UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

UNIDAD DE ESTUDIOS DE POS GRADOS

MAESTRÍA EN DERECHO PENAL ECONÓMICO

TEMA

“Limitaciones del sistema penal para investigar y probar la comisión del Ciberdelito en El Salvador.”

TESIS PARA OBTENER EL GRADO DE

MAESTRO EN DERECHO PENAL ECONÓMICO

PRESENTADA POR

LIC. LUCIO ALBINO ARIAS LÓPEZ

DOCENTE ASESOR

DR. ARMANDO ANTONIO SERRANO

CIUDAD UNIVERSITARIA, SAN SALVADOR, NOVIEMBRE 2021

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias

RECTOR

Dr. Raúl Ernesto Azcunaga López

VICE RECTOR ACADÉMICO

Ing. Juan Rosa Quintanilla Quintanilla

VICE RECTOR ADMINISTRATIVO

Msc. Francisco Antonio Alarcón Sandoval

SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín

FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata

DECANA

Dr. Edgardo Herrera Medrano

VICE DECANO

Msc. Digna Reina Contreras de Cornejo

SECRETARIO

Msj. Hugo Dagoberto Pineda Argueta

DIRECTOR DE LA ESCUELA DE CIENCIAS JURÍDICAS

Dr. José Miguel Vásquez LÓPEZ

JEFE DE LA UNIDAD DE POST GRADOS

Licda. Diana del Carmen Merino de Sorto

DIRECTOR DE PROCESOS DE GRADUACIÓN

TRIBUNAL CALIFICADOR

PRESIDENTE

Dr. Reinaldo González

SECRETARIO

Msc. Hugo Dagoberto Pineda Argueta

VOCAL

Dr. Armando Antonio Serrano

AGRADECIMIENTOS

Dedico este trabajo A:.L:.G:.D:.G:.A:.D:.U:., por darme la iluminación y la fuerza para continuar mis estudios y haber realizado esta tesis de forma satisfactoria a costa de muchos sacrificios

A mi padre, José Efrén Arias Villalta, quien me apoyo hasta el último día de su vida en seguir adelante con este proyecto. Gracias por ser un ejemplo de vida para mí.

A mi madre, María Elvira por ser en toda mi vida mi piedra angular, apoyarme siempre en mis proyectos y sueños por alentarme en cada uno de ellos, pero en especial por su amor, sin el cual no conocería la senda de la verdad.

A mis Hermanos, Urania, Aleyda y Fredy, por ser parte importante de mi vida y a pesar de que en muchas ocasiones siento que soy una carga para Uds. espero en lo que me resta de vida compensarles todo lo que me han dado.

A mi mujer Jacqueline, por tu paciencia, tu comprensión por las horas de tiempo dedicadas a este trabajo y tu amor. Dedico este trabajo a nuestro hijo Juan Pablo quien espero se encuentre orgulloso de su padre por este trabajo que hoy culmino.

A mi asesor de tesis, Dr. Armando Serrano, por la paciencia en la espera de este trabajo investigativo, por el tiempo, palabras de aliento y la guía brindada para la realización de esta tesis y de quien he aprendido que el Derecho Penal es una rama jurídica con mucha riqueza, siendo un gran reto escribir e investigar científicamente sobre esta materia lo cual redobla mi admiración y respeto hacia el Dr. Serrano por ser uno de los pocos profesionales que ha difundido la Dogmática Penal en nuestro país.

A mi eterna compañera Avril, quien ha visto mermado el tiempo para estar juntos por el desarrollo de mis estudios, gracias por estar siempre a mis pies mientras estudiaba y también mientras redactaba esta tesis, tú me has enseñado lo que es la fidelidad y el amor a costa de todos los sacrificios.

ÍNDICE DE CONTENIDOS

SUMARIO

El ciberdelito es una categoría nueva en la ciencia penal, que tiene su desarrollo a partir de que la delincuencia comienza a utilizar la internet para cometer hechos ilícitos que eran conocidos como delitos tradicionales, pero ahora cometidos a través del Internet. Con el paso de los años esta ciberdelincuencia ha mutado, por lo que en la actualidad los ciberdelitos tienen por objeto de ataque los sistemas de la información y la comunicación o son realizados por medio de máquinas basadas en estas tecnologías e incluso han creado situaciones ilícitas que no existían en el Derecho Penal tradicional y liberal. Por lo cual esta tesis brinda información básica sobre los sistemas de información y comunicación, como de las técnicas más sobresalientes que puede usar la policía en la investigación de los mismos, así como se hace un análisis de las limitantes que tiene el sistema penal salvadoreño para luchar contra este flagelo.

ABREVIATURAS UTILIZADAS

Art. .....Artículo

Cfr. ..... Confróntese

Cn. .....Constitución de la Republica

C.N.J .....Consejo Nacional de la Judicatura

C.P. ..... Código Penal

C.P.C.M. .....Código Procesal Civil y Mercantil

C.P.P. .....Código Procesal Penal

C.S.J. .....Corte Suprema de Justicia de El Salvador

D.L. .....Decreto Legislativo

D.O. .....Diario Oficial

EE.UU. ..... Estados Unidos de América

FGR .....Fiscalía General de la Republica

IP .....Protocolo de Internet

ISP .....Proveedores de servicios de internet

LECDIC.....Ley Especial Contra los Delitos Informáticos y Conexos

OCDE ..... Organización de Cooperación y Desarrollo Económico

Nº.....Número

p./pp.....página/s

Paraf. .....Paráfrasis

p. e. .....Por ejemplo

PNC .....Policía Nacional Civil

RAE .....Real Academia de la Lengua Española

TIC´S ..... Tecnologías de la Información y la Comunicación

v. gr.....verbi gratia (por ejemplo)

INTRODUCCIÓN

El siglo XXI se ha caracterizado por la necesidad del ser humano de vincularse en sus tareas cotidianas con el uso de las computadoras o diversos aparatos tecnológicos que le permiten una vida más productiva, que también han llevado a la globalización de la información y la comunicación; es por ello que no es raro hablar que en la actualidad también exista una conjunción entre la informática y el derecho principalmente en lo tocante al comercio electrónico o las transacciones bancarias por medio de las Tecnologías de la Información y la Comunicación (en lo sucesivo TIC´S). No obstante, dicha realidad no es ajena a ciertas conductas antisociales que se apoyan en la tecnología para lesionar bienes jurídicos, ya sea como un medio para realizar los hechos delictivos o como un objeto sobre el que recae la acción ilícita.

Desde la década de los noventas del siglo pasado, con el advenimiento de la sociedad de la información y el uso de la red de redes conocida como “internet”, se ha generado una mutación en la vida del ser humano para quien el uso de instrumentos tecnológicos ya es parte de su diario vivir pues facilitan el comercio, la adquisición de bienes o servicios y en general en la actualidad una muy buena parte de la población mundial tiene acceso a estos; pero a la vez su uso ha dado nacimiento a ciertas actividades delictivas que generan una transformación del clásico Derecho Penal -ya que existen ataques a bienes jurídicos tutelados-, pero esta vez se realizan mediante el uso de las TIC´S que por su no tipificación en la legislación penal quedaban dentro de un margen de impunidad sin que las victimas pudieran tener una tutela legal efectiva

Este fenómeno ilícito ha sido denominado por la doctrina más representativa “Ciberdelito” que es una categoría nueva en la ciencia penal, que tiene su desarrollo a partir de que la delincuencia comienza a utilizar la red de redes para cometer hechos ilícitos que eran conocidos como delitos tradicionales, pero ahora cometidos a través del Internet. Con el paso de los años esta ciberdelincuencia ha mutado, por lo que en la actualidad los ciberdelitos tienen por objeto de ataque los sistemas de la información y la comunicación

o son realizados por medios de máquinas basadas en estas tecnologías e incluso han creado situaciones ilícitas que no existían en el Derecho Penal tradicional y liberal.

