independizarse El Salvador de España en nada se modificó la legislación penal vigente en nuestro país porque se mantuvo vigente el contexto penal de la colonia, este código contempla un catálogo completo de delitos, de circunstancias modificativas y excluyentes de penas, así como de reglas para su aplicación, respecto de las penas contempladas en este código, estas se dividían en penas corporales, no corporales y pecuniarias.

Como obra del presbítero y doctor Isidro Menéndez, con la ayuda del ciudadano José Mateo Ibarra, en el año de 1855 se incorporó en El Salvador, el primer Código Penal a la Recopilación de Leyes Patrias de 1855, para la aprobación de este Código, se necesitó la cooperación de Don José Mariano Méndez, diputado por el departamento de Sonsonate, este primer Código aporto la primera definición del delito de Hurto.

Posteriormente con el Código Penal de 1859 el artículo 425, se estableció que son los reos de hurto, expresando que son todos aquellos que con ánimo de lucro y sin violencia o intimidación en las personas ni fuerza en las cosas, toman las cosas muebles ajenas sin la voluntad de su dueño, en este primer

[7] Nelson Geovanny Castro, Kevin Everardo Ramos Gómez, “Juicio para la aplicación exclusiva de medidas de seguridad" (Trabajo de grado para obtener el título de Licenciado en Ciencias Jurídicas, 2003), 70.

numeral solo se describía la conducta típica, conteniendo propiamente lo que en la actualidad es el delito de hurto.

En el Código Penal de 1881 en su Artículo 473 se establecía, el termino violencia de forma exclusiva para la figura delictiva del Robo, ya que en este caso el sujeto activo puede conocer o no, a quien pertenece la cosa encontrada, y este con ánimo de lucrarse de ella no da aviso a la autoridad competente, por consiguiente realiza la acción penal de hurto, dentro de este se establecían las siguientes penas: 1º con la pena de presidio menor en su grado máximo, si el valor de la cosa hurtada excediere de cien pesos, 2º con la pena de presidio correccional en su grado máximo, si no excediere de cien pesos y pasare de diez.

El Código Penal de 1904, en su Artículo 468 establecía un concepto más delimitado del actuar de Hurto, pues se regula como la mera acción de tomar cosas ajenas sin la voluntad del dueño, su consecuencia jurídica se regulaba en el Artículo 469 que establecía la pena de la siguiente manera: 1. Con la pena de cinco años de presidio si el valor de las cosas hurtadas excediere de mil pesos. 2. Con tres años de presidio si lo hurtado pasare de quinientos y no excediere de mil pesos. 3. Con dos años de prisión mayor si pasare de cien pesos y no excediere de quinientos y 4. Con un año de prisión mayor si no excediere de cien pesos y pasare de veinticinco.

El Código Penal de 1974, en su Artículo 237 presento un avance significativo en el tipo penal del hurto, como es, el hecho de establecer la cuantía para la consumación del mismo, debido a que el valor de la cosa hurtada debe ser mayor a veinte colones, la incorporación de elementos para la fijación de la pena que se deberán evaluar previamente para imponer la sanción penal, entre ellos el valor real de la cosa, que se traduce a una cantidad en dinero, el cual hace referencia al precio suplementario que en cosas propias se concreta

por la utilización desde larga data o relevante utilidad personal, y, más aún por haber pertenecido a personas de la intimidad, entre ellos de la familia u otros; el lugar de la ocasión, para referirse al lugar específico donde se ha cometido el delito de hurto; condiciones en que se cometió el hecho delictivo, ya sea aprovechando circunstancias de ventaja para la apropiación de la cosa y los antecedentes de conducta del culpable, con lo cual se juzgaba con un derecho penal de autor y no de actos.

El Código Penal de 1998 que en su Artículo 207 establece 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 doscientos colones. Este código se elabora en relación a los avances que han venido aportando los anteriores códigos, respecto a la regulación del delito de hurto, establece los requisitos para la configuración del ilícito de una forma completa, como el ánimo de lucro, que la cosa sustraída puede ser total o parcialmente ajena, el incremento de la cuantía de veinte colones a doscientos y se da un incremento en el mínimo de la pena de uno a dos años.

1.2.3 Evolución tecnológica del Hurto

Si bien, las tecnologías de la Información y la Comunicación han tenido un gran impacto en nuestro país en las últimas décadas, como anteriormente se ha mencionado con el pasar de los años el delito de hurto ha venido evolucionando y con la evolución de las TICS surgió una nueva manera de cometer el delito de Hurto ya que en la actualidad, este delito es cometido a través de medios informáticos, afectando de esta manera tanto a personas naturales como jurídicas, padeciendo cada una de ellas en su medida, graves detrimentos patrimoniales a través de la pérdida de sus bienes económicos e información privada a la que acceden de manera ilegal los delincuentes.

La ocurrencia de este delito se relaciona directamente con todas aquellas operaciones que los clientes bancarios y en especial los tarjetahabientes realizan a través de sus computadores, tablets, celulares y todos aquellos dispositivos que por su capacidad pueden almacenar o copiar información digital, como son las tarjetas de débito o crédito, los cajeros electrónicos, entre otros; pues a través de estos medios es que los delincuentes informáticos acceden a las cuentas de los clientes bancarios y realizan operaciones sin su autorización o consentimiento las cuales se constituyen en hurtos por medios informáticos, aunque en El Salvador hasta la fecha no se encuentran antecedentes históricos acerca del surgimiento de dicha figura delictiva ya que únicamente se cuenta con el artículo 13 de la LECDI, que nos establece únicamente la tipificación del delito como tal.

CAPITULO II

BASES DOCTRINARIAS DE LOS DELITOS INFORMATICOS Y EL DELITO DE HURTO POR MEDIOS INFORMATICOS

El presente capitulo tiene como propósito establecer las bases doctrinarias de los Delitos Informáticos de forma general para lograr entender en primer lugar de que se tratan y como están conformados para luego desarrollar de forma específica el Delito de Hurto realizado por un medio Informático estableciendo en primer lugar su concepto, características, elementos diferenciadores, el bien jurídico protegido por los mismos, sus tipos y la diferencia entre este tipo de delitos con otros que han sido cometidos por medios informáticos.

2. Desarrollo de Conceptos Básicos y Estudio de los Delitos Informáticos

Luego de conocer la historia de la Computadora y la evolución Histórica de los Delitos Informáticos, es importante entender la diferencia esencial entre un delito informático y los delitos electrónicos, siendo de esta manera importante comprender que se entiende en todo caso por Electrónica y por Informática, para obtener una mejor comprensión en el tipo de Delito del cual nos enfocaremos en el presente trabajo de investigación.

La electrónica “es un campo de la física que se refiere al diseño y aplicación de dispositivos”[8], por lo general circuitos electrónicos, cuyo funcionamiento se basa en la conducción y el control del flujo microscópico de los electrones u otras partículas cargadas eléctricamente para la generación, transmisión, procesamiento o almacenamiento de la información codificada eléctricamente, las computadoras son máquinas electrónicas que procesan datos, que permiten su almacenamiento y proporciona resultados, estas computadoras

[8] Gustavo Ruíz Robredo, Electrónica Básica para Ingenieros (España: El autor, 2001), 11.

están compuestas por dos partes que son el Software y el Hardware, pero para el tema que interesa en este punto se hace referencia al Hardware, el cual se define como aquel conjunto de componentes físicos de los que están hechos los equipos, es decir que son las partes que se pueden ver y tocar de los dispositivos.

Por su parte, la informática "es la rama de la ingeniería que estudia el hardware, las redes de datos y el software necesarios para tratar la información de forma automática"[9], en otras palabras, es aquella que se encarga del procesamiento, almacenamiento y transmisión de la información en formato digital, mediante el uso de los diversos dispositivos electrónicos y sistemas computacionales.

El software es aquel conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo, en otras palabras, estos son los programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador, como ejemplos, de software están los sistemas operativos, aplicaciones, navegadores web, juegos o programas.

2.1 Concepto

Hoy en día no es fácil conceptualizar a los delitos informáticos por su novedad, variedad y complejidad, la doctrina actualmente no se apoya en un parámetro claro y común desde el cual se pueda comenzar a intentar definirlos, no obstante, hay que despejar algunas confusiones habituales que permitan llegar a dar un concepto de delito informático.

Alguno autores para conceptualizar los Delitos Informáticos se basan de dos vertientes, primero establecen que si se busca dar un concepto de los mismos

[9] Arturo Díaz, Informática I (México: Fondo Editorial, 2003), 15.

desde una perspectiva atípica se podrá establecer que los Delitos Informáticos son “actitudes ilícitas en que se tiene al computador como instrumento o fin”, pero si lo que se busca es una perspectiva tomada desde lo típico se puede establecer que en este sentido serán “conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin”[10].

Por su parte otros autores definen los delitos informáticos como “aquellos que se dan con la ayuda de la informática o de técnicas anexas”[11], en cambio para otros, el delito informático “es cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo”[12], pero también hay autores que entienden a los “delitos informáticos como toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”[13].

Ahora bien, lo que se busca es conceptualizar las conductas ilícitas nuevas, cometidas generalmente a través de equipos electrónicos, pero en donde el elemento central no es el medio de comisión sino que es el hecho de atentar contra un bien informático, se hace necesario en ese sentido destacar que no todos los bienes son objeto de estos delitos, como sabemos los sistemas de tratamiento automatizado de la información se basan en dos grandes tipos de soportes, el físico y el lógico, así, por una parte, los bienes informáticos que tienen relación con el soporte físico conforman el hardware, es decir, los equipos electrónicos, que son bienes corporales muebles como el procesador, la unidad central de procesamiento, los dispositivos periféricos de entrada y

[10] Julio Téllez Valdés, “Derecho Informático”. (México: McGraw-Hill, 1996), 104.
[11]“Delitos Informáticos: Generalidades”. Acceso el 26 de junio de2019.https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.
[12] Miguel Estrada Garavilla, “Delitos Informáticos”, Revista Derecho Penal, n1 (2008): 4.
[13] María Cinta Castillo Jiménez, Miguel Ramallo Romero; “El delito informático” (Zaragoza: Acribia, 1989), 22-24.

salida, los dispositivos de almacenamiento y la red de comunicaciones, por otro lado, podemos determinar que existen bienes intangibles que son los que constituyen el soporte lógico del sistema o también conocido como software, dentro de él están los datos digitalizados, que se ingresan a la computadora para que sean procesados y puedan constituir información, además, que son un conjunto de instrucciones usadas directa o indirectamente a fin de efectuar u obtener un determinado proceso o resultado.

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, cibercrímenes, delincuencia conexa con la computadora, etc., por lo que podemos decir entonces que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes de comunicación 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.

Como último punto es importante expresar que la legislación Salvadoreña establece que para el cometimiento de los Delitos Informáticos se debe hacer uso de las tecnologías de la información y la comunicación, entendiendo por ellas a todo “aquel conjunto de tecnologías que permiten el tratamiento y la comunicación de los datos, registro, presentación, creación, administración, modificación, movimiento, visualización, distribución, intercambio, transmisión

o recepción, control y manejo de la información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros"[14], ahora bien, tomando como referencia el aporte de dichos autores y la legislación Salvadoreña, se puede determinar que los Delitos Informáticos son aquel conjunto de Delitos que usando las tecnologías de la Comunicación y la Información tienen por objeto una conducta típica, antijurídica y culpable cuyo medio para su realización es la utilización de equipos o dispositivos electrónicos que le permitirá manipular, gestionar o guardar la información obtenida mediante el acceso no autorizado a registros o programas de un sistema produciendo un daño en la privacidad de la persona perjudicada.

2.1.1 Características

Los Delitos Informáticos tienen diversas características entre las cuales se pueden encontrar[15]: 1. Son conductas que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas; 2. Son acciones ocupacionales debido a que muchas veces se realizan cuando el sujeto se encuentra trabajando; 3. Provocan serias pérdidas económicas, porque casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan"; 4. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo sin una necesaria presencia física pueden llegar a consumarse; 5. Son muchos los casos y pocas las denuncias, todo ello debido a la falta de regulación por parte del Derecho; 6. Son muy sofisticados y relativamente frecuentes en el ámbito militar; 7. Presentan grandes dificultades para su comprobación, por su carácter técnico, y; 8. Tienden a proliferar más.

[14] Ley Especial Contra Delitos Informáticos y Conexos (El Salvador, 2016), arts. 3, literal L.
[15] Jonathan Alexander Ávila Umaña, Antonio Alexander Barrera Argueta, "Elementos diferenciadores del delito de estafa regulado en el artículo 215 del código penal con la estafa informática regulada en la ley especial contra delitos informáticos y conexos" (Trabajo de grado para obtener el título de Licenciado en Ciencias Jurídicas, 2018), 65.

2.1.2 Sujetos

En el derecho penal, la ejecución de la conducta punible supone la existencia de dos tipos de sujetos, uno activo y otro pasivo que, a su vez, pueden ser una o varias personas naturales quienes cometen la conducta punible en el caso del sujeto activo, pero en el caso del sujeto pasivo estos pueden ser una o varias personas naturales o jurídicas, ya que son quienes se ven perjudicados por el sujeto activo, a continuación, ambas se detallaran:

2.1.2.1 Sujeto Activo

El sujeto activo *"se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal"*[16], en ese sentido el Sujeto Activo en los Delitos Informáticos es aquel que posee 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 estos sistemas, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

2.1.2.2 Sujeto Pasivo

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, y todos aquellos que usan sistemas automatizados de información, generalmente conectados a otros, dicho de otra manera, es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

[16] Mario Garrido Montt, Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992. Citado por Jijena Leiva Renato, Los Delitos Informáticos y la Protección Penal a la Intimidad, Editorial Jurídica de Chile, 1993.

2.1.3 Bien Jurídico Protegido

El bien jurídico protegido es aquel bien lesionado o puesto en peligro por la conducta del sujeto activo, este constituye la razón de ser del delito y no suele estar expresamente señalado en los tipos penales, sin embargo, son tutelados por el cuerpo normativo.

En los Delitos Informáticos el bien jurídico protegido en general es la información, pero considerada en diferentes formas, ya sea como un valor económico, como uno 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: El patrimonio: en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar; la privacidad, 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; la seguridad o fiabilidad del tráfico jurídico y probatorio: en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos y; el derecho de propiedad: "*se trata sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático"*[17].

Por tanto, el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde se almacena o transfiere, para algunos autores, los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno*

[17] Claudio Paul Magliona Marcocicht, Macarena López Medel, "Delincuencia y Fraude Informático" (Chile: Editorial Jurídica, 1999), 66.

de tales bienes este independientemente tutelado por otro tipo"[18]. En conclusión, no se afecta un solo bien jurídico, sino una diversidad de ellos.

2.1.4 Tipos de Delitos Informáticos

Es importante tener en cuenta que los Delitos Informáticos pueden clasificarse de diferente manera según las diversas legislaciones de los diferentes países del mundo en que se regulen este tipo de delitos, a continuación, se expondrán algunas clasificaciones:

a) La Convención de Delitos Informáticos del Consejo de Europa, clasifica las conductas lesivas a la información en cuatro tipos diferentes entre los cuales podemos encontrar:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: El cual sanciona el acceso y la intercepción ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
2. Delitos de fraude informático: Falsificación y fraude computacional
3. Delitos por su contenido: Producción diseminación y posesión de pornografía infantil.
4. Delitos relacionados con la infracción de la propiedad intelectual y derechos afines: la amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor.

b) La Unión Europea, en la Propuesta de Decisión sobre el Marco del Consejo Relativa a los Ataques de los que son objeto los Sistemas de Información, identifica la siguiente clasificación de acuerdo al rango de amenaza que esta proporciona:

1. Acceso no autorizado a sistemas de información, que incluye la "piratería" informática;

[18] Alfonso Reyes Echandía, "La Tipicidad" (Colombia: Universidad de Externado de Colombia, 1981), 50.

2. Perturbación de los sistemas de información, como la “denegación de servicio”;
3. Ejecución de programas perjudiciales que modifican o destruyen datos, incluye virus, bombas lógicas y gusanos;
4. Interceptación de las comunicaciones, denominada intromisión (sniffing);
5. Declaraciones falsas, se trata de la usurpación de la identidad de una persona en Internet, se llama “spoofing” (modificación de datos).

c) En cuanto a las Naciones Unidas, esta reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras: Manipulación de datos de entrada, manipulación de programas, manipulación de datos de salida y fraude efectuado por manipulación informática.
2. Falsificaciones informáticas: como objeto, porque se alteran los datos de los documentos almacenados y como instrumentos.
3. Daños o modificaciones de programas o datos computarizados: sabotaje informático, virus, gusanos y bomba lógica o cronológica.
4. Falsificaciones informáticas: Acceso no autorizado a sistemas o servicios, piratas informáticos o hackers y reproducción no autorizada de programas informáticos.

Es importante establecer que estos atentados contra la información se distinguen a partir de las diversas conductas realizadas sobre las propiedades esenciales de la información: confidencialidad, integridad y disponibilidad, a continuación, se explicaran cada una de estas.

2.1.4.1 Conductas lesivas a la confidencialidad

En las conductas lesivas a la confiabilidad de la información se encuentran:

El espionaje Informático (Industrial o Comercial), con los términos industrial y comercial se pretende delimitar esta categoría, excluyendo bienes jurídicos

distintos como sería el caso de delitos contra el Estado y la defensa nacional o contra la intimidad, esta conducta debe entenderse como la obtención con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio, en los comportamientos que pueden ser incluidos en esta descripción se identifican: la fuga de datos (Data Leakage), que las empresas o entidades guardan en sus archivos informáticos, las puertas falsas (Trap Doors), consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas; las "llaves maestras" (Supperzapping) que implica el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información, el pinchado de líneas (Wiretapping), que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se trasmiten las informaciones procesadas y la apropiación de informaciones residuales (Scavenging) que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

El Intrusismo informático es la introducción a sistemas de información o computadoras, infringiendo las diversas medidas de seguridad destinadas a proteger los datos contenidos en ellos, a primera vista pareciera que el sabotaje informático y el intrusismo son comportamientos idénticos, sin embargo, es el elemento subjetivo de estos el que delimita su comportamiento, debido a que en el primer supuesto, la intencionalidad que tiene el agente es obstaculizar el funcionamiento de un sistema informático y en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la producción del perjuicio que se produzca, es ajeno al comportamiento, aunque es evidente que lo agrava. En ese sentido se puede determinar que ambas figuras, aunque parecen similares, no lo son pues tienen elementos que las diferencian.

2.1.4.2 Conductas lesivas a la integridad

Las conductas lesivas a la integridad de la Información, consisten en el acceso directo u oculto no autorizado a un sistema informático mediante la introducción de nuevos programas denominados virus. El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema, recibe el nombre de “sabotaje informático”.

2.1.4.3 Conductas lesivas a la disponibilidad

Los virus informáticos son un ejemplo claro de las conductas que pueden afectar transitoriamente la disponibilidad de la información, sin destruirla, otro de los mecanismos que pueden impedir el acceso a un sistema de información por parte de los usuarios legítimos, son los denominados “spam” o el “electronic-mail bombing”, que consisten en el envío de cientos de miles de mensajes de correo electrónico no solicitados o autorizados, para bloquear los sistemas.

2.2 Desarrollo de Conceptos Básicos y Estudio del Delito de Hurto Informático

2.2.1 Concepto

Según la doctrina estudiada, no se encontraron autores que hagan referencia a un concepto o definición de lo que es el delito de Hurto por medios Informáticos, razón por la cual para hacer una aproximación a un concepto del mismo, la legislación penal Salvadoreña, establece en el Art. 207 del Código Penal lo siguiente: "*El que con ánimo de lucro para sí o para un tercero se apodere 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 doscientos colones*"[19].

[19] Código Penal (El Salvador, 1993), art. 207.

Antes de continuar, es importante aclarar en este punto que, si el valor de lo hurtado no fuere mayor de doscientos colones, ya no se está en presencia de un delito como tal, sino que se hará referencia a una falta relativa al patrimonio, tal como se menciona en el artículo 379 del Código Penal que dice: *"El que cometiere hurto, si el valor de lo hurtado no excediere o fuere igual a doscientos colones, será sancionado con arresto de diez a veinte fines de semana y de diez a veinte días multa".* Al igual que los delitos, las faltas se tratan de una conducta típica (aparece tipificada en la ley), antijurídica (contraria a Derecho) y culpable, pero en la legislación viene regulado como falta debido a su menor gravedad, ya que sus consecuencias no son las mismas. Por lo tanto sus penas son mucho menores que las de los delitos, ya que éstas nunca llegarán a ser penas de cárcel sino simplemente pueden ser el arresto de fin de semana, el arresto domiciliario, la prestación de trabajo de utilidad pública y la multa.

Ahora bien dicho lo antes mencionado podemos ver que el delito de hurto contemplado en nuestro Código Penal en el artículo 207, establece que el bien jurídico protegido es la propiedad, mientras que el objeto material, es decir, aquel sobre el cual se ejecuta una acción o conducta antijurídica es una cosa mueble ajena, por lo tanto, el delito se entenderá consumado con el apoderamiento del bien despojado de su poseedor, pero que además implica el lucro para sí mismo por parte del sujeto activo o a favor de un tercero, en este punto no se entrara a discutir si el concepto de bien mueble incluye a los bienes inmateriales, sino lo que se pretende es entender los elementos esenciales del delito, para a continuación analizar los elementos del hurto por medios informáticos, ya que por su parte la Ley Especial contra Delitos Informáticos y Conexos, describe el tipo penal del Hurto por Medios Informáticos estableciendo en su Art. 13 que: *"El que por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o*

valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años"[20], siendo este articulo el único aporte encontrado sobre lo que entenderemos por Hurto Informático.

Por lo que antes de entrar a analizar los elementos que componen este delito, se debe comprender que son las tecnologías de información y la comunicación, estipuladas en el literal L) del artículo 3 de la misma ley, dicho esto, se establece que las Tecnologías de la Información y la Comunicación son: "*el conjunto de tecnologías, que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros"*[21]

En ese sentido, toda la tecnología que permita el uso de la información en forma automática, será considerada como Tecnología de la información y la comunicación, siendo las acciones descritas en la definición registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción, entre otros, funciones que son típicas de éstas.

Para lograr profundizar en el análisis del Delito de Hurto por Medios Informáticos, se establece que la acción típica del delito de hurto por medios informáticos la realiza "el que se apodere de una cosa mueble ajena" y por apoderamiento, debe entenderse el "entrar en dominio de una cosa, consiste

[20]Ley Especial Contra Delitos Informáticos y Conexos (El Salvador, 2016) 13.
[21]Ibíd.

entonces en tener la posibilidad de actuar respecto de un bien como si se fuese señor y dueño de él, entonces el apoderamiento se consuma cuando el agente elude de forma definitiva todas las medidas de custodia del bien de parte de la víctima, para mejor comprensión de lo antes expuesto se toma por ejemplo, cuando el sujeto activo accede a las plataformas informáticas de una entidad financiera, y traslada los fondos contenidos en una de las cuentas, pasándolos a otra cuenta de propiedad del delincuente y retirándolos mediante un cajero automático, de igual forma se presenta el apoderamiento, cuando el autor del delito manipula el sistema informático de tal manera que, todas las consignaciones que se realicen en determinada cuenta, sean desviadas a otra cuenta de una entidad financiera distinta, cuyo titular sea el sujeto activo de la conducta criminal.

Sin embargo, si el delincuente no logra superar las barreras de protección del sistema informático, no se habrá dado el apoderamiento, y, por ende, la conducta no se habría consumado, por lo que el sujeto activo deberá responder por el delito de hurto por medios informáticos en modalidad tentada, pues si el delincuente sustrae determinado monto de la cuenta de una entidad financiera, mediante la instalación de un virus que rompe con las medidas de seguridad del sistema informático, y logra que dicho dinero entre en una cuenta de su propiedad, pero el sistema informático cuenta con una alerta de fallas, lo que permite que la entidad financiera bloquee casi de forma inmediata la transacción fraudulenta, aun cuando el delincuente llegó a tener el dinero en su cuenta por unos instantes, lo cierto es que nunca tuvo la posibilidad real de actuar como señor y dueño de él. Por lo que, podría afirmarse que el apoderamiento nunca se dio, y, por ende, que la conducta típica nunca se consumó.

En ese sentido se entiende que los medios que deben utilizarse para que se estructure el tipo del delito de hurto por medios informáticos son los siguientes:

1. Manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o 2. Suplantación de un usuario ante los sistemas de autenticación y de autorización establecidos, ahora bien cuando hacemos referencia a la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, hacemos referencia al grupo de conductas cometidas por el "cracker" que supera las medidas de seguridad del sistema con el fin de apoderarse de los recursos que se manejan y canalizan a través de ese sistema. Por ejemplo, cuando el delincuente logra controlar de forma cabal las operaciones que se realizan por intermedio de ese sistema informático, así, desde la comodidad de su casa, el delincuente que manipuló el sistema informático podrá desviar recursos de una cuenta a otra, sustraerlos e incluso eliminarlos a su antojo.

De acuerdo a lo anterior, se puede entender que el delito de hurto por medios informáticos, se relaciona de forma directa con las operaciones que los clientes bancarios y en especial los tarjeta habientes realizan a través de sus computadores, tablets, equipos celulares, y todos aquellos dispositivos que por su capacidad pueden almacenar o copiar información digital, como son las tarjetas de débito o crédito, los cajeros electrónicos, entre otros; pues es a través de estos medios que los delincuentes informáticos acceden a las cuentas de los clientes bancarios, y realizan operaciones sin su autorización o consentimiento, las cuales constituyen el delito en mención, ya que se accede por medio del uso de las TICS a un soporte informático para sustraer un bien o valor intangible y para ello es menester que esté plasmado en un soporte que le dé materialidad al mismo para permitir una apropiación.

La fórmula a la que se hace referencia implica normalmente el acceso al sistema operativo de la víctima a través de la red sin que ésta sea consciente, pues el acceso a distancia a la computadora del sujeto pasivo puede llevarse a cabo a través de distintas vías, sin embargo, en la actualidad suele

producirse mediante el recurso a archivos espía (Spyware), aplicaciones o programas que se consiguen introducir en la PC de la víctima y cuyo objetivo es él envió de los datos del sistema donde se encuentran instalados habitualmente a la computadora del sujeto activo, esto sin que la persona se dé cuenta. Otra técnica frecuentada es el uso de Keyloggers, los cuales registran todo lo que el usuario de la computadora teclee, de este modo el sujeto activo se apodera de la información personal, como puede ser datos bancarios y las claves de acceso que serán posteriormente utilizados en una segunda fase para realizar transferencias a su favor o de un tercero[22].

Mediante entrevista obtenida en la División de Policía Técnica y Científica de la Policía Nacional Civil, se advirtió que existe una cifra negra respecto a este tipo de delitos, ya que, el mismo se encuentra estrechamente relacionado con entidades financieras, las cuales prefieren asumir los costos o responsabilidad de estas conductas delictivas, evitando con ello transmitir una imagen de vulnerabilidad.

De acuerdo a lo anterior, se entenderá como delito de Hurto por medios Informáticos aquella conducta realizada por un sujeto que haciendo uso de las tecnologías de la Información y la Comunicación se apodere de bienes o valores tangibles e intangibles sustrayéndolos a su propietario, tenedor o poseedor de manera dolosa, con el fin de obtener un provecho económico para sí mismo o para otro por medio de la suplantación de un usuario ante los sistemas de autenticación y de autorización establecidos, en los sistemas Informáticos, sin ser posible que al momento de realizarse la acción, esta fuera realizada con culpa.

[22] Escuela de capacitación judicial Dr. Arturo Zeledón Castrillo, del Consejo Nacional de la Judicatura. "Monográfico: Debates sobre el sistema de justicia penal y penitenciario". Acceso 3 de agosto de 2019.http://www.cnj.gob.sv/web/images/documentos/pdf/publicaciones/MONOGRAFICO_DebatesSistemaJusticiaPenalyPenitenciario.pdf.

2.2.2 Características

Para que se consume el delito de hurto por medios informáticos debe concurrir un desplazamiento digital o informático, equiparable al físico en la realidad material, del bien mueble. De ahí que sean dos los verbos rectores principales: el primero es “apoderarse”, de los bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor y el otro, es “obtener” un provecho económico para sí o para otro, por medio del uso de las Tecnologías de la Información y la Comunicación.

Cabe agregar que en el ámbito de la criminalidad informática es posible sustraer información sin necesidad de proceder a un desplazamiento físico o material, esto en virtud de que basta con que el bien quede de alguna forma bajo el control del sujeto activo, así por ejemplo en la sustracción de información, el apoderamiento puede realizarse con una simple lectura o memorización de datos, de cuya utilización no queda excluido el titular, en ese sentido podemos determinar que algunas de sus características son: 1. Ser un delito de conducta momentánea, pues la acción típica se agota en el momento del apoderamiento o sustracción de datos o dinero a través de retiros o transferencias fraudulentas utilizando medios informáticos; 2. Ser un delito de resultado porque para su consumación es imperativo el apoderamiento de datos o dinero, que implicará un perjuicio para quien tenga la posesión dichos bienes o valores; 3. Ser realizados por medio del uso de las Tecnologías de la Información y la Comunicación; 4. Presentar grandes dificultades para su comprobación; 5. Ofrecer facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse y; 6. Son conductas que sólo determinado número de personas con ciertos conocimientos técnicos pueden llegar a cometerlas.

Es importante establecer que el delito de Hurto por medios informáticos, se encuentra situado dentro del Capítulo II de la Ley Especial Contra Delitos

Informáticos y Conexos, denominado: "De los Delitos Informáticos", pero que además se puede sub clasificar dentro los delitos informáticos que buscan un aprovechamiento o afectación de carácter patrimonial, junto a la estafa informática y al fraude informático, ya que sus acciones están encaminadas a esa obtención, aprovechamiento o perjuicio patrimonial del sujeto pasivo.

Por su parte, el Hurto por medios informáticos se desarrolla como una modalidad residual respecto a los otros dos comportamientos, ya que, si en la estafa informática y al fraude informático el engaño o la tergiversación de la realidad es necesaria, en este caso, el sujeto activo no debe manipular por medios informáticos al sujeto pasivo (como en la Estafa), ni manipular el sistema informático para su beneficio (como en el fraude), se trata entonces de casos en los que el sujeto activo por alguna razón conoce la forma de acceso y manejo del sistema, y abusando de estos privilegios se apodera de bienes o valores tangibles o intangibles, o bien realiza mínimas instrucciones al sistema que no clasifican a criterio del juzgador como “insertar instrucciones falsas al sistema”.