En diversos países del mundo, los legisladores se han visto en la obligación de configurar normativas especiales para el tratamiento de los Ciberdelitos a fin de garantizar seguridad jurídica y paz social a su población; El Salvador no ha sido la excepción ya que el año 2016 dictó la Ley especial contra delitos informáticos y conexos la cual como se verá en el desarrollo de esta investigación refleja datos estadísticos muy bajos de casos judicializados respecto de los casos que han sido denunciados ante la Fiscalía General de la República, por lo cual pareciera que solo ha sido una ley penal simbólica o que aún no existen los suficientes elementos necesarios para realizar investigaciones sobre hechos delictivos cometidos en el internet.

Se debe reconocer que la sociedad salvadoreña está naciendo a la vida en el ciber espacio, ya que cada día más salvadoreños están teniendo acceso a teléfonos inteligentes, computadoras o tabletas que abren la puerta a las redes sociales, al uso de aplicaciones de comunicación o intercambio de información a través del uso de plataformas virtuales, aunado a los esfuerzos del Gobierno de la Republica actual de proporcionar equipo informático con acceso a internet a los niños y niñas, así como a los adolescentes para poder realizar estudios en línea. También se ha dado inicio en El Salvador al comercio electrónico que permitirá a las personas, naturales y jurídicas, la adquisición o promoción de bienes o servicios vía la internet, pero no todo es bueno en estas transformaciones sociales que están sucediendo, pues el acceso “a la red” entraña también el peligro de ser víctima de la “ciberdelincuencia” o “ciber criminalidad” que no es otra cosa que la realización de hechos delictivos tradicionales a través del uso de Tecnologías de la Información y la comunicación, así como en ciertos casos también hechos delictivos autónomos o clásicos que inician sus actividades ilícitas utilizando como medio una computadora.

Lo dicho en el párrafo anterior ha llevado a la dogmática penal a plantear la necesidad de una política criminal orientada a la prevención y combate de la nueva modalidad de

delincuencia que ha permitido que conductas realizadas por medio de una o varias TIC´S se vuelvan ilícitos penales por su elevación a la categoría de ley y su conminación a través de una pena para disuadir a la población de la práctica de las mismas por consideradas como hechos punibles que vulneran bienes jurídicos protegidos para la sociedad.

Es por ello que con el desarrollo de esta investigación se pretende obtener como resultado una aproximación al estudio del ciberdelito con criterios dogmáticos que permitan interpretar en buen sentido las conductas delictivas cometidas a través del internet y determinar las limitaciones del sistema penal para su investigación y posterior prueba. Por lo cual esta tesis brindara información básica sobre los sistemas de información y comunicación, que técnicas son las más sobresalientes que puede usar la policía en la investigación de los ciberdelitos, así como se hace un análisis de las limitantes que tiene el sistema penal salvadoreño para luchar contra este flagelo.

La orientación de esta investigación ha sido de tipo dogmática – jurídica porque el fenómeno investigado es abordado exclusivamente a nivel doctrinario habiendo consultando así como fuentes de información textos bibliográficos, articulos académicos, páginas web con datos oficiales de diferentes países de habla hispana, pero dejando de lado todo tipo de realización, operacionalización o comprobación de hipótesis-, en iguales circunstancias, se consultarán, textos normativos internacionales y nacionales relacionados al objeto de estudio.

En el entendido a que el problema de estudio fue planteado con la siguiente pregunta: *¿Qué tipo de limitaciones tiene el sistema penal en El Salvador para investigar y probar la comisión del Ciberdelito?* La respuesta de esta tesis a dicha interrogante hace que la naturaleza de este estudio haya sido **exploratoria** en cuanto a los niveles de profundidad pues se ha investigado un fenómeno desde la realidad de diferentes países de donde se ha tomado las exposiciones doctrinarias para determinar luego como podría aplicarse a la realidad salvadoreña, lo que sin lugar a dudas lleva un componente **explicativo** por la novedad de los temas a tratarse que pueden propiciar tanto a nivel legislativo una reforma

a la LEDIC o al Código Procesal Penal, y a nivel científico, jurídico-penalmente hablando abonará elementos para el debate de estos temas.

El lector podrá encontrar en el presente estudio en el capítulo I los antecedentes históricos de la informática como base de lo que provocó el desarrollo de la internet, considerada la "red de redes" pues en la actualidad es el principal medio de comunicación y traslado de información, pero no siempre fue así por tal motivo en este capítulo se aborda su evolución histórica hasta la actualidad. Finalmente se realizará un esbozo de lo que la Doctrina del Derecho Penal ha dado en llamar "la delincuencia informática" en la cual se realizan comportamientos ilícitos a través de la internet o cuyo objeto de ataque son los aparatos que se basan en Tecnologías de la Información y la Comunicación.

En el capítulo II se hace un estudio básico y general de la informática que ayudarán a entender el uso de las máquinas basadas en las TIC´S, que debe entenderse por sistema informático, el Ciberespacio, las redes sociales y lo que se conoce como nuevas tecnologías que permitirán en entendimiento del último de dicho capítulo que es lo relativo a la *Deep Web* o "red profunda" para entenderla y verificar como desde ahí se cometen hechos delictivos o se pueden encontrar los contactos o tecnologías útiles para perpetrarlos con lo que nace la *Dark Web.*

En el capítulo III se expone dogmáticamente lo que debe entenderse por el fenómeno objeto de este estudio, descartándose otros conceptos planteados por la doctrina que si bien son aplicables a los ilícitos cometidos con el uso de las nuevas tecnologías solo abordan el comportamiento contrario a la ley desde una faceta, siendo atendible y más abarcador el término "Ciberdelito" por las razones que ahí se expondrán. En el mismo se realiza un análisis del Ciberdelito desde la teoría general del delito determinando como encajar el objeto de estudio en sus diferentes categorías o niveles de análisis dogmático.

A nivel internacional se han desarrollado en los países que han decidido confrontar la Ciberdelincuencia una serie de técnicas de investigación de los ilícitos cometidos a través del uso de las TIC´S o que tienen por objeto de ataque las máquinas basadas en dichas

tecnologías, mismas que son aplicadas por la policía para determinar la realización de los Ciberdelitos y lograr individualizar a sus hechores con la finalidad de luego llevarlos ante los tribunales de justicia e iniciar el respectivo proceso penal en donde los actos de investigación aludidos lograrán determinar los diversos medios de prueba que el órgano persecutor del delito podrá presentar ante los jueces para poder propiciar que se brinde una resolución judicial donde se tenga la certeza de la realización del hecho y la participación de los que resulten imputados al respecto del mismo. Motivo por el cual estos temas son tratados en el capítulo IV de este estudio.

Finalmente se puede deducir de todo lo dicho que el objetivo general de esta tesis que era indagar qué tipo de limitaciones tiene el sistema penal Salvadoreño para investigar y probar la comisión del Ciberdelito fue alcanzado luego del análisis de datos oficiales proporcionados por diversos órganos que forman parte del sistema penal salvadoreño como podrá apreciarse por el lector al revisar en especial el capítulo V como se pone de manifiesto en su desarrollo.

En el capítulo VI de este estudio el lector podrá encontrar las conclusiones y recomendaciones que el autor del mismo presenta en resumen luego de esta investigación, los cuales se espera que sean tomados en cuenta por otros investigadores que pretendan profundizar aún más en el fenómeno de la Ciberdelincuencia y a la vez que los mismos sean tomados en cuenta, como se dijo párrafos arriba, por los legisladores para propiciar reformas legales que habiliten la protección de la ciudadanía ante estos hechos ilícitos.

CAPITULO I: ANTECEDENTES HISTORICOS

SUMARIO: 1.1. Breve reseña histórica de la informática. 1.2. Breve reseña histórica de la internet. 1.2.1. Etapa militar. 1.2.2. Etapa académica. 1.2.3. Etapa comercial. 1.2.4. Etapa social. 1.3. Breve reseña histórica de la delincuencia informática. 1.3.1. A nivel mundial. 1.3.2. A nivel nacional

RESUMEN:

En el presente capitulo se abordarán de forma muy breve la evolución histórica de la informática, la internet y de la delincuencia asociada a la misma, a fin de que el lector pueda hacerse a la idea de cómo nace la informática y sus avances al día de hoy, pero a la vez comprenderá que el fenómeno de la delincuencia también ha penetrado en este ámbito, así como que hasta hace muy pocos años los legisladores en diversos países del globo han tomado cartas en el asunto para crear cuerpos normativos que regulen las conductas delictivas realizadas en el campo de las TIC´s y el internet.

1.1.Breve reseña histórica de la informática.

Al iniciar este apartado debe tenerse en cuenta que lo que hoy en día es la informática nace de la necesidad del ser humano de calcular, para tal fin el primer instrumento inventado fue el ábaco, que permitió a los comerciantes realizar operaciones matemáticas de una forma ágil, rápida y precisa lo cual ahorraba tiempo y permitía una mejor certeza en cuanto a la forma de realizar operaciones básicas.

No obstante el ábaco, con el paso del tiempo, fue quedando obsoleto ya que las relaciones humanas vinculadas con los cálculos con el devenir del tiempo se fueron realizando de forma más compleja y el ingenio humano fue

desenvolviéndose para crear nuevas formas de hacer operaciones matemáticas, por ello con sobrada razón se ha dicho que la informática está basada, principalmente, en las matemáticas[1].

Para una mejor comprensión de lo dicho al final de párrafo anterior, es necesario, para fines didácticos, establecer dos etapas de la informática: La primera que se denominará informática especulativa y la otra informática práctica, que permitirá que el lector tenga una mejor comprensión de la evolución de la temática que se está desarrollando.

Por ***informática especulativa*** se entenderá las diversas teorías planteadas por científicos o libre pensadores que diseñaron las ideas de cómo debía funcionar una máquina que pudiese llevar a cabo gran número de cálculos con poco esfuerzo humano. Como lo pone de manifiesto GONZALEZ, la primera persona que entendió la utilidad de la mecanización del cálculo fue G.W. Leibniz (1646 – 1716) que estableció la idea que para mejorar el cálculo era necesario la utilización de máquinas, idea sobre la cual empezaron a volcarse en los sucesivo otro físicos y matemáticos[2]; luego aparece el científico Charles Babbage (1791 – 1871) que sienta las bases de lo que considerará en la siguiente etapa como una computadora programable y no sólo una máquina que realizará operaciones aritméticas; se debe hacer énfasis que esta máquina "nunca llego a ser construida, entre otras cuestiones por las dificultades técnicas que suponía hacerlo en esa época"[3].

---

[1] Jorge Alexandre González Hurtado, "Delincuencia informática: Daños informáticos del Artículo 264 del Código Penal y propuesta de reforma" (Tesis Doctoral, Madrid, Universidad Complutense de Madrid, 2013).21.
[2] Ibid. 21.
[3] Ibid. 22.

En 1936 el libre pensador, Alan Turing, realiza un modelo teórico de máquina, basándose en los modelos de Babbage, sus trabajos no se basaban en la idea de construir un **ingenio mecánico** que cumpliese la teoría por el expuesta. Sin embargo, la relevancia científica de su teoría se fundamenta en que las computadoras construidas con posterioridad responden perfectamente al modelo de la máquina de Turing[4].

Luego de esa etapa eminentemente teórica, se pasa a la ***informática práctica*** que da inicio a finales de la segunda guerra mundial cuando el científico Konrad Zuse (1910 – 1995) crea en el año 1941, en la Alemania Nazi, el sistema Z3 la cual era una máquina que respondía a las ideas de Turing que era programable y totalmente automática[5], con lo que nace la informática moderna.

La nota característica de todos los avances posteriores a la creación del Z3 se centran en cuestiones relativas a la miniaturización de los sistemas, el aumento de su capacidad de procesos por unidad de tiempo a través del desarrollo de la electrónica y la integración de sistemas de apoyo anexos a la propia computadora para, en un momento algo más avanzado, dar comienzo a la creación de redes informáticas[6].

En la década de los cincuenta del siglo pasado, comienzan a desarrollarse lenguajes de programación, que son representaciones digitales o numéricas y resuelven los problemas matemáticos en un sistema dual (0/1-interruptor),

---

[4] Ibid. 22
[5] Como se pone en evidencia según González en la página http://www.etsisi.upm.es, consultada el 30/12/2020 sin encontrar la referencia a la misma, más que en la tesis citada por el autor.
[6] González Hurtado, Delincuencia informática. 23.

cuya indicación elemental se llama ***"bit"*** , una serie de 8 bits forma un octeto (p.e. 10011101) que corresponde a una cifra o un carácter en el teclado, este sistema permite traducir las órdenes que los humanos dan a la máquina en un lenguaje que esta entiende[7].

Así mismo desde 1950 se presentan nuevos equipos capaces de desarrollar mayor número de procesos por unidad de tiempo, en donde la compañía norteamericana IBM jugo un papel fundamental en la concepción de nuevas técnicas para la construcción de estas modernas máquinas, utilizando nuevos materiales para componentes y la miniaturización de estos.

A partir de la década de 1970, parafraseando a GONZALEZ, se produce una inflexión con la invención del ***"microprocesador"***, gracias a la cual se consiguen abaratar significativamente los costos de producción de las computadoras y las dimensiones del mismo[8] para dar nacimiento a lo que se conoció como ***"la computadora personal"*** más conocida por su abreviatura "PC" que en sus primeros modelos requerían conocimientos especializados para su uso[9], lo que con la comercialización de las mismas fue cambiando volviéndolas más sencillas de usar para todo tipo de personas, como se verá a continuación.

---

[7] Francisco Castillo González, *La estafa informática* (San José, Costa Rica: Editorial Jurídica Continental, 2016).15.

[8] Se debe tener en cuenta que las primeras computadoras que realizaban 5 mil operaciones aritméticas por segundo tenían un tamaño equivalente a varios campos de futbol con un gran consumo de energía eléctrica para su funcionamiento, para profundizar más sobre este tema se recomienda la lectura de la historia del *Electronic Numerical Integratos and Calculator* conocido por sus siglas como "ENIAC" en https://histinf.blogs.upv.es/2011/12/05/proyecto-eniac/#:~:text=El%20proyecto%20ENIAC%20(%20Electronic%20Numerical,la%20maquina%20hasta%20el%201946. Consultado el 30 de diciembre de 2020.

[9] González Hurtado, Delincuencia informática. 25.