2.2.3 Elementos Objetivos

2.2.3.1 Sujeto Activo

Es todo individuo que se apropia de bienes ajenos haciendo uso de las Tecnologías de la Información y la Comunicación, con el fin de obtener un provecho económico para sí o para otro.

2.2.3.2 Sujeto Pasivo

Sujeto pasivo es la persona natural o jurídica que sufre la privación de la propiedad de sus bienes, con la utilización de los referidos métodos, en otras palabras, es el sujeto sobre el cual recae la acción o conducta del sujeto activo, el cual le genera un perjuicio en su patrimonio o en su privacidad, dependiendo de lo hurtado.

2.2.4 Elementos Subjetivos

2.2.4.1 El dolo

Este delito sólo puede ser realizado con dolo, es decir con la intención de causar daño a otra persona, al apropiarse ilícitamente de sus bienes, no cabe, por lo tanto, la culpa.

2.2.4.2 El ánimo de lucro

Está representado en el delito en comento, como la pretensión del sujeto activo en el sentido de obtener como resultado de la conducta típica, un beneficio económico para sí mismo o para otro.

2.2.5 Bien Jurídico Protegido

En el delito de hurto por medios informáticos además del patrimonio económico (entendido éste como los bienes pecuniarios correspondientes a una personas, donde se incluyen por ende, derechos reales, la posesión, la tenencia, inciso derechos personales de carácter patrimonial y los créditos), se protege otro bien de naturaleza colectiva, en razón de que la ejecución de la conducta punible no sólo causaría efectos sobre el patrimonio individual, sino también sobre los elementos del propio sistema informático, es decir, que la protección individual y colectiva del bien jurídico, obedece a que en la comisión de este tipo de delito ocasiona además de la pérdida patrimonial para un individuo, la lesión de la seguridad y la confianza que los usuarios tienen en los sistemas informáticos, las redes de sistemas electrónicos, telemáticos y otros medios análogos, es decir, la protección de la información y de los datos.

Con base en esto, no habría obstáculo alguno en admitir a la información computarizada como bien mueble y, por lo tanto, objeto material del delito de hurto, en cuanto sea susceptible de gozar de un determinado valor económico en el mercado, siendo por medio de la información que el delincuente

informático desplaza el patrimonio económico de las personas existentes en las diferentes entidades bancarias, quienes custodian a través de cuentas asignadas a miles de sus afiliados el dinero por ellos depositado; dinero que es sustraído luego de apoderarse, a través de diferentes medios ilegítimos de carácter informático, de la información privilegiada de cada cliente; información necesaria para ingresar a los sistemas bancarios y que consiste en datos, tales como códigos, claves, números de cuentas bancarias, números de tarjetas de crédito, números de identificación personal, en fin, toda aquella secuencia numérica o alfanumérica necesaria para que las personas tengan acceso a las diferentes actividades comerciales, personales y de comunicaciones que surgen de la utilización de los sistemas informáticos, bien jurídico patrimonial que está para este caso, íntimamente ligado a ese nuevo bien construido por los legisladores como es “la protección de la información y de los datos”, y que protege ya desde un perfil más amplio la información personal y privada del conglomerado social, sean personas naturales o jurídicas quienes utilizan la red conocida como Internet.

CAPÍTULO III

LA LEGISLACIÓN NACIONAL E INTERNACIONAL RELACIONADA CON EL DELITO DE HURTO POR MEDIOS INFORMÁTICOS

El presente capitulo tiene como propósito establecer un análisis de la legislación Salvadoreña, la legislación extranjera y la legislación Internacional aplicable al delito de Hurto por medios Informáticos para lograr con ello determinar si la regulación aplicada en nuestro país al tratamiento de dicho delito es efectiva para darle el tratamiento respectivo al momento de encontrarnos delante de un delito de dicha índole y de igual manera que sirva como un aporte el tratamiento que se le da al delito en estudio a nivel internacional con el fin de tomar elementos que sirvan en nuestro país como forma de tipificar, regular y tratar el Hurto por medio Informático.

3. Legislación salvadoreña

3.1 Constitución de la República de El Salvador

La Constitución de la República no aborda de manera específica los delitos informáticos, pero si podemos encontrar que dentro de sus artículos se encuentran tutelados los bienes jurídicos que se pretenden proteger ante este tipo de delitos, en nuestro caso en particular nos referiremos a aquellos bienes que son protegidos ante el cometimiento del Delito de Hurto por medios informáticos, encontrando así que en el artículo 1 inciso 1°, se establece que: *"El Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común"*[23]*;* Por lo tanto, el Estado como garante de justicia, seguridad jurídica y bien común, debe brindar especial protección a los ciudadanos, debido a la diversidad de actividades

[23]Constitución de la República (El Salvador, Asamblea Legislativa, 1983) Art. 1

delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, cuyo daño representa severas repercusiones en materia social, política, económica y el desarrollo tecnológico.

Asimismo, el artículo 2 inc. 2° Cn., regula el derecho a la *intimidad*, estableciendo que: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*[24]*;* por ello decimos que como ciudadanos contamos con protección constitucional de la información o datos que almacenamos en dispositivos de almacenamiento de información, pues de conformidad a reiterada jurisprudencia de la Sala de lo Constitucional de la Corte Suprema de Justicia, dicha intimidad se expresa en diversas facetas de la persona[25]:

"A fin de profundizar en el concepto de intimidad, cabe señalar cierta postura que se puede calificar de "funcionalista", la cual parte de que el interés protegido por la intimidad es el de limitar el acceso de extraños a la vida privada, individual y familiar, en el sentido más amplio. Desde esta perspectiva, el concepto de intimidad estaría integrado por tres elementos: el secreto, el anonimato y la soledad. La intimidad, entonces, se podría afectar por una alteración de cualquiera de dichos elementos. Con base en lo anterior, se afirma que la intimidad cumple las siguientes funciones: (i) restringe el acceso físico de otros; (ii) promueve la libertad de actuar, en la medida en que protege al individuo de reacciones hostiles de los demás; (iii) contribuye al aprendizaje, creatividad y autonomía, al evitar que el individuo sea ridiculizado, censurado o recriminado; (iv) promueve la salud mental, ya que otorga a las personas un reducto exento de las presiones sociales; (v) favorece la autonomía moral, que

[24] Ibíd.
[25]Sala de lo Constitucional de la Corte Suprema de Justicia. 91-2007. Inconstitucionalidad. San Salvador, a las quince horas con cincuenta minutos del día veinticuatro de septiembre de dos mil diez.

sólo se puede desarrollar plenamente en la esfera íntima del sujeto; (vi) fomenta las relaciones humanas, pues la intimidad es el punto de partida para su establecimiento y mantenimiento; y (vii) permite a los individuos decidir en qué cantidad y en qué circunstancias exponen sus datos personales".

Sobre lo anterior, continúa diciendo en esa Sentencia la Honorable Sala de lo Constitucional:

"Pues bien, se puede entender que la intimidad afecta dos esferas: (i) la esfera íntima, que comprende la faceta sexual, mental y sentimental de las personas. Afectan esta esfera los datos relativos a la enfermedad, nacimiento, muerte, vida sexual y desnudez de los individuos. Como es natural, esta esfera debe gozar de la máxima protección legal; (ii) la esfera privada, que trasciende la interioridad del individuo, refiriéndose a su círculo de parientes, amigos y conocidos cercanos. Aquí evidentemente también debe existir tutela, aunque menos intensa que en el anterior ámbito. Pero una vez se ingresa al ámbito social o público, referido a las relaciones sociales de las personas, se cae fuera del campo del derecho a la intimidad.

En conclusión, el derecho a la intimidad es un derecho fundamental estatuido directamente en el art. 2 inciso 2° Cn., del que son titulares todas las personas, consistente en la preservación de la esfera estrictamente interna y de la privada (que incluye a la familia) frente a intromisiones no consentidas del Estado o de otros particulares. Por lo tanto, la violación por excelencia - no la única- en la dinámica de las sociedades actuales, al derecho a la intimidad, es la obtención y/o revelación indeseada por parte de terceros, de datos o informaciones comprendidas en dichas esferas".

De lo mencionado por la Sala de lo Constitucional, es importante aclarar que en los delitos informáticos, el bien jurídico a protegerse es diverso pues en algunos casos es el patrimonio, poniendo énfasis en que la mayor parte de las

conductas surgidas a través de un medio informático, han tenido como finalidad perjudicar económicamente a las empresas o personas, pero por otro lado tenemos que si se trata de la información concentrada en un banco de datos personales, al cual se accede para alterar la información, o para obtenerla maliciosamente, dicha conducta debería estar entre las que protegen la intimidad tanto individual como familiar.

Cuando se trata de buscar el bien jurídico que corresponda a la información, se está tratando de seguir los caminos ya recorridos sin tomar en consideración un hecho innegable y es que se trata de un fenómeno que existía pero que en el momento en que se redactó el Código Penal vigente, no tenía mayor relevancia como la tiene al día de ahora.

Por otra parte, no se puede ignorar que la acción cometida a través de los ordenadores afecta o hace uso de la información contenida en la parte lógica del mismo, en ese sentido la información es la lesionada, .y es a través de esa información obtenida o manejada que se lesionan ciertos intereses penalmente protegidos, en el delito de hurto por medio informático se debe, tener presente que el objeto de la conducta, es la información, pero no la cosa tangible, no el bien material en sí, por esa razón es que no se puede comprender que la conducta ejecutada a través de la Informática, encaje en los tipos penales tradicionales, sin que por lo menos se reformen dichos tipos penales ampliándolos o configurando otros.

Por la razón anterior, para este tipo de delitos se exige que se establezca un tipo penal que contenga los elementos relacionados con la informática; de lo contrario, por falta de tipicidad, sería imposible proteger penalmente ciertos derechos garantizados por el Estado como fundamentales para el individuo o para la sociedad, como la protección del derecho a la intimidad, pues nos parece que cualquier legislación penal que pretenda criminalizar las conductas

cometidas a través de medios Informáticos, debe inspirarse necesariamente en los aspectos siguientes:

Se debe destacar que lo que se pretende proteger es la "información" en general, cualquier clase de información que se encuentre automatizada, o tenga como sede los bancos de datos.

Se debe concretar cuáles son los objetos jurídicos que se pretenden proteger. Si la "información" está referida a las personas en particular, es indudable que se debe proteger la "intimidad", en el sentido que anteriormente lo explicamos, pero si la "información" contiene manifestaciones económicas, entonces se acepta que la protección está dirigida a la defensa del patrimonio en general; y si la "información" tiene como contenido elementos que inciden en la seguridad nacional, entonces la protección está dirigida a la seguridad del Estado, sea esta interna o externa.

Se debe recordar que, en cuanto al objeto material de las infracciones cometidas a través de la Informática, dicho objeto está constituido por elementos intangibles, como es la información, lo que hace muy difícil que la conducta lesiva pueda adecuarse a cualquiera de los tipos que contienen las actuales leyes penales, redactadas antes que el fenómeno informático aprehendiera la mayor parte de las actividades sociales e individuales.

Se hace presente que la protección a la información debe extenderse no sólo al producto ya elaborado sino en todas y cada una de las etapas de su conformación, pues, de lo contrario, quedarían sin protección una o más fases de desarrollo o tratamiento, lo que podría ser de graves consecuencias sociales o individuales.

Que al tipificar la conducta que afecte al derecho a la intimidad se debe tener presente que este es "el derecho que tienen los individuos, los grupos, o las

instituciones, de determinar por su cuenta, cómo y en qué medida las informaciones que les atañen pueden ser comunicadas a otras personas".

En ese sentido la protección de los datos personales que se hayan automatizado electrónicamente debe comprender cuatro fases principales, a saber: a) la recopilación de los datos; b) el procesamiento de los mismos (comparación, agregación, análisis finalizado); c) el resultado obtenido y puesto a disposición, y d) su transmisión en redes informáticas y su difusión, pues la recopilación de los datos debe estar limitada, en cuanto se refieran a los datos públicos, como el derecho a no obtener los datos privados.

Los datos deben ser verdaderos, completos, obtenidos mediante medios lícitos y para fines concretos, ya que el procesamiento debe garantizar el respeto al secreto de los datos obtenidos, concediendo la respectiva seguridad de que no serán difundidos, ni alterados, ni suprimidos por personas que no hubieren sido autorizadas para su respectivo procesamiento. En lo que se refiere al resultado del procesamiento, ha de ponerse de relieve que es en esta fase en la que la libertad informática toma consistencia como derecho de control sobre los propios datos personales.

3.1.1 Código Penal de El Salvador

El Código Penal vigente incluye algunos delitos que contemplan a las Tecnologías de la Información y las Comunicaciones como medio para realizar una conducta típica, es decir, son utilizadas como herramientas para la comisión del hecho punible, pero no regula a los delitos informáticos propiamente, ni establece normas de carácter procesal para el abordaje y tratamiento de los mismos. Es por ello, y a raíz de la necesidad de regular esta problemática que en julio de dos mil diez, el Diputado en ese entonces Douglas Avilés, presentó un proyecto de reforma del Código Penal, con el fin que se incorporará el Título VI BIS, denominado: "De los delitos relativos a la

protección de la información y los datos", incluyendo estos delitos en un solo título, y proponiendo además como medida alterna la emisión de una Ley Especial sobre Delitos Informáticos, tomando como referente los países de Colombia y Venezuela, cuyo expediente legislativo ingresó a la Comisión de Legislación y Puntos Constitucionales, bajo la referencia número 858-7-2010-1, para su análisis y estudio pero que a petición de la misma Comisión y dada la complejidad del asunto se decidió trasladar el referido proyecto a la Comisión de Seguridad Pública y Combate a la Narcoactividad de la Asamblea Legislativa, donde se solicitó la opinión técnica de varias instituciones, entre ellas la Fiscalía General de la República a través del Fiscal General, concluyéndose la necesidad de crear un Anteproyecto de la Ley Especial contra Delitos Informáticos y Conexos (ALECDIC).

Tomando en cuenta que la creación de esta Ley requería de un análisis profundo en cuanto al tema del desarrollo investigativo se termina optando por someter la formulación de dicho proyecto a un consultor internacional, quien cumple efectivamente su labor, proponiendo un proyecto de Ley bastante integral, del cual se puede destacar más allá de la parte especial que toda Ley en materia penal debe contener, proponía además un apartado que establecía medidas preventivas en materia de delitos pornográficos y reglas de responsabilidad para las empresas prestadoras de servicios de red y similares, asimismo, ofrecía regular la producción, preservación y divulgación de datos, entre otras cosas; pero que al final la misma Comisión de Seguridad Pública y Combate a la Narcoactividad, decidió someter el análisis y conocimiento del proyecto de Ley a un equipo interinstitucional, por considerar que el anterior proyecto por haber sido elaborado por un consultor internacional incluía términos que no se ajustaban a nuestra legislación y contexto.

Dicho equipo estuvo conformado por instituciones como el Ministerio de Justicia y Seguridad Pública, Fiscalía General de la República, el Consejo

Nacional de la Niñez y la Adolescencia, la Superintendencia General de Electricidad y Telecomunicaciones, incluyendo a las diferentes empresas que prestan servicios de red y similares; y es el proyecto de Ley propuesto por este equipo interinstitucional el que termina siendo tomado en cuenta para la creación de la vigente Ley Especial contra Delitos Informáticos y Conexos, que se crea y entra en vigencia en el año de dos mil dieciséis[26].