A nivel comercial destaca el inicio de operaciones de la empresa Intel en 1960, así como Apple y Microsoft en la década de los setenta del siglo pasado; por eso un selecto grupo de compañías fue el encargado del desarrollo de la informática a partir de 1980 coincidiendo en el tiempo con el principio de la era de la informática personal, que busca llevar a cada hogar del planeta una computadora, que está ligada a la aparición de nuevos dispositivos portátiles y la integración de la telefonía; a su vez en esta misma época inicia el uso civil de la red de redes conocida como la internet.

1.2. Breve reseña histórica de la Internet.

El desarrollo de las computadoras dio nacimiento a los entornos de red, mejor conocido como el Internet, esta no es un cuerpo físico o tangible, sino una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. En la actualidad se puede observar que Internet es un sistema internacional de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse, con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general, pero para llegar a esta visión se ha pasado por distintas fases o etapas.

Como lo afirma QUEVEDO “la historia de internet es bastante compleja”[10] por lo que siguiendo a esta autora se presentarán las cuatro etapas por las que ha atravesado lo que ahora se conoce como red de redes.

[10] Josefina Quevedo González, “Investigación y prueba del ciberdelito” (Tesis Doctoral, Barcelona, Universidad de Barcelona, 2017). 31.

1.2.1. Etapa militar.

En esta etapa se desarrolló una red conocida como DARPA, acrónimo de la expresión en ingles de *"Defense Advanced Research Proyects Agency",* Agencia del Departamento de Defensa de Estados Unidos, responsable del desarrollo de nuevas tecnologías para uso militar, que fue fundada en 1958 como consecuencia tecnológica de la llamada Guerra Fría y creó con carácter experimental una red informática llamada ARPANET[11] que es la abreviatura de *"Advanced Research Proyect Agency Net"* que traducido al español significa "Red de agencias de proyectos de investigación avanzada"[12] que estaba formada por los más prestigiosos centros de investigación académicos y militares del país, con el objetivo de compartir cualquier tipo de información necesaria disponible en cada uno de ellos[13] Esta red fue desarrollada y entró en servicio en el año 1969 para el complejo militar norteamericano[14].

La ARPANET surgió cuando el ejército de los Estados Unidos se planteó un supuesto probable y altamente posible ataque nuclear procedente de Rusia o desde cualquier otro enemigo de la unión. Por lo cual la inteligencia militar se planteo el supuesto que en un caso de conflicto bélico o similar, ¿cómo mantener las comunicaciones en el hipotético caso que el Centro de Control fuera destruido? Había que buscar nuevos cauces para mantener y desviar la información y que ésta pudiera llegar a sus destinatarios. Tras tiempo de investigación se pudo observar que construyendo una estructura de comunicación entre ordenadores interconectados que utilizara cualquier vía de comunicación (satélites, cable de teléfono, onda de radio, ...), la información podría navegar en el supuesto de una gran catástrofe bélica. Es decir, había

[11] Ibid. 32.
[12] Para su traducción se utilizó el traductor de Google.
[13] Quevedo González, "Investigación y prueba del ciberdelito". 32.
[14] Castillo González, *La estafa informática*. 17.

que crear una red[15] sin centro donde la señal no tuviera un único camino para pasar de un punto a otro.

Es así que la ARPANET funcionaba al haber conectado varias computadoras en diferentes centros de investigación en una red, sus principales objetivos fueron:

- Desarrollar una red que no se viese fuertemente debilitada en caso de que se perdieran partes físicas de la red, como podría ocurrir en caso de un conflicto nuclear.

- Que la red principal no debería ver afectadas sus prestaciones básicas con la incorporación de nuevos ordenadores dentro del sistema.

- Convertir a la red en un medio de comunicación independiente de la plataforma informática empleada lo cual aseguraría la compatibilidad ante cualquier circunstancia.

Para dar vida a estos requerimientos, el primer paso fue crear un “idioma” que hablaran los ordenadores para comunicarse entre sí. Es el origen del protocolo[16] de comunicación. Con la creación de estos protocolos de comunicación se garantizó la supervivencia de la red en caso que un enlace o canal fuera destruido ya que se prescindió de una red centralizada y se descentralizaron todas las redes conteniendo rutas alternativas de tal modo

[15] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc, consultada el 31/12/20.
[16] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc consultada el 31/12/20.

que cada computadora formaba un nodo en la distribución de la red, ofrecía servicios a otros nodos o usaba servicios de otros nodos dentro de la red.[17]

De lo anteriormente expuesto afirma QUEVEDO que nacieron los protocolos distribuidos que hacían posible que hubiera comunicación entre los extremos gracias a la existencia de múltiples caminos para que los mensajes alcanzasen su destino, cada mensaje era dividido en paquetes y estos paquetes se distribuían y circulaban por los múltiples enlaces y rutas de comunicación, siendo en el destino cuando se producía la reordenación de los paquetes entrantes y la confección del mensaje enviado.[18]

No obstante el procedimiento de transmisión de información anteriormente descrito, con el rápido crecimiento de la red hizo que su sistema de comunicación de protocolos distribuidos quedara obsoleto, dando paso al Protocolo TCP/IP: formado por el Protocolo de Control de Transmisión, que se abrevia "TCP", y el Protocolo de Internet, que se abrevia "IP", cuyo procedimiento de transmisión de información es el siguiente: El TCP divide en paquetes los mensajes generados en una computadora origen de la transmisión, asignándoles un numero de secuencia y la dirección de destino, y los recompone en el destino, mientras que el protocolo IP se ocupa del direccionamiento o transporte de los paquetes que pueden recorrer el camino por rutas diversas, incluso por tecnologías diferentes.[19]

---

[17] Quevedo González, "Investigación y prueba del ciberdelito". 33.
[18] Ibid.
[19] Cfr. https://www.youtube.com/watch?v=1pB2kan_AFk, y https://www.youtube.com/watch?v=KbHlWaeniHE, consultados ambos el 31/12/20, con Josefina Quevedo González, "Investigación y prueba del ciberdelito". 34

El TCP/IP (Transmission Control Protocol/Internet Protocol), se impone como protocolo de transmisión de la red y es el que se mantiene hasta nuestros días en el uso de la Internet. Las primeras versiones se publicaron en 1978, pero fue en 1981, cuando realmente fue terminado e implementado.[20]

1.2.2. Etapa académica.

En los años ochenta del siglo pasado, con los diversos sucesos políticos que llevaron a la caída de la Unión Soviética la ARPANET perdió la raíz para la que fue creada, es decir, servir como medio de comunicación en caso de una catástrofe nuclear, por ello fracasó su significado militar, pero se acentuó su uso para fines académicos y de investigación.

En la década antes dicha, surgen otras redes similares que pretenden dar cabida a investigadores no integrados en aquella; así surge la *"National Science Foundation"* que crea su red denominada NSFNET, partiendo de la tecnología de ARPANET, cuyo objetivo era la comunicación de científicos, investigadores y estudiantes para intercambiar ideas[21] lo que hace que se desliguen de ARPANET los militares, que pasaron a tener su propia red denominada *"Military Network o Military Net"* que se abrevia "MILNET" que es una nueva red creada por los Estados Unidos que se integra a la *Defense Data Network* (1982)[22].

Esta división generó que en 1983 la NSFNET absorbiera a ARPANET, formando el embrión de lo que hoy se conoce como la Internet; esto también fue consecuencia de que se extendió el uso de las computadoras al sector

---

[20] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc, consultado el 31/12/20.
[21] Castillo González, *La estafa informática*. 17.
[22] Quevedo González, "Investigación y prueba del ciberdelito". 34.

privado de los países de primer mundo, lo que fue posible por la simplificación de su manejo a través del "click" de un dispositivo denominado "mouse" y a través de la unificación de tecnologías y de lenguajes[23] de computadora.

En 1985 Internet ya era una tecnología establecida que se fue globalizando, cuando diversos países, sobre todo europeos, empezaron a conectar sus redes académicas y de investigación a esta infraestructura[24] aunque desconocida para la mayor parte de la población por la escasa implantación[25] de computadoras personales con acceso a la misma.

1.2.3. Etapa comercial.

En 1990 se estima que existían alrededor de 100,000[26] computadoras personales lo que hace que se sienten las bases de la nueva etapa de Internet de marcado carácter comercial, que poco a poco va ganando terreno a la vertiente académica; el científico británico Tim Berners-Lee, que trabajaba en el Laboratorio Europeo de Física de Partículas de Ginebra (CERN), crea el sistema de transmisión de imágenes, texto y sonido a través del hipertexto[27] denominado la *"Worl Wide Web"* conocida por sus siglas en ingles "WWW" o telaraña mundial creado para navegar por la red internet y acceder a miles de servidores donde encontrar información simplificada en su proceso de búsqueda y que proporciona información dotada de sonido, color, movimiento, etc. Contrario a la creencia popular WWW no es un sinónimo de internet, es un servicio que es parte de internet[28].

---

[23] Castillo González, *La estafa informática*.17.
[24] Quevedo González, "Investigación y prueba del ciberdelito". 35.
[25] González Hurtado, "Delincuencia informática". 27.
[26] Ibid.
[27] Ibid.
[28] Quevedo González, "Investigación y prueba del ciberdelito". 35.

El físico estadounidense Paul Kunz, de la universidad estadounidense de Stanford creó el 12 de diciembre de 1991 el primer sitio web de Internet, lo que supuso el inicio de su uso popular y el lanzamiento de un nuevo medio de comunicación[29]

En febrero de 1993 aparece el llamado *"Mosaic"* que es el primer navegador gráfico del mundo o motor de búsqueda, cuyo uso se generaliza en el año 1995.[30]

Es en ese momento, que internet comenzó a crecer más rápido que otros medios de comunicación, convirtiéndose en lo que hoy todos conocemos[31]: Una red que dispone de multitud de servicios o aplicaciones que constituyen las herramientas de trabajo del usuario de internet[32].

1.2.4. Etapa social.

Paulatinamente se han incorporado a internet nuevos protocolos y formas de uso que fomentan la comunicación entre usuarios particulares o grupos de usuarios y la participación en actividades cooperativas. Lo que en general se ha llegado a denominar Web 2.0, con servicios como diarios personales (blogs), las redes sociales, las enciclopedias colaborativas, etc., que han hecho de internet un medio activo en el que el usuario particular aporta y comparte información y ya no se limita a recibirla[33].

---

[29] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc Consultada el 31/12/20.
[30] En esto coinciden tanto el Dr. Francisco Castillo como la Doctora Josefina Quevedo González en sus respectivas publicaciones citadas a lo largo de este capítulo.
[31] González Hurtado, "Delincuencia informática". 27
[32] Quevedo González, "Investigación y prueba del ciberdelito", 36.
[33] Ibid. 37.

Se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos[34].

La Internet ha cambiado notablemente en su corta existencia, creciendo hasta convertirse en una infraestructura informática ampliamente extendida con capacidad para interconectar a todo el planeta, ignorando fronteras políticas y superando barreras geográficas, lingüísticas, culturales o religiosas, sentando las bases de lo que se conoce como *Sociedad de la Información.*[35]

No se puede concluir diciendo que Internet ha acabado su proceso de cambio. Aunque es una red por su propia denominación y por su dispersión geográfica, su origen está en las computadoras, y con el paso del tiempo seguirá evolucionando en la medida que nuevos dispositivos tecnológicos la incorporen y faciliten que las comunicaciones, que como puede apreciarse ya forman parte de la vida en sociedad de los seres humanos, por ello es una autentica herramienta de interacción social que a futuro requiere una verdadera tutela en cuanto a su funcionamiento o una regulación jurídico penal que imponga sanciones por la realización de hechos delictivos por medio de su entorno.

1.3. Breve reseña histórica de la delincuencia informática.

Debe tenerse en cuenta que en este apartado no existe una secuencia clara de hechos cronológicamente realizados, ya que hasta la década de los ochenta del siglo pasado tanto la Doctrina penal como los legisladores de distintos países comenzaron a tener conciencia que la red de redes no era una

[34] Ibid.
[35] Ibid. 38.

espacio de paz y armonía donde el ser humano pudiera concretar sus más grandes aspiraciones, sino que en dicha infraestructura era posible la realización de hechos delictivos, tanto los considerados como parte del Derecho penal liberal, es decir, conductas ilícitas tradicionales cometidas "por medio de internet" como verdaderos tipos penales autónomos que han hecho necesaria una regulación especial o reformas a los códigos penales de distintas naciones o Estados.

1.3.1. A nivel mundial

Si bien es cierto, como lo afirma GONZALEZ, durante los primeros pasos de la informática moderna no aparece en la sociedad la necesidad de una regulación específica en el ordenamiento jurídico en este ámbito ya que se trataba de investigaciones privadas con escasa trascendencia pública o bien de proyectos de universidades o administraciones públicas (etapa académica) pero se podían vislumbrar las posibilidades en negativo de los avances técnicos de la mecanización de cálculos en el campo militar para la decodificación de mensajes cifrados.[36]

En los años ochenta del siglo pasado, debido al incremento en la producción de computadoras personales, se dio el surgimiento de la piratería de software, dando lugar a las primeras infracciones contra la propiedad intelectual[37].

En la década de los noventa la expansión de la internet llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como la pornografía infantil o discursos racistas o xenófobos. Serán precisamente las conductas vinculadas a la difusión de contenidos ilícitos las

[36] González Hurtado, "Delincuencia informática". 24.
[37] Quevedo González, "Investigación y prueba del ciberdelito". 35.

que más pueden aprovecharse de la enorme implantación que tiene la red a nivel mundial, así como sus características técnicas dificultan su descubrimiento, persecución y prueba.[38]

En 1995, en los Estados Unidos de América, cuando el uso de las primeras computadoras personales se encontraba popularizándose con el uso del Windows versión 3.1, la mayoría de los usuarios se quejaba del poco espacio de almacenamiento de datos que tenía el mismo y de memoria RAM[39] que las PC´s tenían en esos años. Por lo cual una empresa denominada Syncronys fue la desarrolladora de un programa titulado "SoftRAM" que prometía a los usuarios del sistema operativo antes mencionado duplicar la capacidad de la memoria RAM, por ende modificaba la velocidad de respuesta del equipo, vendiéndose cada programa por la cantidad de ochenta Dólares cada copia vendiendo alrededor de seiscientos mil unidades del programa sucediendo que dicha duplicación de memoria era falsa pues no producía ningún efecto en el sistema, siendo esta la primera estafa informática registrada de la historia actual[40].