Del articulado del Código Penal merece la pena salvar al delito de hurto, contemplado en el Art. 207 del mismo cuerpo normativo, el cual a pesar de tratarse de un delito simple, sirve de base para la tipificación del hurto por medios informáticos regulado en la Ley Especial contra Delitos Informáticos y Conexos (Art. 13 LECDIC), pues su estructura conserva los elementos propios del hurto simple, con la particularidad o condición del uso de las tecnologías y la comunicación para la comisión del mismo.

3.1.2 Código Procesal Penal

Este código tampoco proporciona un tratamiento o regulación para los delitos informáticos propiamente, pero determina que ninguna persona podrá ser condenada a una pena ni sometida a una medida de seguridad sino es mediante una sentencia firme, dictada en juicio oral y público, de conformidad a los principios, garantías y derechos previstos para las personas (Art. 1 CPP) es decir, sin previo juicio; y para tal finalidad establece la obtención y resguardo de información electrónica (Art. 201 CPP) que será utilizada cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, pudiendo el fiscal asignado al caso solicitar autorización judicial para adoptar las medidas que garanticen la

[26]Expediente legislativo N° 858--2010-1

obtención, resguardo o almacenamiento de la información, lo cual es aplicable a la comisión de delitos informáticos, la referida disposición legal es una innovación producto del avance tecnológico, en el que se orienta a facilitar algunas de las actividades del ser humano con instrumentos de almacenamiento de información; aunado a lo anterior, debemos destacar la figura del perito (Art. 226 CPP) quien será nombrado por el juez o tribunal competente para intervenir en determinados procesos, a efecto de descubrir o valorar elementos de prueba, cuando sea necesario y/o conveniente poseer conocimientos especiales en alguna ciencia, arte o técnica en específico.

La prueba pericial es de suma importancia en la investigación, debido al desarrollo de la tecnología y la sofisticación con la que se cometen estas nuevas modalidades delictivas y dada la necesidad de hacer frente a las organizaciones criminales que cometen estas conductas, facilitando así la labor de administrar justicia, especialmente la labor de la Fiscalía General de la República, a quien le corresponde el monopolio y dirección de la investigación del delito, en cooperación con la Policía Nacional Civil, a su vez le corresponde la recolección de pruebas pertinentes para fundamentar el ejercicio de la acción penal ante los Tribunales respectivos, así como velar porque la institución cuente con recursos tecnológicos que optimicen la prestación de sus servicios.

3.1.3 Ley Especial Contra Delitos Informáticos y Conexos

Como ya se dijo, la LECDIC es creada y entra en vigencia en el año de dos mil dieciséis, dada la relevancia adquirida por los instrumentos electrónicos mediante los que se envía, recibe o resguarda la información, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país, y por ende, debe el Estado priorizar y proteger dicha información, ya que, al no protegerla se estaría atentando contra la confidencialidad, integridad, seguridad y disponibilidad de los datos.

En la parte general de la LECDIC, se encuentra que la misma tiene como objeto proteger los bienes jurídicos tutelados de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de la información y datos almacenados, procesados o transferidos. Siendo aplicable a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También, a cualquier persona natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de igual manera será aplicable si la ejecución del hecho, se inició en territorio extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por Tribunales extranjeros o ha evadido el juzgamiento o la condena.

Para efectos de esta Ley, entenderemos por Delito Informático, la comisión de un delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información; por otra parte, el Bien Jurídico Protegido es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros; otra definición importante es la de Tecnologías de la Información y la Comunicación, siendo estas el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros.

El Art. 13 LECDIC, regula el Hurto por medios informáticos, tipificándolo de la siguiente manera: *"El que por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años"*, Siendo este la base principal de nuestra investigación, el cual además hemos analizado de manera más detenida en el capítulo anterior, pero siempre considerando los elementos propios del delito que la misma Ley le ha otorgado.

3.2 Legislación Internacional

En cuanto a tratados y/o convenios internacionales suscritos por El Salvador en materia de delitos informáticos, a pesar de contar con una normativa especial que regula dichos delitos, advertimos que no existen convenios dedicados especialmente al tratamiento y persecución de los delitos informáticos, sin embargo, podemos mencionar algunos que pueden ser de gran ayuda para regular y tipificar dichos delitos en nuestro país, siendo estos los siguiente:

3.2.1 Tratado de Asistencia Legal Mutua en Asuntos Penales entre las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá

Este es un tratado que procura la asistencia legal en asuntos penales relacionados con cualquier hecho punible tipificado tanto en el Estado requirente como en el Estado requerido, dicha asistencia abarca la recepción de declaraciones testimoniales, la obtención y ejecución de medios de prueba, la notificación de resoluciones judiciales y otros documentos emanados de autoridad competente, la ejecución de medidas cautelares, la localización de personas, y cualquier otra asistencia legal acordada entre dos o más Estados contratantes.

3.2.2 Convenio sobre la Ciberdelincuencia

Este convenio es también conocido como Convenio de Budapest, suscrito en la ciudad de Hungría, el día 23 de noviembre de 2001, por el Comité de Ministros del Consejo de Europa, es importante mencionar que el referido Convenio no ha sido ratificado ni suscrito por El Salvador, pero en la actualidad existe la iniciativa y la intención de adoptar un marco penal común basado en el presente convenio, el cual está encaminado a la protección de la sociedad contra la delincuencia informática y el fomento de la cooperación internacional en materia de seguridad cibernética; es por ello que los días 1 y 2 de julio se llevó a cabo una misión consultiva y un taller sobre legislación en delitos cibernéticos, prueba electrónica y el Convenio de Budapest, la cual tuvo como sede la ciudad de San Salvador.

La reunión contó con la participación de los parlamentarios de los países de: Honduras, Costa Rica, México, Guatemala, Belice y Diputados de El Salvador, en el desarrollo de la reunión, el Secretario Ejecutivo del Foro de Presidentes de Poderes Legislativos de Centroamérica, la Cuenca del Caribe y México (FOPREL) instó a la Comisión Interparlamentaria de Seguridad Ciudadana y Administración de Justicia (CISCAJ) a continuar trabajando en el proceso de armonización legislativa en materia de ciberdelito y a promover y apoyar desde los poderes legislativos de los países miembros de este organismo, la adhesión al convenio de Budapest sobre ciberdelincuencia.

En el último día del encuentro, los representantes parlamentarios firmaron una carta compromiso a fin de intensificar esfuerzos a favor de la integración del tema de ciberdelito y prueba electrónica, en las agendas de cada país, así como priorizar ante los Presidentes de los Poderes Legislativos, integrantes del FOPREL, la solicitud de adhesión al convenio de Budapest, en aquellos países que aún no lo han suscrito y elaborar leyes armonizadas, ya que con esto se garantizaría un mejor tratamiento a este tipo de delitos.

El convenio fue celebrado a nivel del Consejo de Europa, pero no existe ningún impedimento legal para que otros países puedan suscribirlo y ratificarlo, al contrario, es considerado como referente y primer tratado internacional que busca hacer frente a los delitos informáticos, mediante la armonización de leyes Nacionales, por lo que consideramos pertinente dar a conocer las generalidades y abordar los aspectos específicos del Convenio, que a nuestro criterio resultarían beneficiosos para complementar y suplir las Leyes relativas a la problemática de los delitos informáticos existentes en nuestro país.

Expresado de otra manera, lo antes expresado es importante hacer énfasis en que este convenio sirve como un instrumento internacional que lo que busca es homogenizar la manera en que los diversos países contratantes abordan y definen la cibercriminalidad, sirviendo como un tratado internacional vinculante en materia pena que establece herramientas legales para perseguir penalmente aquellos delitos cometidos ya sea en contra de sistemas o medios informáticos o mediante el uso de los mismos.

Este convenio nació en vista de la necesidad prioritaria de aplicar una política penal común entre sus miembros, así como de mejorar la cooperación internacional entre ellos con el fin de proteger a la sociedad frente a la ciberdelincuencia.

La política penal común implica otorgarle a los Estados signatarios del Convenio la facultad de detectar, investigar y sancionar aquellas conductas que ponen en peligro los sistemas, redes y datos informáticos con el fin de poder proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.

Al tratarse de un instrumento internacional que busca homogenizar la manera en que los países contratantes abordan y definen la cibercriminalidad o ser el marco de referencia, este incorpora de manera amplia, vaga y general las

conductas mínimas que cada Estado deberá criminalizar en su derecho interno para combatir este fenómeno, el problema aquí es que no todos los Estados parten de los mismos contextos, ni enfrentan los mismos obstáculos, por eso es que el convenio de Budapest busca implementar nuevos tipos penales así como el establecimiento de facultades de investigación más robustas para que los Estados puedan perseguir a los ciberdelincuentes.

En si este convenio cuenta con cuatro capítulos en los que además de definirse una serie de términos o conceptos en común se establecen tres ejes esenciales para hacer frente a estos delitos, el primer eje de esta tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática al definir diversos delitos que se clasifican en cuatro categorías que son:1) Delitos que tienen a la tecnología como fin, dentro de los cuales encontramos todos aquellos delitos que atentan contra la confidencialidad, integridad o disponibilidad de la información o de los datos; 2) Delitos que tienen a la tecnología como medio: refiriéndose a aquellos delitos que ya se conocen pues se cometen a través de un sistema informático, son delitos comunes que se encuentran tipificados en la mayoría de legislaciones, pero ampliados a los medios digitales; 3) Delitos relacionados con el contenido: este establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil, y; 4) Delitos relacionados a la propiedad intelectual: refiriéndose estos a la reproducción y difusión en internet de contenido protegido por derechos de autor sin la debida autorización.

En el segundo eje encontramos que lo que el convenio busca es establecer conforme al derecho procesal penal de cada país las facultades necesarias para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico. Entre otras cosas

determina la obtención y conservación de datos digitales para ser utilizados como pruebas; como tercer eje vemos un apartado que contiene las normas de cooperación internacional, es decir, establece un régimen rápido y eficaz de reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras disposiciones, la localización de sospechosos, la recolección o envío de evidencia digital, así como lo referente a extradición.

Para efectos de la investigación, se toman en cuenta dos puntos que son los que merecen especial atención, por su utilidad y pertinencia, para efectos del tema de investigación. El primer punto es el concerniente al tratamiento y abordaje de la Parte procesal, el cual se encuentra desarrollado a partir de los artículos del 14 al 22 del Convenio Contra la Ciberdelincuencia, conocido como Convenio de Budapest, disposiciones de las que se resalta el ámbito de aplicación, la parte referente a la conservación rápida de datos informáticos almacenados, el registro y confiscación de datos informáticos almacenados, la intercepción de datos relativos al contenido, y lo pertinente a la jurisdicción; el segundo punto, es el referente a la cooperación internacional, el cual se encuentra estipulado en los artículos del 23 al 34 también del Convenio Contra la Ciberdelincuencia, conocido como Convenio de Budapest, iniciando con los principios aplicables, procedimientos relativos a solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables, confidencialidad y restricciones de uso, disposiciones específicas, revelación de datos almacenados, entre otros.

Para el primer punto que se mencionó anteriormente es importante destacar que en el capítulo dos de dicho convenio referente a la parte procesal hay que determinar que el alcance de este apartado va más allá del catálogo de delitos definidos en la Sección 1 del mismo Convenio, ya que, se aplica a cualquier delito cometido por medio de un sistema informático o a las pruebas que se

encuentren en formato electrónico, a continuación, establece las siguientes disposiciones procesales: La conservación rápida de los datos informáticos almacenados; la conservación y revelación parcial rápida de los datos relativos al tráfico; la orden de presentación; el registro y la confiscación de los datos informáticos almacenados; la obtención en tiempo real de los datos relativos al tráfico, y; la interceptación de datos relativos al contenido.

Los artículos de esta Sección describen algunas medidas procesales que deben adoptarse a nivel nacional con el fin de facilitar la investigación penal de los delitos establecidos en la Sección 1, otros delitos cometidos por medio de un sistema informático y la obtención de pruebas en formato electrónico relativas a un tipo penal. De conformidad con el Artículo 39, párrafo 3, nada en el Convenio requiere o invita a una Parte a establecer facultades o procedimientos distintos a los que figuran en el presente Convenio, ni impide que una Parte los establezca.

Uno de los principales desafíos que se plantean en la lucha contra los delitos que se cometen en el entorno de las redes interconectadas es la dificultad para identificar al autor del delito y para estimar la magnitud y el impacto del acto delictivo. Otro problema obedece a la velocidad de la transferencia o transmisión de los datos electrónicos, que pueden ser alterados, movidos o borrados en cuestión de segundos. Por ejemplo, un usuario que tiene el control de los datos puede utilizar el sistema informático para borrar datos que son objeto de una investigación penal, destruyendo así las pruebas.

El Convenio de Budapest o Convenio Contra la Ciberdelincuencia, adapta las medidas procesales tradicionales, tales como el registro y confiscación, al nuevo entorno tecnológico. Además, se han creado nuevas medidas, tales como la conservación rápida de los datos, con el fin de garantizar que las medidas tradicionales para obtener información, tales como el registro y la

confiscación, seguirán siendo eficaces en el ligero entorno tecnológico. Además, se han adaptado otros procedimientos tradicionales de obtención de información pertinentes para las telecomunicaciones, tales como la obtención e interceptación de los datos en tiempo real, con el fin de permitir la obtención de datos electrónicos que se encuentren en el proceso de la comunicación.

Por otra parte, el capítulo tres del convenio de Budapest, establece la cooperación internacional que dicho de otra manera es la que contiene todas las disposiciones relativas a la asistencia jurídica mutua entre las partes en relación con los delitos tradicionales y con los delitos relacionados con la informática, así como también las referentes a la extradición. Da cuenta de la asistencia mutua tradicional en dos situaciones: cuando entre las partes no existen fundamentos jurídicos (tratados, leyes de reciprocidad, etc.) en cuyo caso corresponde aplicar sus disposiciones; y cuando existe dicha base, en cuyo caso los acuerdos existentes también se aplican a la asistencia que se concede en virtud del presente Convenio.

La asistencia específica en materia de delitos informáticos o de delitos relacionados con la informática se aplica a ambas situaciones y abarca la misma serie de facultades procesales definidas en el Capítulo II. Por otra parte, el Capítulo III, del Convenio de Budapest, contiene una disposición acerca de un tipo específico de acceso transfronterizo a datos informáticos almacenados, que no requiere la asistencia mutua (cuando media un consentimiento o cuando están disponibles públicamente) y prevé el establecimiento de una red que funcione las 24 horas del día los 7 días de la semana con el fin de asegurar una asistencia rápida entre las Partes.

El Convenio de Budapest en su Artículo 23 establece tres principios generales relativos a la cooperación internacional en el marco del Capítulo III. Éste inicia señalando que las Partes cooperarán entre sí "en la mayor medida posible".

Este principio exige que las Partes se brinden una amplia cooperación recíproca, y que reduzcan al mínimo los impedimentos a la circulación fluida y rápida de la información y las pruebas a nivel internacional. A continuación, establece el alcance general de la obligación de cooperar: "la cooperación abarcará todos los delitos penales relacionados con sistemas y datos informáticos y también la obtención de pruebas en formato electrónico de los delitos". Esto quiere decir que los términos del capítulo III son aplicables tanto cuando un delito se comete utilizando un sistema informático, o cuando un delito común que no se ha cometido mediante el uso de un sistema informático (por ejemplo, un asesinato) pero involucra pruebas electrónicas.