Posteriormente en el año 2004 las oficinas del banco japonés Sumitomo Mitsui fueron atacadas por un grupo de sujetos por medio de una herramienta informática denominada keylogger[41] utilizada para robar las contraseñas de

---

[38] Ibid. 36.
[39] Sigla de Random Access Memory ('memoria de acceso aleatorio'), memoria principal de la computadora, donde residen programas y datos, sobre la que se pueden efectuar operaciones de lectura y escritura. https://www.google.com.sv/?gws_rd=cr,ssl&ei=l1_9WOGdNcPemAH6lpCwDw#q=ram+que+signific sin autor, consultada en 23/04/2017.
[40] Se considera la primera estafa informática de la historia en vista que estaba relacionada con un objeto informático sobre el que recaía la conducta. La información de este párrafo ha sido interpretada de la web https://hipertextual.com/2016/05/softram-historia-duplicadores-ram, sin autor, consultada el 23/03/17.
[41] Derivado del inglés: key ('tecla') y logger ('registrador'); 'registrador de teclas' es un tipo de

las cuentas bancarias, con lo cual lograron estafar alrededor de 420 millones de dólares, sin embargo, los sujetos activos de este ilícito no supieron cómo deshacerse de tanto dinero y lo depositaron en distintas cuentas en otros bancos; así, al tratar de depositar 27 millones de dólares en una cuenta en el Banco de Israel, el ciudadano israelí Yeron Belondi fue detenido por las autoridades de dicho país, sucediendo así con los demás miembros de esta red que intentaron depositar en diferentes bancos el dinero procedente de esta estafa informática.[42] Por lo que se considera esta la primera estafa registrada, realizada contra un banco utilizando un programa que permite una manipulación tal que produce un daño económico a un tercero con una transferencia no consentida y con ánimo de lucro.

Se debe resaltar un aspecto político muy importante, es el caso del líder norcoreano Kim Jong Un quién, ante las múltiples sanciones impuestas por Naciones Unidas por el desarrollo de armas nucleares y constantes violaciones a los derechos humanos de los nacionales norcoreanos, ha tenido que buscar fuentes de financiamiento para su carrera armamentista por lo cual ha desarrollado un programa de talentos entre los jóvenes escolares que destacan por su especial inteligencia en las matemáticas, quienes son entrenados por una agencia especial del gobierno a fin de convertirse en verdaderos hackers informáticos[43] para realizar ataques a bancos y empresas a través del internet alrededor del mundo para obtener dinero para el régimen.

---

programa o un dispositivo externo específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

[42] Información parafraseada de la web http://www.sopitas.com/378293-los-estafas-realizadas-eninternet-mas-grandes-de-la-historia/ , sin autor, y de la web https://www.youtube.com/watch?v=7qaoSIeySzI consultadas ambas el 23/04/2017.

[43] Como lo pone en evidencia el documental de la DW colgado en https://youtu.be/3ZTrnnV1AAk consultada el 28 de mayo de 2021.

Este grupo especial de hackers norcoreanos están vinculados con el virus ***"wannacry"*** el cual, en el año 2017, secuestro la información de computadoras de hospitales, escuelas, empresas y bancos, en la cual el pirata informático exigía para devolver el ingreso a la computadora la cantidad de trescientos Dólares americanos por la primera hora, luego de la misma exigía el doble, es decir, seiscientos Dólares Americanos y así sucesivamente según el tiempo aumentaba; esta circunstancia genero daños a las entidades que fueron víctimas por varios miles de Dólares.[44] Según las investigaciones existentes se considera que los ataques hechos por estos hackers norcoreanos han defraudado más de dos mil millones de Dólares Americanos en diversos ataques cibernéticos que han sido alertados por parte del FBI.[45]

Lo dicho en párrafos anteriores hace reflexionar que también ciertos Estados están utilizando o promoviendo la existencia de ciberdelitos como forma de financiamiento o como estrategia para desestabilizar tanto a instituciones como a la población en general o con fines militares, lo que puede verse como una doble moral ya que por un lado hay presiones para castigar la ciberdelincuencia mientras que por otro lado se promueve la misma para fines oscuros, esto se expresa en vista que hay información pertinente que establece que la vulneración existente en plataformas sujetas a soporte de Microsoft fue lo que dio origen a los daños del "wannacry" lo cual era de conocimiento del Departamento de Estado de los Estados Unidos, pero que se mantenía en secreto como una forma de poder ser utilizado como arma, hasta que fue empleado por Corea[46] del Norte.

---

[44]Ver https://youtu.be/s6epDe7lqno, consultada el 29 de mayo de 2021.
[45]Verhttps://www.delitosfinancieros.org/corea-del-norte-y-los-ataques-ciberneticos-a-instituciones-financieras/#:~:text=actores%20cibern%C3%A9ticos%20patrocinados%20Corea%20del,en%20m%C3%A1s%20de%20150%20pa%C3%ADses. Consultada el 29 de mayo 2021.
[46] Ver https://youtu.be/s6epDe7lqno, consultada el 29 de mayo de 2021.

Para finalizar este apartado es importante hacer notar que países como: Alemania, los Estados Unidos de Norteamérica, España, México y Costa Rica, por citar algunos, fueron los países pioneros en regular los delitos informáticos como una forma de garantizar la protección de sus ciudadanos contra la cibercriminalidad. No obstante, esta forma de crimen trasciende las fronteras nacionales volviendo necesario que más Estados realicen una policita criminal encaminada a contrarrestarla.

1.3.2. A nivel nacional.

En El Salvador en el año dos mil doce la Comisión de Seguridad Publica y Combate a la Narco Actividad analizó la necesidad de realizar reformas al Código Penal a fin de prevenir y reprimir las actividades delincuenciales que pudieran cometerse mediante el uso de la tecnología informática, ya que al no encontrarse suficientemente reguladas expresamente en el Derecho Penal salvadoreño generan inseguridad jurídica para las personas naturales y jurídicas que las utilizan e impunidad para quienes la cometen[47]. Con esto lo que se pretendía es que estas actividades delictivas no quedaran en la impunidad o sirvieran de mecanismo para que bandas de crimen organizado pudieran utilizar tecnología de información para cometer delitos, pero dicha propuesta de reforma a la legislación no genero ninguna iniciativa de ley, ni mayores discusiones por lo que fue archivada en la Asamblea Legislativa.

[47]Alba De Leiva “Analizan penalizar delitos cometidos a través de la tecnología informática” en Asamblea Legislativa de El Salvador (sitio web), 14 de agosto de 2012, consultada el 27 de junio 2015, http://www.asamblea.gob.sv/noticias/legislatura-2012-2015/noticias/analizan-penalizar-delitos-cometidos-a-traves-de-la-tecnologia-informatica.

No obstante, en el año 2015 se da un suceso sin precedente en la historia de El Salvador, el cual fue el primer ciberataque documentado, perpetrado contra el matutino “La Prensa Gráfica” en el cual se hace una clonación de la página oficial y se desprestigia desde la misma a un alto Ejecutivo de ese periódico además de que se publicaron otras noticias falsas; en el ámbito juridicial fue conocido como “Caso Troll Center” donde se vinculó a ciertos políticos como las personas que estaban detrás de los hechores. Este ataque, produjo como efecto que los Legisladores Salvadoreños volvieran a discutir la necesidad de una regulación de las actividades de los particulares en el internet y establecer categorías de bienes jurídicos protegidos penalmente de actos hechos por medio o en de la red.

La discusión parlamentaria a que se hizo referencia en el párrafo anterior concluyo en el año 2016 con la vigencia del D.L. 260 del 04 de febrero publicado en el D.O. 40 de fecha 26 de febrero todos del mismo año que se promulgo la LECDIC constituyéndose en la primera ley de la República en regular y reprimir los hechos delictivos cometidos en la red a través de las TIC´S.