Por último, se establece que la cooperación se llevará a cabo "de conformidad con las disposiciones del Capítulo e mención" y "en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca, y de su propio derecho interno". Esta última cláusula establece el principio general de que las disposiciones del Capítulo III del Convenio de Budapest, no reemplazan las disposiciones de los acuerdos internacionales en materia de asistencia jurídica mutua y extradición, los acuerdos de reciprocidad entre las partes o las disposiciones pertinentes del derecho interno de cada país en materia de cooperación internacional.

Si bien es cierto el Convenio sobre la Ciberdelincuencia, no tipifica un delito que contenga los elementos propios del hurto por medios informáticos, pero en su Art. 14 establece que cada Estado parte deberá adoptar las medidas necesarias para plasmar las facultades y procedimientos previstos en el mismo, los cuales no se limitan estrictamente a los delitos regulados en el Convenio, sino que permite aplicarlos a cualquier delito cometido a través de un sistema informático, lo que implica que con toda libertad podríamos aplicar las disposiciones del Convenio a la legislación penal Salvadoreña, y de

manera particular a la vigente Ley Especial contra Delitos Informáticos y Conexos, la cual carece de disposiciones que regulen la parte Procesal relacionada a estos delitos, el tratamiento de la prueba informática, y aspectos relacionados a la cooperación internacional.

CAPITULO IV

REGIMEN PROBATORIO PERICIAL

El presente capitulo tiene como propósito establecer la falta de regulación probatoria de los delitos informáticos en El Salvador de forma general, para lograr con ello determinar si la prueba pericial es el medio de prueba pertinente para demostrar que una conducta puede ser considerada como punible en el delito de hurto por medios informáticos, estableciendo con ello la naturaleza jurídica y científica de la labor pericial en el ámbito de conocimiento e intervención del perito informático y su capacitación en las diversas instituciones de nuestro país.

4. Generalidades de la prueba

Una vez hecho un análisis acerca de la regulación nacional e internacional en relación a los delitos informáticos de forma general y en particular del delito de hurto por medios informáticos, hay que hacer énfasis que en El Salvador existe una Ley Especial Contra Delitos Informáticos y Conexos donde se regula el delito pero esta Ley no cuenta con una parte procesal ni probatoria en relación a este tipo de delitos, en ese sentido lo que se pretende es determinar si la prueba pericial es el medio de prueba pertinente para demostrar el delito de hurto por medios informáticos como conducta delictiva.

Para tal efecto se realizó una entrevista en la División de la Policía Técnica y Científica de la Policía Nacional Civil, debido a que esta institución es la encarga de brindar la experticia y recurso técnico y científico a la Fiscalía General de la Republica en la persecución de los delitos, por ser la única institución que cuenta con una Unidad de Delitos Informáticos, en la entrevista se externaron las limitantes con las que se enfrenta la División de la Policía Técnica y Científica de la Policía Nacional Civil al combatir el fenómeno de la

Delincuencia Informática, que va más allá de problemas de interpretación de los tipos penales, así como de las diversas dificultades operativas frecuentes.

Es importante establecer que por prueba vamos a entender a aquella actividad desarrollada por las partes que pretende convencer psicológicamente al juez de la veracidad o falsedad de las afirmaciones de hecho efectuadas por ellas, debiendo el juez decidir de acuerdo con las reglas de la sana critica, la prueba tasada y la libre convicción.

De lo antes mencionado se establece que los hechos y circunstancias sobre la existencia de un delito y la participación delincuencial se pueden probar por cualquier medio, debido a la libertad procesal con la que cuenta cada una de las partes en el proceso, sin embargo esta prueba carece de valor cuando es obtenida mediante tortura, amenaza, violación de los derechos fundamentales de la persona o en virtud de información originada en un procedimiento o medio ilícito, en ese sentido únicamente tendrán valor aquellas pruebas que fueron obtenidas unicamente por medios lícitos y practicadas ante los diversos organismos jurisdiccionales, respetando de esa manera, los derechos y garantías fundamentales que están establecidos en la Constitución y demás leyes, para ser admitidas, de lo contrario su consecuencia, por lo general es la nulidad del acto y todo aquello que está relacionado con él.

Para que un medio de prueba sea admitido debe haber sido obtenido, ofrecido e introducido, conforme a las reglas establecidas en el Código Procesal Penal, una vez admitida la prueba, ésta se valorara para determinar la eficacia o la influencia que los elementos probatorios aportados a través de los medios de prueba, tendrán en la formación de la convicción del juez, por lo tanto esta valoración será una actividad intelectual que corresponde únicamente al órgano jurisdiccional, ya que mediante esta valoración de la prueba, el juez depura los resultados obtenidos en la práctica de los diferentes medios de

prueba, relacionándolos unos con otros para llegar finalmente a formar su convencimiento, esta valoración puede realizarse a través de tres sistemas que son: 1. La prueba legal o tasada; 2. La libre convicción o prueba libre y; 3. La sana critica.

La sana critica se entiende como aquel “conjunto de normas directamente relacionadas con el entendimiento humano en las que se complementan las reglas de la lógica, la psicología y la experiencia del juez”, en ese sentido vamos a entender que la sana critica es aquella que le permite al juez analizar cualquier tipo de prueba, que posteriormente se ve reflejado en la sentencia dictada por el tribunal, asegurando así que exista una conexión lógica entre el hecho de probar y el medio de prueba, y que la evidencia admitida durante el juicio oral respalde la convicción del juez.

Gracias a la sana critica es que los jueces son libres de valorar la prueba rigiéndose únicamente por el razonamiento lógico, la rectitud, la imparcialidad y el deber de motivar o fundamentar su resolución, esto sin dejar de lado los requisitos sobre la carga de la prueba.

4.1 Prueba pericial

Uno de los problemas respecto al contenido, alcances y límites del peritaje, se debe a que en El Salvador no existen “Reglas de Evidencia”, entendidas éstas como reglas claras y precisas para admitir o rechazar los medios y elementos de prueba ofrecidos, independientemente de su valoración posterior por el Juez o Tribunal. Lo que ha generado un amplio margen de actuación, no solo a los peritos con sus dictámenes, sino a los abogados al momento de ofrecer o impugnar la prueba (fiscales y defensores) pero especialmente a los Jueces.

4.1.1 Concepto

Para nuestra investigación es de vital importancia hacer énfasis en la prueba pericial, en virtud de determinar si esta es el medio de prueba pertinente para

establecer el delito de Hurto por medios Informáticos como conducta punible, en ese sentido, entenderemos que la prueba pericial es aquella prueba *"utilizada cuando son necesarios los conocimientos científicos, artísticos, técnicos o prácticos de los que en principio el juez puede carecer, es decir que es una prueba que se realiza interviniendo el perito como auxiliar del juez, por faltarle o poderle faltar, a este las posibilidades técnicas de realizarla eficazmente"*[27].

La pericia viene a constituir un auxilio judicial para suplir la ausencia de conocimientos científicos o culturales de los jueces y ayudarlo a constatar la realidad no captable directamente por los sentidos o a interpretar esa realidad.

La pericia consiste en auxiliar a las partes y al juez en la búsqueda de La "verdad" material del hecho investigado. Ante el indicio o evidencia material, el perito debe seguir los siguientes pasos: identificar el indicio (describirlo e individualizarlo), compararlo (el espécimen de comparación con el espécimen de referencia) y sacar sus conclusiones. Conclusiones que pueden ser sin márgenes de error o con márgenes de error. Y en la práctica, el perito tiene libertad en la identificación del método de comparación (aunque se encuentran institucionalmente estandarizados) pero las conclusiones del perito son personales.

4.1.2 Deberes del Perito

Hay que establecer que los principales deberes que tiene el perito están: 1. Ser objetivo y ajeno completamente al proceso en el cual se le requiere su participación; 2. Ser una persona imparcial y sin intereses particulares; 3. Poseer los conocimientos, la experiencia y la formación teórica práctica como experto en la materia; 4. Rechazar cualquier proceso que le sea imputado por coacción y no pueda ejercer de manera voluntaria; 5. Aceptar el cargo que le

[27] Francesco Carnelutti, La prueba civil (Buenos Aires: De palma 2° edición, 2000), 84.

es asignado, colaborar con los asesores jurídicos y el resto de los peritos o consultores técnicos, declarar ante el juez en el caso de que este lo requiera, bajo juramento; 6. Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas, y; 7. Respetar el código de ética que le impone su profesión[28].

4.1.3 La Cadena de Custodia

Otro eje que debe tenerse presente respecto de la pericia, es el aseguramiento de la calidad de la misma, es decir, el proceso mediante el cual se garantiza al solicitante de una pericia, que el dictamen pericial otorgado por el científico forense satisface una serie de requisitos que no permiten que sea cuestionado más allá de la duda razonable, pues si bien puede garantizarse la calidad técnica y científica, debe garantizarse además la "cadena de custodia de la prueba"[29]. Si bien el perito no es el responsable de toda la cadena de custodia, sí lo es desde que recibe el indicio hasta que lo entrega o devuelve, por lo que debe asegurar la cadena de custodia interna dentro de la Institución.

En la práctica del peritaje, se deben garantizar que los procedimientos eviten en lo posible transferencias entre dos fuentes diferentes (contaminación), que el indicio no sea o esté "alterado", debe llevarse un registro cuidadoso y permanente de todas las operaciones durante la pericia y llevar una documentación de los métodos y procedimientos de análisis.

La bitácora no constituye el dictamen pericial en sí, sino que esta constituye el registro y documentación que sustenta dicho dictamen. Es determinante respecto al aseguramiento de la calidad de la pericia, además, de que existan

[28] Escuela Técnica Superior de Ingeniería Informática, Universidad Politécnica de Valencia. "Guía actualizada para futuros peritos informáticos y ultimas herramientas de análisis forense digital". Acceso el 7 de septiembre de 2019. Ibid.28. http://www.pensamientopenal.com.ar/ system/fi les/2016/05/doctrina43429.pdf.
[29] Ibíd.

los establecimientos adecuados, que haya personal capacitado y diestro en cuanto a la protección del indicio y aseguramiento de la prueba, mantener cánones de seguridad y realizar auditorías, validar los métodos, calibrar y darle mantenimiento al equipo, hacer pruebas de experticias, ejecutar acciones correctivas y elaborar periódicamente informes y revisiones al respecto.

4.2 Perito Informático Forense

4.2.1 Concepto

La persona encargada para realizar el análisis informático forense es un perito informático forense o también conocido como perito informático, el cual es *"una persona experta con conocimientos especializados en determinados campos de la ciencia y conocimientos técnicos o prácticos, que transmite al juez a través del dictamen pericial, para que aquél pueda valorar hechos o circunstancias relevantes y adquiera certeza sobre los mismos, el perito debe, pues, tener conocimientos especializados de interés para el proceso y dichos conocimientos deberán acreditarse mediante un título profesional"*[30].

Las áreas de conocimiento del perito informático forense son extensas, no abarca únicamente aspectos solo del software, sino también del hardware, redes, seguridad, hacking, cracking y recuperación de información, por lo que estos requieren de una constante actualización tanto en aspectos tecnológicos y metodológicos como legales, por ello, el perito informático forense, debe ser consciente de sus limitaciones profesionales, pues es imposible ser experto en todas las ramas y especialidades y con ello abarcar todas las áreas de especialización, este a su vez debe garantizar que el resultado de su trabajo sea objetivo, metódico, demostrable, reproducible, veraz, auditable, creíble, honesto y profesional.

[30] Tesis doctoral. "La prueba electrónica: sus implicaciones en la seguridad de la empresa". Acceso el 4 de septiembre de 2019. https://www.tesisenred.net/handle/10803/285237

Es importante tener en cuenta que la disciplina que estudian este tipo de peritos es la de la informática forense pues esta disciplina tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica, la cual para el cumplimiento de sus objetivos desarrolla técnicas idóneas para identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable, es importante tener en claro que esta disciplina actúa en todo hecho dentro del que un sistema informático esté involucrado, ya sea como fin o como medio, y que pueda ser objeto de estudio y análisis, pudiéndose llevar a juicio como medio probatorio.

De todo lo anterior el perito informático forense realizara un análisis informático forense, que lo vamos a entender como la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar los datos que sean válidos dentro del proceso legal. Este análisis forense informático se deriva del peritaje, ya que es a través del peritaje que se buscan las evidencias y pruebas necesarias.

4.2.2 Tipos de análisis forense digital

Existen diversos tipos de análisis forenses como los siguientes: 1. Análisis forense de redes (nube); 2. Análisis forense de las computadoras (laptops); 3. Análisis forense dispositivos los dispositivos móviles (celulares); 4. Análisis forense de malware (virus), y; 5. Análisis forense de inalámbricos (Wireless).

4.2.3 Ámbito de actuación Judicial

En el ámbito judicial, el perito informático forense, es un experto designado por la autoridad del proceso judicial, es decir, por el Juez, para que, mediante la investigación especializada en materia informática y en base a los diversos requerimientos exigidos, dictamine con objetividad, honestidad, imparcialidad y veracidad, las conclusiones de su pericia mediante un dictamen pericial.

El resultado de su investigación es aportado en función de la localización de las evidencias digitales, las herramientas utilizadas para el análisis forense, los métodos y normas aplicadas en relación a su desempeño como experto en la materia.

En muchos países se ha podido establecer por medio del Órgano Judicial como por parte de los abogados lo importante e imprescindible que resulta la localización de las evidencias digitales, que sirven de apoyo para el esclarecimiento de los diversos casos, por lo que contar con un perito informático forense es vital para el proceso, ya que su peritaje ayudara a determinar el establecimiento de una pena.

4.2.4 Fases de la Pericia Informática

La pericia informática forense, cuyo objeto es el análisis de todo tipo de material informático, está conformado por las siguientes etapas si unimos la perspectiva técnica con la jurídica:

La inspección, la cual puede ser realizada tanto de la escena física del crimen, como por ejemplo en una casa o en una oficina; y la inspección de la escena digital del crimen, por ejemplo, en un celular o en el internet, para identificar fuentes potenciales de evidencia, esta es realizada en todo dispositivo electrónico o informático que pueda haber sido utilizado para cometer el ilícito.

La recolección o adquisición, consiste en tomar y preservar la evidencia digital, el objetivo de esta fase es la preservación, es decir realizar una copia de la información digital original para examinarla sin comprometer a la información digital original, dentro de esta etapa hacemos referencia al clonado de la información y cálculo de la clave “hash” o resumen. El clonado del material informático intervenido se realiza en el lugar en el que se encuentra el dispositivo o en una diligencia posterior, mientras que el cálculo de la clave “hash” o resumen sirve únicamente para determinar el material incautado.

La robustez de la evidencia digital se refiere a la validez del método de recolección y preservación de la evidencia; así como a mantener la cadena de custodia, la evidencia debe ser recolectada sin alterar la información y esta debe ser copiada según un duplicado exacto de la información original, el análisis digital forense es único debido a que la preservación se refiere a la habilidad de realizar un duplicado de la evidencia original, y de esta forma preservar la fuente Imaging: *"es el proceso de realizar una copia exacta (bit por bit) extraída del dispositivo original y trasladada en un nuevo dispositivo de almacenamiento"*[31]. El nuevo dispositivo de almacenamiento debe estar limpio de información digital para prevenir la contaminación, para garantizar que no se realicen modificaciones a la evidencia, se utiliza un bloqueador de escritura en la fuente de la información original, el cual deja al dispositivo en un modo de solo lectura.

El análisis y examen, se trata únicamente de la emisión del dictamen pericial informático, pero para poder emitir correctamente este dictamen pericial informático se debe realizar las siguientes 2 tareas: 1. Analizar la información objeto del dictamen; 2. Documentar la pericial informática forense, dentro del cual es fundamental documentar el análisis forense informático realizado y detallar todos los pasos realizados en el mismo, a su vez es importante establecer que el trabajo del analista digital forense no es el demostrar la culpabilidad o inocencia de un sospechoso si no que su prioridad fundamental es la de garantizar la integridad de la evidencia, es decir que esta se encuentre libre de todo aquello que pueda perjudicarla, para así garantizar su legalidad.

En la presentación del dictamen pericial y su ratificación, los descubrimientos que son considerados como relevantes para la investigación son presentados en un reporte ante el juez, su pertinencia radica en su vínculo con el caso, el

[31]Oficina de las Naciones Unidas contra la droga y el delito. "Análisis Forense Digital", Ponencia dictada en el Consejo Nacional de la Judicatura, enero de 2019.

día del juicio oral, el perito informático deberá ratificar y pronunciarse sobre su dictamen, aclarando cualquier duda que le surjan a las partes o al Juez, por último, la valoración del dictamen, está sometida a la libre valoración, lo que significa que el Juez aplica las reglas de la sana crítica.

4.3 Evidencia Digital

4.3.1 Concepto

Como ya se mencionó en el capítulo dos del presente trabajo de investigación es importante volver a recalcar la diferencia que existe entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este, es decir contenida en el software (evidencia digital), distinción que es útil al momento de diseñar los diversos procedimientos adecuados para tratar cada tipo de evidencia y crear una comparación entre la escena física del crimen y la escena digital del mismo, en este sentido el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo, es necesario distinguir entre los aparatos electrónicos y la información digital que estos contengan. Esto es indispensable ya que el foco de la investigación siempre será la evidencia digital, aunque en algunos casos también serán los aparatos electrónicos.

De lo antes mencionado se establece que la evidencia digital es: “Aquel registro generado y guardado por un medio tecnológico y que es utilizado para demostrar la comisión de un delito, cuya forma de realización especialmente involucra la red, sirviendo como medio de prueba en un juicio”, dicho en

nuestras palabras, vamos a entender que las evidencias digitales son todas aquellas que están contenidas dentro de un soporte físico, que contienen información del usuario del dispositivo a analizar, y no meramente información destinada a tareas o funciones necesarias para la máquina.

4.3.2 Características

Las características principales de la evidencia digital son: 1. Es volátil, debido a que la prueba digital es mudable e inconstante por su propia naturaleza intangible, y especialmente sujeta a la posibilidad de modificación o alteración, lo que añade especial complejidad para que una prueba digital adquiera capacidad probatoria; 2. Es duplicable, porque se encuentra en formato digital, pudiéndose copiar o replicar tantas veces como se desee, con ello se plantea el problema de distinción de la originalidad, el cual se declara como trivial para su adquisición de fuerza probatoria si se puede acreditar indubitadamente que original y copia son exactos, bit a bit; 3. Es alterable y modificable, esto significa que la evidencia digital puede ser modificada y cambiada fácilmente; 4. Es eliminable, porque la prueba digital puede ser fácilmente destruida, no siendo necesaria la destrucción del soporte digital que la contiene; 5. Es Intangible, no pudiendo apreciarse directamente a través de los sentidos, sino mediante complejos procesos informáticos.

Cada una de estas características nos permiten tener un panorama más claro de cómo es la evidencia digital, lo cual nos ayuda a poder darle un mejor tratamiento a la misma y así evitar la destrucción o perdida de la información digital que se encuentre en los diversos soportes informáticos que la contengan y con ello poder obtener evidencia que sea relevante para el caso en estudio.

Normalmente esta información digital es contenida en un formato binario, a través de un sistema que transforma los impulsos eléctricos.

4.3.3 Fuentes de evidencia digital

Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos[32]: 1. Los sistemas de computación abiertos, son aquellos que están compuestos de las llamadas computadoras personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital; 2. Los sistemas de comunicación, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet, siendo también una gran fuente de información y de evidencia digital, y; 3. Los sistemas convergentes de computación, son los que están formados por los teléfonos celulares llamados inteligentes o Smartphone, los asistentes personales digitales, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

4.3.4 Tipos de evidencia digital

La evidencia digital puede clasificarse en diversos tipos como: 1. Documentos de office, Word, Excel; 2. Correos electrónicos; 3. Mensajes de texto; 4. Imágenes digitales; 5. Bases de datos; 6. Log: son los ficheros de registro de actividades; 7. Host: son las memorias, conexiones, usuarios conectados, y; 8. historial de la computadora: navegaciones y descargas.

Una vez establecidos algunos de los tipos de evidencia digital, es importante establecer en el presente trabajo de investigación que, si el investigador presume que existe algún tipo de evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una

[32]"Manual de Manejo de Evidencias Digitales y Entornos Informáticos". Acceso el 8 de septiembre de 2019. https://www.oas.org/juridico/english/cyb_pan_manual.pdf

infracción. Este debe pedir autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

Antes de realizar un allanamiento e incautación de Equipos Informáticos o Electrónicos se debe tomar en cuenta lo siguiente: 1. La hora de realización, esto para minimizar la destrucción de equipos y datos, que el sospechoso este en línea y la seguridad de los investigadores; 2. Se debe entrar sin previo aviso, utilizando seguridad y evitando la destrucción y alteración de los equipos, o la evidencia contenida en esta; 3. Los materiales a utilizar deben estar previamente preparados (cadena de custodia), embalajes de papel, etiquetas, discos y disquetes vacíos, herramientas, cámara fotográfica, entre otras; 4. Se deben realizar simultáneamente los allanamientos e incautación en diferentes sitios ya que los datos pueden estar en más de un lugar por los sistemas de red o conexiones remotas; 5. Realizar un examen del equipo; 6. Se debe realizar la creación de respaldos en el lugar, creación de imágenes de datos. (Autorización para duplicar, reproducir datos encontrados); 7. Se debe fijar o grabar la escena, los códigos o claves de acceso y contraseñas; 8. Se tiene que buscar los documentos que contienen información de acceso, conexiones en redes, etc.

4.3.5 Medios o Herramientas básicas utilizadas en la investigación de un delito informático

Cualquier información de una persona es considerada como datos personales de ésta, información que nos identifica de manera única como persona, estos datos incluyen las imágenes y los mensajes que a diario intercambiamos con familiares y amigos mediante el uso de internet, otra información, como nuestro nombre, número de seguro social, la fecha y el lugar de nacimiento o número telefónico, datos médicos, educativos, financieros y laborales, también se puede utilizar para identificarnos.

Las tecnologías de la Información y la Comunicación se han convertido en una herramienta importante y de mucha utilidad para la sociedad en nuestros días, diferentes organizaciones como instituciones médicas, financieras, educativas y gubernamentales, utilizan estas tecnologías para brindar prestaciones o servicios, utilizando los diversos sistemas informáticos para poder recopilar, procesar, almacenar y compartir la información que se encuentra dentro de los mismos.

La ciberseguridad es el esfuerzo constante por proteger los sistemas informáticos y los datos contenidos en estos contra el uso no autorizado o contra la afectación que los mismos pueden llegar a experimentar, pues si se tiene algo de valor, los ciberdelincuentes lo quieren, ya que los datos o información que nosotros podemos considerar como irrelevantes, son valiosas para ellos, por ejemplo: nuestras credenciales, ya que otorgan a los ladrones acceso a nuestras cuentas, podemos pensar que los kilómetros de viajero frecuente adquiridos no tienen valor para los delincuentes cibernéticos, pero esto debe reconsiderarse, luego de que se hackearan aproximadamente 10,000 cuentas de American Airlines y United, los delincuentes cibernéticos reservaban vuelos gratuitos y mejoras con estas credenciales robadas[33]. Pueden ser diversos los datos que los ciberdelincuentes sustraigan de los bancos de datos, razón de la importancia que tiene la ciberseguridad.

4.3.5.1 Protocolo estándar de una investigación

La finalidad de toda investigación delictiva es demostrar la participación de una o varias personas en el hecho o hechos punibles que se le imputan. La recolección de pruebas que puedan determinar y ubicar a una persona en un lugar concreto a una precisa hora es la base de toda investigación. En el caso

[33] Introducción a la Ciberseguridad. Programa en línea impartido por la OEA; Capítulo I: La necesidad de la ciberseguridad.

de delitos informáticos, los datos van a determinar el camino de un proceso penal, y para tal efecto es primordial la perfecta localización de la IP del autor[34]. Estos datos, que no son públicos, están guardados cada uno en su correspondiente servidor del proveedor de internet o servicios (ISP), en el caso de España los proveedores tienen la obligación de guardar los datos personales de sus clientes por un periodo mínimo de 2 años, en donde de existir una orden judicial debe establecerse tanto la IP afectada como su proveedor al que posteriormente se le solicitara los datos del cliente final en base a dicha orden, por tanto debe averiguarse previamente a que proveedor pertenece esa IP.

Una manera más fácil y sencilla es utilizar alguna página web que realice este trabajo por nosotros, por nuestra parte investigamos y para tal cometido recomendamos la dirección web: http://cqcounter.com/whois/; en dicha página se introduce la dirección IP y nos facilita una serie de datos, de los que merece destacar el proveedor de servicios de internet (IPS), haciendo caso omiso de la información relativa a la ubicación, ya que, esta indica la posición del servidor de internet y no el domicilio del usuario. Sin embargo, nos muestra además la dirección física del proveedor de servicios de internet donde podemos ir a solicitar la información e incluirla en la orden judicial.

4.3.5.2 Correo Electrónico

Todo correo electrónico una vez es recibido, contiene la ruta que ha seguido desde el lugar desde el que ha sido enviado, hasta el lugar en el que ha sido abierto por primera vez, estos datos no son visibles a simple vista, pero hasta los propios correos gratuitos que se visualizan a través de los distintos navegadores de internet permiten acceder a esta información. Siempre

[34]Técnicas de Investigación Criminal. 2012. Vol. 2a edición. Madrid: Dykinson. 316. Acceso el 20 de agosto de 2019. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=687491&lang=es&site=ehost-live.

tenemos que tener el email en cuestión abierto y posteriormente debemos buscar algún apartado donde nos indique ver código fuente del mensaje o ver mensaje original[35].

A continuación, se ejemplifica todo lo expresado anteriormente, para ello se exponen los correos electrónicos de mayor frecuencia en el entorno: para el caso de Gmail, se observa una flecha azul en la parte superior derecha donde se abrirá un menú desplegable y encontraremos la opción "mostrar original", aquí se nos abrirá una nueva pantalla con muchos datos; en el caso de Hotmail u Outlook como es conocido en la actualidad, encontraremos al lado de la opción de responder en la parte superior derecha una flecha que desplegará un menú donde se localizara la opción "ver código fuente del mensaje", y como en el caso de Gmail se abrirá una nueva pantalla con toda la información.

La forma de interpretar los datos obtenidos es la siguiente: en primer lugar tenemos el email del receptor, así como la IP donde ha sido abierto ese email por primera vez, a continuación nos indica los distintos servidores por lo que ha ido pasando en el caso de Gmail y Hotmail, hasta que finalmente llegamos al apartado X-Originating-IP, ésta es la dirección IP original desde donde se ha mandado el correo y por tanto la información más valiosa, el resto de información va relacionada con las fuentes y caracteres originales del mensaje, incluyendo el texto íntegro, estos datos son una base sólida de cara a solicitar una orden judicial.

Otra manera eficaz, aunque mucho más lenta es solicitar directamente al servidor de correo los datos relacionados con el tráfico de la cuenta de correo, hablando del ejemplo anterior, habría que contactar con Gmail y Hotmail, como

[35]Técnicas de Investigación Criminal. 2012. Vol. 2a edición. Madrid: Dykinson. 318. Acceso el 1 de septiembre de 2019. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=687491&lang=es&site=ehost-live

se ha indicado el proceso sería muy largo debido a que estos organismos se encuentran normalmente en el extranjero.

4.3.5.3 Páginas Web

De la misma manera que el delito puede ser cometido a través de un correo electrónico, este también puede ser perpetrado utilizando una página web; por ejemplo, mediante un comentario en un foro o una publicación en línea, etc., si la víctima es el responsable de la página web, la labor es mucho más sencilla, ya que, éste nos facilitará todos los datos necesarios. En el caso de no ser así, la investigación será más laboriosa por lo que necesitamos poseer conocimientos básicos[36].

Toda página web, entendida como tal la dirección que introducimos en la barra superior del navegador tiene una equivalencia en direcciones IP, ya que, el navegador traduce los números de la dirección IP en letras, por ejemplo, el navegador de Google, cuya dirección en su versión española es www.google.com, equivale a la IP 74.125.230.88.

La forma de averiguar cuál es la IP es a través del editor de comandos de MS-DOS, a este se accede desde cualquier sistema operativo Windows, en los sistemas operativos más recientes, y después de pulsar en INICIO, dentro del recuadro de búsqueda o buscar, introducimos directamente el comando "CMD", en la ventana nueva que nos aparecerá, veremos una línea de comando con la ruta c:\nombre usuario, a continuación escribimos la orden "ping" seguida del nombre de la página web que necesitamos conocer su IP, aquí se nos mostrarán los datos necesarios para identificar la dirección IP que necesitamos conocer.

---

[36] Técnicas de Investigación Criminal. 2012. Vol. 2a edición. Madrid: Dykinson. 32. Acceso el 3 de septiembre de 2019. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=687491&lang=es&site=ehost-live.

De todos estos datos, los más relevantes son los relacionados con la persona que dio el alta o administra el dominio, nos aparecerán direcciones de correo electrónico, direcciones físicas y teléfonos, tanto personales como profesionales, con esta información ya podemos solicitar una orden judicial de manera precisa, pudiendo incluir ambas ubicaciones, la personal y la profesional.

En el caso de este tipo de investigaciones, necesitamos la plena colaboración del administrador de sistemas o responsable del servidor, salvo que este, sea parte del proceso y esté imputado en el mismo, los datos almacenados en estos sistemas van a esclarecer las direcciones IP de terceros desde donde se han cometido los hechos.

A través de páginas web se pueden perpetrar delitos tan variados como, transferencias bancarias fraudulentas o no realizadas por su legítimo dueño, amenazas en un foro, y el delito de hurto por medios informáticos mismo, entre muchas otros.

4.3.5.4 Secuestro de Información

Una labor tan importante como la propia investigación, es la recolección de pruebas y la exposición de las mismas en el juicio oral, como en otras ramas de la investigación criminal, las pruebas se deben manipular, estudiar y analizar, para remitir un informe pericial con el resultado de las mismas. En el caso de las nuevas tecnológicas tenemos una ventaja muy importante que se debe aprovechar, todas las pruebas se encuentran recogidas en un formato el cual podemos duplicar para nuestro estudio, sin necesidad de alterar el original, en esta categoría se encuentran incluidos los discos duros, tanto internos como externos, las tarjetas de memoria de teléfonos móviles, de consolas de juegos y de cámaras fotográficas y/o de video, así como todos aquellos elementos que contengan información en formato digital.

Si algún aparato que disponga de dispositivos de almacenamiento se encuentra apagado, nunca se debe encender, por el contrario si algún aparato esta encendido, es fundamental anotar los datos que pueden ser relevantes a la hora de la investigación, ya que, pueden eliminarse cuando este se apague, por ejemplo: fecha y hora del sistema, conexiones de red que se encuentren activas, puertos que se encuentren abiertos o comunicando, archivos ejecutables activados, usuarios conectados, aplicaciones abiertas, procesos en ejecución, tareas programadas, memoria y todos los datos que consideren apropiados.