Sin embargo, a cinco años de vigencia de la LECDIC no se han conocido casos llevados a los tribunales en cumplimiento de dicha normativa, según datos oficiales de la Fiscalía General de la República las denuncias hasta el año dos mil diecinueve, por ejemplo: De los delitos de Estafa Informática y Hurto de Identidad presentaban los siguientes valores a nivel nacional [48]:

[48] Según Resolución de solicitud de información Nº 103-UAIP-FGR-2020, de UNIDAD DE ACCESO A LA INFORMACIÓN PUBLICA de las doce horas con treinta minutos del día dos de marzo de dos mil veinte.

Tabla 1: Casos iniciados en sede Fiscal

CANTIDAD DE CASOS INICIADOS POR LOS DELITOS DE ESTAFA INFORMÁTICA (10 L.D. INFORMÁTICOS) Y HURTO DE IDENTIDAD (22 L.D. INFORMÁTICOS), A NIVEL NACIONAL, DEL AÑO 2016 AL 2019; DETALLADO POR AÑO Y DELITO.				
DELITOS	**Año 2016**	**Año 2017**	**Año 2018**	**Año 2019**
Estafa informática (10 L.D. Informáticos)	0	6	7	2
Estafa informática (10 Lit. a. L.D. Informáticos)	1	1	0	0
Estafa informática (10 Lit. c. L.D. Informáticos)	1	0	0	0
Hurto de identidad (22 L.D. Informáticos)	19	45	82	10
Total	**21**	**52**	**89**	**12**

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 25022020

La información presentada en la tabla anterior llama la atención por el escaso uso de esta herramienta legal para la defensa de bienes jurídicos en el ciberespacio por parte de la población salvadoreña que prácticamente ya es parte de la sociedad de la información desde comienzos del siglo XXI, cuando se inició la conformación de las grandes empresas proveedoras de los servicios de internet y telefonía celular de Latinoamérica, como lo son: Movistar, TIGO y CLARO -por citar las más influyentes- que brindan servicios desde México, pasando por el istmo centroamericano, Panamá y Colombia; así como el abaratamiento de instrumentos informáticos para el uso de toda la población como: Las computadoras, las Tabletas y los aparatos telefónicos de tercera generación los cuales se encuentran al alcance de todas las clases sociales.

Todo lo cual aunado con el uso y proliferación de las redes sociales, ha permitido un acceso y desarrollo de una sociedad virtual en el país, la cual tiene un desarrollo dinámico y expansivo pues cada vez son más usuarios los que demandan servicios de internet, aparatos telefónicos o computadoras de

mejor capacidad, calidad y comodidad económica que les permita estar “en línea”; pero paralelamente esto genera un riesgo de actividades delictivas realizadas por estos medios electrónicos.

Por las razones esgrimidas en los párrafos precedentes, son muy alarmantes ya que, si se contrasta esta información de la Tabla 1 con el número de casos judicializados por estos mismos delitos y en el mismo periodo, no puede denotarse una efectividad por parte del ente persecutor de las conductas delictivas del sistema penal salvadoreño se obtiene la siguiente información[49]:

Tabla 2: Casos Judicializados por Fiscalía

CANTIDAD DE CASOS JUDICIALIZADOS, POR LOS DELITOS DE ESTAFA INFORMÁTICA (10 L.D. INFORMÁTICOS) Y HURTO DE IDENTIDAD (22 L.D. INFORMÁTICOS), A NIVEL NACIONAL, DEL AÑO 2016 AL 2019; DETALLADO POR AÑO Y DELITO.				
DELITOS	**Año 2016**	**Año 2017**	**Año 2018**	**Año 2019**
Estafa informática (10 L.D. Informáticos)	0	0	1	1
Estafa informática (10 Lit. a. L.D. Informáticos)	1	0	0	0
Estafa informática (10 Lit. c. L.D. Informáticos)	0	1	0	0
Hurto de identidad (22 L.D. Informáticos)	0	0	2	0
Total	**1**	**1**	**3**	**1**

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 25022020

Se puede apreciar en la tabla 2 que hay un reducido número de casos judicializados, con relación a la cantidad de denuncias que existieron sobre estos ilícitos en el mismo periodo de tiempo en la Fiscalía, lo que pone en evidencia que existen ya casos de ciberdelitos en El Salvador los cuales o no han tenido un buen tratamiento procesal en los tribunales de justicia o existen deficiencias o limitaciones para realizar las debidas investigaciones.

[49] Idem.

Un hecho notorio fue el ataque al sistema de control y registro de notas de la Universidad de El Salvador denominado “Prometeo” por parte de un grupo de Hackers que en el mes de julio de 2020 alteraron los registros de notas de la mayoría de la población estudiantil, sin que a la fecha de la redacción de este capítulo se haya esclarecido el hecho por parte de la Fiscalía General de la República.

Así mismo hay que hacer notar que las tablas de información antes presentadas van a diferir grandemente este año en el cual desde inicios del mes de agosto la Superintendencia del Sistema Financiero inició una serie de publicaciones, siendo la primera del 13 de agosto del corriente año, en la cual advierten a la población de posibles estafas informáticas hechas por gente inescrupulosa que se hacen pasar por personeros de entidades bancarias enviando correos electrónicos, utilizando redes sociales o mensajes de texto por la aplicación de *WhatsApp* solicitando información sensible de clientes de entidades bancarias, la cual puede dar como resultado que se afecte patrimonialmente a las personas que brinden la información. Según datos de esta entidad, cada mes se presentan entre 20 a 25 denuncias de fraudes sufridos por usuarios de la banca salvadoreña, principalmente por vía de redes sociales, mensajes de WhatsApp y correos electrónicos.[50]

[50] https://www.laprensagrafica.com/economia/El-Salvador-advierten-de-fraudes-bancarios-por-correos-electronicos-20210822-0026.html, consultado el día 08/SEP/21

SUPERINTENDENCIA DEL
SISTEMA FINANCIERO

AVISO

Ante la circulación de mensajes enviados por medio de correos electrónicos y redes sociales, por remitentes que suplantan la imagen de entidades financieras, solicitando a través de enlaces, la actualización de datos relacionados con cuentas bancarias, advertimos:

- Ningún banco o entidad financiera solicitará actualizar datos, por medio de enlaces enviados por correo electrónico o redes sociales, ni pedirá códigos, contraseñas o claves de seguridad de cuentas bancarias.

Hacemos un llamado a la población a mantenerse alerta para evitar ser víctimas de actos irregulares que pueden perjudicar sus finanzas.

Cualquier consulta o duda relacionada a productos y servicios financieros que brindan las entidades financieras supervisadas por esta Superintendencia, pueden contactarse con nuestra Oficina de Atención al Usuario, llamando al teléfono 2261-8400 opción 1 y escribiendo al correo electrónico: atencionalusuario@ssf.gob.sv o al número de WhatsApp: 7840-9741.

13 de agosto de 2021

Fig. 1: Publicación de la Superintendencia del Sistema Financiero advirtiendo sobre la realización de hechos delictivos

A principios de agosto del corriente año, el Banco Agrícola dio a conocer sobre la existencia de una circulación de estos correos electrónicos supuestamente enviados por la institución con enlaces para hacer gestiones y de llamadas

telefónicas a sus clientes, con la finalidad de defraudarlos[51]. No obstante, dicha problemática se ha alzado ya que el 7 de septiembre de este año el Banco Agrícola informó a la población de que debido al incremento de denuncias de clientes por casos de fraude ha reforzado sus medidas de seguridad ya que su equipo de ciberseguridad ha desmontado alrededor de 1,300 sitios web dedicados a diversas modalidades de estafa[52].