En el juicio oral y ante pruebas irrefutables, se va a cuestionar la manera de obtención de las pruebas, así como la manipulación de las mismas. En este caso podremos solventar tal situación y dejando a la defensa sin argumentos, siendo el propio secretario de actuaciones, quien dé fe del procedimiento durante el registro, obtención y manipulación de las pruebas al momento del reconocimiento judicial o secuestros de las mismas, para así evitar que se genere incertidumbre acerca del modo de obtención de los mismos.

Si el fiscal o investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento del hecho punible, éste debe solicitar la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe contar con la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos[37]. En ningún momento se podrá acceder a algún dispositivo que contenga evidencia digital sin previa autorización judicial.

[37] Dr. Santiago Acurio del Pino: "Manual de manejo de evidencias digitales y entornos informáticos". Acceso el día 13 de septiembre de 2019. https://www.oas.org/juridico/english /cyb_pan_manual.pdf.

4.3.5.5 Descifrado de contraseñas

El sistema operativo del ordenador se encarga, entre muchas funciones, de hacer invisibles e inaccesibles muchas de las contraseñas que necesitaremos, por ello, lo más recomendable es utilizar el disco a analizar como externo y liberarlo de su propio sistema.

Las maneras de acceder a la información contenida en cualquier software y que nos permita acceder a archivos encriptados son tres básicamente: 1. Por fuerza bruta, consiste en probar todas las combinaciones posibles y existentes una por una hasta encontrar la correcta; 2. Por diccionario, el programa utilizado tiene memorizadas una serie de palabra, números y combinaciones las cuales va usando hasta encontrar la correcta, y; 3. Por criptoanálisis, que consiste en descifrar la combinación o algoritmo utilizado en la contraseña durante el cifrado, de esta manera la contraseña se hace mucho más accesible para un ataque posterior por diccionario.

La mayoría del software utiliza estos métodos para aumentar su nivel de eficacia y disminuir el tiempo de espera. Los dos softwares por excelencia en este campo son "Caín y Abel" y "Man in the Middle", de modo genérico son muy útiles con una gran diversidad de archivos, todas las contraseñas de un sistema operativo Windows se almacenan es un fichero llamado SAM, el cual se aloja en ":/Windows/system32/config/", los archivos exactos son SAM y SAM.log.

Estos archivos son inaccesibles si se está trabajando desde el propio disco duro, solo de manera externa son visibles y accesibles, aunque Caín y Abel, son programas que están preparados para acceder al SAM, otros programas como ats take, LC4, SAM Inside y pass dump 3, son más eficaces en el trabajo con este tipo de archivo, ya que ellos logran obtener el acceso a las contraseñas de una manera más rápida y sin dejar evidencia alguna.

4.4 Formas usuales de cometer el delito de Hurto por medios Informáticos: Obtención de datos o claves de acceso

4.4.1 SPYWARE: Sustracción de claves de acceso sin el consentimiento del sujeto pasivo

Existen ciertas herramientas destinadas a la sustracción de datos que permiten la suplantación de la víctima para obtener las claves bancarias, datos de tarjetas de crédito o claves de acceso a determinadas páginas o servicios, lo cual servirá principalmente al sujeto activo del delito o a un tercero para obtener un beneficio de carácter patrimonial, todo esto facilita el acceso a los sistemas informáticos, haciendo más fácil la obtención de la clave de acceso. Una de las formas usuales de esta modalidad, se da a través de lo que se denomina *archivos espía* o *spyware* que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario. A través de un *spyware* se puede tener acceso por ejemplo a un correo electrónico, conocer la contraseña, la dirección IP, páginas que se visitan, que tiempos se está en ellas y con qué frecuencia se regresa; tarjeta de crédito, etc.[38].

Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías, si el usuario comprende plenamente que datos están siendo recopilados y a quién se distribuyen, ejemplo de ellos son las cookies que se definen como archivos en los que se almacena información sobre un usuario de Internet en su propio ordenador, y se suelen asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento. La existencia de los *cookies* y sus uso generalmente no están ocultos al usuario, quien puede desactivar el

[38] Karla Ivette Peña Martel, "Delitos Informáticos: Estafas, atentados contra la propiedad intelectual y delitos contra la intimidad". (Tesis de Maestría, Universidad Centroamericana José Simeón Cañas, 2008) 21

acceso a la información de estos; sin embargo, dado que un sitio web se puede emplear un identificador *cookie* para construir un perfil de un usuario sin que este usuario conozca la información que se añade a su perfil, se puede considerar que el software que transmite información de las *cookies*, sin que el usuario consienta la respectiva transferencia es una forma de *spyware*[39].

Los keyloggers (registrador de teclas), consisten básicamente en el registro de todo lo que los usuarios teclean desde su ordenador; es decir, se encargan de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet. Quien coloca el archivo espía puede recibir periódicamente información del usuario sin su conocimiento. Consecuentemente, el defraudador accede a información personal de la víctima y así aprovecharse para su beneficio patrimonial o de un tercero.

El spyware, es un archivo o programa que una vez introducido en el ordenador sin que la víctima advierta tal situación, envía a través de la Red las claves de acceso a diferentes servicios informáticos y entre ellos las de banca on-line, con las cuales el defraudador puede realizar una disposición fraudulenta a su favor o a favor de un tercero. Lo mismo puede decirse de aquellos casos en los que el defraudador mediante el acceso al sistema consigue hacer desaparecer o disminuir deudas propias o ajenas[40]. En virtud de lo anterior, se identificó, que el uso de Spyware facilita la comisión de delitos de esta índole, ya que al ser un malware que recopila toda la información de la computadora y después la transmite a una entidad externa para hacer uso de la misma con o sin el conocimiento y el consentimiento del propietario del computador.

---

[39] Ibíd.

[40] Técnicas de Investigación Criminal. 2012. Vol. 2a edición. Madrid: Dykinson. 324. Acceso el 4 de septiembre de 2019. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=687491&lang=es&site=ehost-live.

4.4.2 PISHING: Obtención fraudulenta de claves, en donde es la propia víctima la que sin ser consiente proporciona al sujeto activo los datos necesarios para realizar transacciones

Lo peculiar en esta modalidad, es que la misma víctima es la que proporciona sus datos al autor del delito. El phishing, es un término informático que denomina una acción que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

El sujeto activo, conocido como phisher, se hace pasar por una persona o empresa de confianza ante el sujeto pasivo, en una aparente comunicación oficial electrónica, por lo general mediante el uso de un correo electrónico o algún sistema de mensajería instantánea o incluso utilizando las llamadas telefónicas para lograr su cometido.

En esta modalidad se han detectado fórmulas tales como: encuestas falsas en nombre de organismos oficiales que tienen por objeto recoger datos personales, páginas falsas de recargas de móviles con tarjetas de crédito o de venta de diversos productos. Una vez obtenidos los datos personales y de la tarjeta, la página enseña algún tipo de error o indica que la operación no se ha podido realizar, etc.

Una variante del phishing es el pharming, derivado del término "farm" (granja) que consiste en que el atacante consigue acceso a un servidor DNS (Sistema de Nombres de Dominio) y tomando control de éste, haciendo uso a placer de los recursos o información que allí se encuentran y cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, es reenviado a otra por el *hacker* que tiene el mismo aspecto que la original, de esa manera el usuario cree estar en la página a la que accedió.

En la actualidad, existen personas naturales o empresas ficticias que reclutan trabajadores por medio de correos electrónicos, chats y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros dudosos beneficios. De esta manera, el sujeto activo recurre a una tercera persona para que reciba la transferencia bancaria y así evitar ser descubierto. A esta tercera persona se le suele denominar en el lenguaje coloquial: “mula” o “mulero”, a quienes se les deposita en sus cuentas personales el dinero procedente de sustracciones bancarias realizadas por el método de phishing.

4.5 Vulnerabilidades en la seguridad

Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware. Un ataque es el término que se utiliza para describir un programa o acción con el fin de aprovecharse de una vulnerabilidad conocida y con ello poder acceder a un sistema, los datos que aloja o recursos específicos.

Las vulnerabilidades de software, generalmente se introducen por errores en el sistema operativo; a pesar de todos los esfuerzos realizados por las empresas para encontrar y corregir las vulnerabilidades, es común que surjan nuevas vulnerabilidades, Microsoft, Apple y otros productores de sistemas operativos lanzan parches y actualizaciones casi todos los días[41].

Las actualizaciones de las aplicaciones también son comunes, ya que las aplicaciones como navegadores web, aplicaciones móviles y servidores web son actualizadas con frecuencia por las empresas y las organizaciones responsables de las mismas.

El objetivo de las actualizaciones de software es mantenerse actualizado y evitar el aprovechamiento de vulnerabilidades. Si bien algunas empresas

[41] Introducción a la Ciberseguridad. Programa en línea impartido por la OEA; Capítulo II: Búsqueda de vulnerabilidades en la seguridad.

tienen equipos de prueba de penetración dedicados a la búsqueda y la corrección de vulnerabilidades de software antes de que puedan ser aprovechadas, hay investigadores de seguridad independientes que también se especializan en la búsqueda de vulnerabilidades de software.

Ejemplo de lo anterior es el Proyecto Zero de Google, el cual después de descubrir varias vulnerabilidades en los diversos programas de software utilizados por los usuarios, formó un equipo dedicado a encontrar las vulnerabilidades del software y así lograr reforzarlo.

CONCLUSIONES

De acuerdo a todo lo desarrollado en los capítulos anteriores, se concluye que:

La información y los datos contenidos en diversos soportes electrónicos e informáticos, en la actualidad, adquiere una relevancia e importancia significativa, debido a la rápida evolución que han tenido las tecnologías de la Información y la comunicación, dentro de la Constitución de la Republica, las tecnologías de la comunicación e información no se encuentran tuteladas, pero existe la necesidad de protegerlas, en ese sentido, es necesario que el legislador valore una reforma, donde se establezca la tutela de la información y los datos como bien jurídico protegido de las mismas.

A su vez la Ley Especial Contra Delitos Informáticos y Conexos, contiene un catálogo de delitos que al analizarlos no son diferentes a los establecidos en el Código Penal, su única variante es el medio por el cual son cometidos estos delitos, en ese sentido, no era necesario la creación de una Ley especial que le diera tratamiento a los mismos, pues se pudo haber agregado en el Código Penal un título más, dicho esto, la recodificación de la Ley, es la alternativa de mayor utilidad para reforzar la legislación penal existente a través de reformas que doten nuevas herramientas que faciliten la investigación y comprobación de estas conductas delictivas, que como ya se dijo son de complejo abordaje.

En el Salvador no existe ningún convenio y/o tratado internacional suscrito en materia de delitos informáticos, por lo que es necesario que se suscriban y ratifiquen convenios y/o tratados internacionales, dentro de estos la suscripción al Convenio sobre la Ciberdelincuencia, mejor conocido como Convenio de Budapest, aportaría en nuestro país elementos fundamentales para el combate de la Ciberdelincuencia, ya que este contiene un apartado que regula la parte procesal, referente al tratamiento de los delitos

informáticos, que resultaría de suma importancia ante la carencia de dicha regulación en nuestra legislación para lograr dar un mejor tratamiento a la investigación de las conductas delictivas que se realicen por medio de un sistema informático.

Las instituciones encargadas de la persecución de los delitos informáticos en El Salvador, no cuentan con personal capacitado para identificar mediante la informática los elementos necesarios para el sustento de los casos relativos a este tipo de delitos, ya que no cuentan con las herramientas necesarias para la recolección de la evidencia digital, no basta unicamente contar con un perito altamente calificado cuando los Jueces, Fiscales y Defensores Públicos no logren dentro de sus funciones dar el tratamiento necesario a los mismos por la falta de conocimiento, en ese sentido las diferentes instituciones del Estado encargadas de la Administración de Justicia deben comprometerse a ampliar los conocimientos de todo aquel que forme parte de estas instituciones, a través de diplomados, maestrías y doctorados referente al tratamiento o persecución de los delitos informáticos, así como la implementación de una materia en las facultades de Jurisprudencia y Ciencias Sociales de las diversas Universidades de El Salvador para que los bachilleres desde sus inicios amplíen sus conocimientos y se preparen para administrar justicia de una mejor manera y poder hacer frente a dichas conductas delictivas.

Finalmente, es necesario promover y publicitar medidas preventivas básicas que permitan a los ciudadanos auto proteger sus dispositivos personales, ello con la finalidad de salvaguardar la información y los datos contenidos en estos soportes, así como hacer conciencia de la amenaza que representan los delitos informáticos en sus diferentes modalidades, de igual forma se deben crear reglas de responsabilidad no solo para los ciudadanos, sino también para las empresas prestadoras de servicios de red y comunicación, que regulen la producción, preservación o divulgación de los datos.

BIBLIOGRAFÍA

Libros

Bretón, Philips. Historia y Crítica de la Informática, (Madrid: Catedra, 1989), p.35.

Carnelutti, F. La prueba civil (Buenos Aires: De palma 2° edición, 2000), 84.

Castillo Jiménez, María Cinta, Ramallo Romero, Miguel. “El delito informático” (Zaragoza: Acribia, 1989), 22-24.

Díaz Alonso, Arturo. Informática I (México: Fondo Editorial, 2003), 15.

Estrada Garavilla, Miguel. “Delitos Informáticos”, Revista Derecho Penal, (2008): 4.

Garrido Montt, Mario. Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992. Citado por Jijena Leiva Renato, Los Delitos Informáticos y la Protección Penal a la Intimidad, Editorial Jurídica de Chile, 1993.

Magliona Marcocicht, Claudio Paul, y López Medel, Macarena. “Delincuencia y Fraude Informático” (Chile: Editorial Jurídica, 1999), 66.

Martínez Jaén, Raquel, José Alberto, y García Beltrán, Ángel. División de Informática: Breve Historia de la Informática Industrial (Madrid: Universidad Politécnica, 2006), p. 22.

Mommsen, Teodoro. Derecho penal romano (Madrid: La España Moderna, 1905), 457.

Reyes Echandía, Alfonso. “La Tipicidad” (Colombia: Universidad de Externado de Colombia, 1981), 50.

Ruiz Robredo, Gustavo. Electrónica Básica para Ingenieros (España: El autor, 2001), 11.

Téllez Valdez., Julio. “Derecho Informático”. (México: McGraw-Hill, 1996), 104.

Trabajos de Graduación

Ávila Umaña, Jonathan Alexander y Barrera Argueta, Antonio Alexander. "Elementos diferenciadores del delito de estafa regulado en el artículo 215 del código penal con la estafa informática regulada en la ley especial contra delitos informáticos y conexos" (Trabajo de grado para obtener el título de Licenciado en Ciencias Jurídicas, 2018), 65.

Castro, Nelson Geovanny y Ramos Gómez, Kevin Everardo. “Juicio para la aplicación exclusiva de medidas de seguridad" (Trabajo de grado para obtener el título de Licenciado en Ciencias Jurídicas, 2003), 70.

Peña Martel Karla Ivette. "Delitos Informáticos: Estafas, atentados contra la propiedad intelectual y delitos contra la intimidad". (Tesis de Maestría, Universidad Centroamericana José Simeón Cañas, 2008), 21

Legislación

Código Penal (El Salvador, 1993), art. 207.

Constitución de la República (El Salvador, Asamblea Legislativa, 1983) Art. 1

Ley Especial Contra Delitos Informáticos y Conexos (El Salvador, 2016), arts. 3, literal L.

Jurisprudencia

Sala de lo Constitucional de la Corte Suprema de Justicia. 91-2007. Inconstitucionalidad. San Salvador, a las quince horas con cincuenta minutos del día veinticuatro de septiembre de dos mil diez.

Documentos Institucionales:

Expediente legislativo N° 858--2010-1

Otras Fuentes

Carballo Mejía, Raymundo. “Ciber delito y evidencia digital”. Ponencia dictada en el Consejo Nacional de la Judicatura, diciembre 2018.

Oficina de las Naciones Unidas contra la droga y el delito. “Análisis Forense Digital”, Ponencia dictada en el Consejo Nacional de la Judicatura, enero de 2019.

Sitios Webs:

“Delitos Informáticos: Generalidades”. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. (Consultado el 26 de junio de 2019).

Dr. Santiago Acurio del Pino: Manual de manejo de evidencias digitales y entornos informáticos. https://www.oas.org/juridico/english/cyb_pan_manual.pdf. (Consultado el día 13 de septiembre de 2019).

Escuela de capacitación judicial Dr. Arturo Zeledón Castrillo, del Consejo Nacional de la Judicatura. “Monográfico: Debates sobre el sistema de justicia penal y penitenciario”. http://www.cnj.gob.sv/web/images/documentos/pdf/publicaciones/MONOGRAFICO/DebatesSistemaJusticiaPenalyPenitenciario.pdf. (Consultado el 3 de agosto de 2019).

Levaggi, Abelardo, “Historia del Derecho Penal Argentino” (Buenos Aires: Perrot, 1939), 94. http://www.derecho.uba.ar/investigacion/documentos/lecciones-de-historia-juridica-v-1978-levaggi-historia-del-derechopenalargentino.pdf. (Consultado el 1 de junio de 2019).

“Manual de Manejo de Evidencias Digitales y Entornos Informáticos”. https://www. oas.org/juridico/english/cyb_pan_manual.pdf. (Consultado el 1 de septiembre de 2019).

“Manual de Manejo de Evidencias Digitales y Entornos Informáticos”. https://www. oas.org/juridico/english/cyb_pan_manual.pdf. (Acceso el 8 de septiembre de 2019).

Mazuelos Coello, Julio, Modelos de Imputación en el Derecho Penal Informático (Alemania, editorial AKAL, 2002), 3. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwj4gtXfzvbkAhVH1VkKHZU5AkEQFjAAegQIARAB&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F3313826.pdf&usg=AOvVaw3wIUk6IidOsuy18yBc5QjG. (Consulta el 1 de junio de 2019).

Schwab, Martín A. I., Manual de derecho penal hebreo (Buenos Aires: editorial Jurídica, 2014), 264, 267. http://www.casi.com.ar/sites/default/files/10953.PDF. (Consultado el 1 de junio de 2019).

Técnicas de Investigación Criminal. 2012. Vol. 2a edición. Madrid: Dykinson. 316. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=687491&lang=es&site=ehost-live. (Consultado el 4 de septiembre de 2019).

Tesis doctoral. “La prueba electrónica: sus implicaciones en la seguridad de la empresa”. https://www.tesisenred.net/handle/10803/285237. (Consultado el 4 de septiembre de 2019).

ANEXOS

Universidad de El salvador
Facultad de Jurisprudencia y Ciencias Sociales
Escuela de Ciencias Jurídicas

Curso de seminario para obtener el grado de Licenciado en Ciencias Jurídicas.

Asesor de seminario: Lic. Luis Antonio Villeda Figueroa.

Alumnos: Gino Romano Aguirre Duran

Alejandra Yamileth Velásquez Corpeño

Celia Elizabeth Vigil Mena

Entrevista dirigida a: Dr. Juan Antonio Duran Ramírez, Magistrado de la Cámara 3° de lo Penal de la 1° sección del Centro de San Salvador".

Respetable Doctor, Durán el presente cuestionario tiene como propósito recolectar información para realizar el trabajo de grado para obtener el título de licenciado en ciencias jurídicas. Tales datos serán de vital importancia para verificar en qué consiste el delito de "Hurto por medos Informáticos en el salvador.

A continuación, se detallarán las preguntas:

1. En sus palabras, bríndenos un concepto de delitos informáticos.
2. En sus palabras, bríndenos un concepto del delito hurto por medios informáticos.

3. Considera usted indispensable la creación de la LECDIC, o es de la opinión que el problema se pudo solventar con una reforma al código penal y procesal penal.
4. ¿Con que deficiencias y obstáculos se enfrenta desde su experiencia profesional al investigar los delitos informáticos?
5. ¿Con base en su experiencia profesional, considera que la vigente legislación ofrece las adecuadas herramientas en materia de prueba para investigar y demostrar las conductas delictivas cometidas mediante el uso de las tecnologías de la información y la comunicación?
6. ¿Con base a su experiencia profesional, cual es el medio de prueba pertinente para demostrar un delito informático?
7. ¿Con base en su experiencia profesional, considera que la prueba pericial es el medio de prueba pertinente para demostrar la comisión del delito de hurto por medios informáticos?
8. ¿Considera necesaria la suscripción de convenios o tratados internacionales en materia de combate a la delincuencia informática, como el caso del convenio sobre la ciberdelincuencia o mejor conocido como convenio de Budapest, que ofrece un aparte referente a la parte procesal y probatoria respecto de los delitos informáticos y otro que regula la cooperación internacional y asistencia mutua entre países suscriptores?
9. ¿Considera que en nuestro país se cuenta con la suficiente publicidad e información respecto de la amenaza de los delitos informáticos?
10. ¿Considera que las instituciones encargadas de perseguir el delito en El Salvador, se encuentran lo suficientemente capacitadas en cuanto a su personal y recursos para hacer frente a la problemática de los delitos informáticos?
11. De todo lo anterior, cuáles serían sus conclusiones y recomendaciones.

Resumen de entrevista

Entrevista dirigida a: "*Dr. Juan Antonio Duran Ramírez, Magistrado de la Cámara 3° de lo Penal de la 1° sección del Centro de San Salvador"*

En dicha entrevista se nos dio a conocer una manual llamado "Aceptación general de la prueba pericial" del año 2016 en el que se habla sobre que "Consiste la prueba pericial ", "como se aplica ", entre otras generalidades la cual tuvo como base la prueba del polígrafo que se lleva a cabo en el proceso penal y la corte suprema de los estados unidos rechazo este tipo de prueba pericial en la llamada prueba de "TAI "por qué no era aceptado por la comunidad científica lo cual implica que para que una pericia sea aceptada como prueba debe de gozar de aceptación general de la comunidad técnica o científica que exista.

Por otra parte, contamos con un precedente llamado "trilogía Daupert" del año 93', consistente en 3 sentencias, en las que el tribunal de la corte suprema de los EE. UU iba perfeccionando las exigencias del peritaje estableciendo con ello requisitos que debe de cumplir el peritaje para que sea visible y tenga eficacia probatoria.

En cuanto al problema de los delitos informáticos se abordó el tema de la "Evidencia", por lo que surgió la interrógate ¿cómo probar el Hurto? En el que según el licenciado existe una técnica llamada "técnica de Salami" la cual consiste en crear un Software más bien llamado "malware" en el que se sustrae parte del dinero de la cuenta de una persona, dicho esto estamos hablando de un Hurto, el problema es como probarlo ya que genera ciertos problemas procesales ya que se tiene que investigar el lugar de donde se cometió el hecho, el lugar donde se encuentra almacenada la prueba, quien es el competente de acceder a esta información.

También dentro de la entrevista proporcionada se nos dio la información consistente en el “Valor Hash” este valor permite asegurar la identidad de la evidencia es decir su autenticidad por ejemplo cuando hacemos mención del Art 250 del CPP en donde tipifica respecto de la “Cadena de Custodia” en donde hace mención que se debe de asegurar la autenticidad de la prueba es decir que este articulado se refiere a asegurar la identidad de la prueba que es lo que asegura el “Valor Hash” es decir que si yo manipulo o altero una base de datos el valor Hache será distinto.

Se nos dio a conocer también que hay distintos tipos de hurtos por medios informáticos los cuales son 1) en cuanto a la técnica utilizada está el Software y 2) la Manipulación de consola que tiene que ver con la manipulación y alteración del “Hardware”

Si bien es cierto que existen diferentes teorías a nivel constitucional y a nivel de nuestro código penal en donde se señala que la afectación del bien jurídico a causa del delito de hurto por medios informáticos se da precisamente en el aspecto del patrimonio económico o en la protección de los datos personales a nivel colectivo, según el licenciado estas perspectivas van más allá, ya que la Sala de lo Constitucional respecto del bien jurídico estableció una sentencia llamada “ la autodeterminación informativa “, la cual tiene que ver con los datos personales, la cual consiste en que toda persona tiene derecho a saber quién tiene acceso a sus datos , quien la actualiza, quien puede acceder a esa base de datos , incluso tiene derecho a solicitar que se borren.

Con base a lo anterior se dio un caso de amparo llamado (DICON) en el que una de las partes involucradas intento hacer un préstamo pero al cerciorarse se dio cuenta que aún en el sistema le aparecía aun dicho préstamo y lo que no se tomó en cuenta es que para borrar dicho crédito hay un plazo de 6 meses para que el dato pueda ser actualizado y fue por esa razón que se

interpuso dicho amparo, esta persona demando a la empresa (DICOM) quien tiene acceso a todos los datos personales de las personas, y que negaba tener información de las personas por lo que se negó a responder por daños causados, la Sala de lo Constitucional por su parte desistió de seguir aunando con la información y como el demandante en el amparo no probo con base a pruebas idóneas que dicha empresa poseía la información se dictó una resolución en donde se sobreseyó el amparo por falta de pruebas.

Dicho lo anterior se empezó a crear a través de los años, la llamada “carga dinámica de la prueba “, la cual consiste en que la prueba deberá ofrecerse por aquella persona que posea la prueba ya sea de manera voluntaria o coactivamente con base a esto la Sala de lo Constitucional pudo haber ordenado el allanamiento en dicho caso, y obtenerse una resolución favorable.

Universidad de El salvador
Facultad de Jurisprudencia y Ciencias Sociales
Escuela de Ciencias Jurídicas

Curso de seminario para obtener el grado de Licenciado en Ciencias Jurídicas.

Asesor de seminario: Lic. Luis Antonio Villeda Figueroa.

Alumnos: Gino Romano Aguirre Duran

Alejandra Yamileth Velásquez Corpeño

Celia Elizabeth Vigil Mena

Entrevista dirigida a: "Subcomisionado Douglas Edenilson Zometa, jefe de la División Central de Investigaciones de la Policía Nacional Civil".

Respetable Subcomisionado Zometa el presente cuestionario tiene como propósito recolectar información para realizar el trabajo de grado para obtener el título de licenciado en ciencias jurídicas. Tales datos serán de vital importancia para verificar en qué consiste el delito de "Hurto por medos Informáticos en el salvador.

A continuación, se detallarán las preguntas:

1. En sus palabras, bríndenos un concepto de delitos informáticos.
2. En sus palabras, bríndenos un concepto del delito hurto por medios informáticos.

3. Considera usted indispensable la creación de la LECDIC, o es de la opinión que el problema se pudo solventar con una reforma al código penal y procesal penal.
4. ¿Con que deficiencias y obstáculos se enfrenta desde su experiencia profesional al investigar los delitos informáticos?
5. ¿Con base en su experiencia profesional, considera que la vigente legislación ofrece las adecuadas herramientas en materia de prueba para investigar y demostrar las conductas delictivas cometidas mediante el uso de las tecnologías de la información y la comunicación?
6. ¿Con base a su experiencia profesional, cual es el medio de prueba pertinente para demostrar un delito informático?
7. ¿Con base en su experiencia profesional, considera que la prueba pericial es el medio de prueba pertinente para demostrar la comisión del delito de hurto por medios informáticos?
8. ¿Considera necesaria la suscripción de convenios o tratados internacionales en materia de combate a la delincuencia informática, como el caso del convenio sobre la ciberdelincuencia o mejor conocido como convenio de Budapest, que ofrece un aparte referente a la parte procesal y probatoria respecto de los delitos informáticos y otro que regula la cooperación internacional y asistencia mutua entre países suscriptores?
9. ¿Considera que en nuestro país se cuenta con la suficiente publicidad e información respecto de la amenaza de los delitos informáticos?
10. ¿Considera que las instituciones encargadas de perseguir el delito en El Salvador, se encuentran lo suficientemente capacitadas en cuanto a su personal y recursos para hacer frente a la problemática de los delitos informáticos?
11. De todo lo anterior, cuáles serían sus conclusiones y recomendaciones.

Resumen de entrevista

Entrevista dirigida a: "*Subcomisionado Douglas Edenilson Zometa, jefe de la División Central de Investigaciones de la Policía Nacional Civil"*

En la entrevista realizada al Sargento, se buscó en primer lugar obtener una mejor compresión del delito de hurto por medios Informáticos por lo cual se nos proporcionó información en base a sus propios conocimientos y experiencia estableciendo que dicho delito consiste en la mera sustracción de la información que se le hace a la víctima, sin su conocimiento, de sus datos, por lo que hay tener cuidado ya que este delito puede prestarse a la configuración de otros delitos como por ejemplo el delito de hurto de identidad simulando así una suplantación.

Cuando hablamos de hurto por medios informáticos, debemos de tener presente que estamos frente a la sustracción de datos pero no podemos obviar que no solo puede ser información si no también podemos hablar de hurto patrimonial a la víctima por ejemplo cuando el sujeto activo, sustrae el PIN de la tarjeta de crédito de la víctima y hace una transferencia de una cierta cantidad de dinero a otra cuenta, es ahí cuando nos damos cuenta que hay una disminución patrimonial para la víctima y al mismo tiempo estamos hablando de una sustracción patrimonial, el hurto no puede ser solo conceptualizado como la sustracción de datos o información sino también como la sustracción que causa una disminución patrimonial.

En dicha entrevista también se nos hizo mención de la llamada ingeniería social la cual consiste en obtener información confidencial a través de la instrucción de usuarios proyectados. Por ejemplo, el PHISHING la cual consiste en una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, credenciales, cuentas bancarias, números de tarjeta de crédito, etc.

El estafador, conocido como phisher, se hace pasar por una persona o empresa en una aparente comunicación oficial electrónica, por lo general un correo electrónico, mensajería instantánea, redes sociales, incluso llamadas telefónicas. Esta es una técnica que debe utilizar ciertas personas para obtener acompañamiento, acceso o restricciones en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

En el contexto del crimen cibernético, es ampliamente descrita como un método no técnico utilizado por los cibercriminales para obtener información, realizar fraudes u obtener acceso ilegítimo a los equipos de las víctimas. La Ingeniería Social se basa en la interacción humana y está impulsada por personas que usan el engaño con el fin de violar los procedimientos de seguridad que normalmente deberían haber seguido.

Y una de las ultimas cosas que se nos enseñó en la entrevista es que para evitar cualquier cometimiento de delitos informáticos es hacer campañas publicitarias en las se den a conocer las consecuencias de cometer este tipo de delitos, dar a conocer en que consiste y cuál es el riesgo legal que se corre así estaríamos evitando cualquier forma de cometimiento de este hecho delictivo tan moderno.