Según periódico de circulación nacional entre las modalidades de fraude que se han detectado están llamadas telefónicas en las que mediante engaños piden datos personales a los usuarios, mensajes de texto (smishing) e incluso la simulación de correos firmados por instituciones en donde piden entrar para validar las cuentas, lo cual permite a los estafadores capturar la información y acceder a cuentas del Banco Agrícola; personeros de dicha entidad afirman que no ha existido filtración de ninguna base de datos y que existe seguridad en los depósitos hechos ya que desde el año 2016 se invirtió $55 millones en un centro de operaciones que permite hacer transacciones "rápidas y seguras"[53].

Así mismo la Asociación Bancaria Salvadoreña (ABANSA) ha pedido a la ciudadanía estar pendientes de este tipo de correos y no ingresar a ningún enlace que ellos contengan o descargar cualquier archivo adjunto, ya que cada usuario de la banca es responsable de no proporcionar sus claves de banca en línea por esta vía, ya que las entidades Bancarias no tienen responsabilidad alguna con lo que está ocurriendo hoy. Sin embargo, el Banco Agrícola desde que se originó esta ola de denuncias, ha dado apoyo a 167 clientes que han

---

[51] Ibid.
[52]https://www.laprensagrafica.com/economia/Banco-Agricola-alerta-a-clientes-ante-alza-de-denuncias-por-fraude-20210906-0078.html, consultado el 08/09/21.
[53] Ibid.

sufrido este tipo de estafas, que los han dejado con saldos a “cero”, pero el cliente debe denunciar estas irregularidades también ante las autoridades de seguridad como la Fiscalía General de la República, porque son constitutivas de delitos[54] informáticos.

La reacción de la población no se ha hecho esperar ya que algunos clientes del Banco Agrícola han denunciado en Twitter las sustracciones de dinero en sus cuentas bancarias; estas denuncias fueron realizadas en redes sociales y según los denunciantes desde hace varios días están ocurriendo estos problemas, ya que han recibido correos electrónicos o mensajes en sus celulares solicitándoles información personal[55], y otros denunciaron que les sacaron dinero en sus cuentas de ahorro sin haber recibido llamadas ni formularios supuestamente enviados por la Institución financiera, sino que se hicieron trasferencias desde su cuenta sin ella conocer a las personas a las que se les hizo dicha transferencia[56].

Finalmente, al momento de redacción de este capítulo, se conoce sobre la detención por el delito de fraude financiero de un experto en informática, quien fuera capturado por supuestamente enviar correos electrónicos falsos a muchos usuarios de bancos, el pasado 1 de septiembre del corriente año, pero después de ser llevado a la División Central de Investigaciones (DCI) de la Policía, fue liberado no sin antes ser decomisados sus teléfonos celulares sobre los cuales la Fiscalía realizará las pericias técnicas necesarias[57]. Lo

---

[54]https://www.elsalvador.com/noticias/negocios/estafas-bitcoin-bancos/871906/2021/, consultada el 08/09/21.
[55]https://www.elsalvadortimes.com/articulo/sucesos/clientes-denuncian-que-algunas-cuentas/20210823153256081461.html, consultado el 07/sep/21
[56]https://www.elsalvadortimes.com/articulo/sucesos/maestra-pierde-salario/20210830122530081561.html, consultado el 07/sep/21
[57]https://www.elsalvadortimes.com/articulo/sucesos/capturan-acusan-especialista-em-sistemas-informacion/20210901105915081592.html, consultado el 07/septiembre/21.

expresado pone en evidencia que la Policía Nacional Civil tiene ciertos protocolos de investigación para los delitos informáticos y hay capacidad técnica para su persecución, pero es un reto este tipo de situaciones para llegar a los responsables del mismo.

En este apartado se han puesto en evidencia casos tanto a nivel mundial como a nivel nacional que están registrados en medios noticiosos o soportes de autoridades gubernamentales, pero existe una gran "cifra negra" de casos que no son denunciados por temor al desprestigio o a la fama mercantil de una empresa que sea víctima de estos ataques, máxime que no existe una respuesta gubernamental rápida que garantice a las víctimas un resarcimiento civil y a la vez que los responsables sean encontrados, apresados y enjuiciados por la realización de estas conductas delictivas en o por medio de la internet.

Lo dicho en el apartado anterior se vuelve aún más alarmante si se piensa que en el país desde el siete de septiembre de 2021 se convierte en el primer país del mundo en adoptar la "Bitcoin" como moneda de curso legal, ya que se pueden realizar pagos a través de un monedero digital[58] conocido como ***"Chivo Wallet"*** la cual ha generado conflictos con las grandes distribuidoras de aplicaciones: "Playstore" de Google y "App Store" de Apple debido a fallas y sin disponibilidad para varios modelos de teléfonos celulares[59], solamente los más recientes, en muchos de los casos de alta gama dejando por fuera las gamas bajas y media que son los más populares del mercado[60] a los cuales

[58] https://www.bbc.com/mundo/noticias-america-latina-58482830 consultado el 15/septiembre/21
[59] https://diario.elmundo.sv/chivo-wallet-sigue-con-fallas-y-sin-disponibilidad-para-varios-modelos-a-una-semana-de-lanzamiento/ consultado el 15/septiembre/21
[60] Ibid.

tiene acceso la mayoría de la población[61] quienes a la vez pueden ser víctimas potenciales de la delincuencia organizada transnacional.

Así también con la popularidad que está teniendo la aplicación ***"Chivo Wallet"*** en los aparatos telefónicos que si funciona y la posibilidad de utilizar los treinta dólares que el gobierno brinda para su uso automático, ha generado que muchos salvadoreños pidan a otro que ayude con la descarga de dicha aplicación o el retiro de ese dinero para cobrarlo en efectivo lo cual ha provocado desde finales de septiembre e inicios del mes de octubre de este año que a muchos ciudadanos se les haya suplantado la identidad por lo cual el Director de la PNC ha declarado que existen varias investigaciones activas vinculadas con delitos informáticos[62].

Por su parte el Fiscal General de la Republica actual, Licenciado Rodolfo Delgado, en reunión con los miembros de la Comisión de Seguridad de la Asamblea Legislativa, quienes estudian una propuesta de reformas a la Ley contra Delitos Informáticos y Conexos, sostuvo que este año 2021 se ha elevado los casos de delitos informáticos a tal grado que solo este año se han recibido 5,394 denuncias sobre delitos informáticos donde la mayor parte de estas, unas 2,000, se registraron en agosto pasado y están "relacionados a vulneraciones de usuarios del sistema financiero. Por tal razón, solicitó a los

---

[61] Solo en la marca Huawei, que es una de las más usadas en El Salvador dicha aplicación estuvo disponible desde la tarde del día siete de septiembre del 2021 en la tienda "App Gallery" que permite la descarga de aplicaciones en los dispositivos de la marca mencionada https://diario.elmundo.sv/chivo-wallet-sigue-con-fallas-y-sin-disponibilidad-para-varios-modelos-a-una-semana-de-lanzamiento/

[62] https://diarioelsalvador.com/policia-nacional-civil-y-fiscalia-investigaran-casos-de-suplantacion-de-identidad-en-la-chivo-wallet/143668/ consultado el 30 de noviembre de 2021.

legisladores la urgencia de poseer una ley actualizada al respecto “para enfrentar este tipo de criminalidad”[63].

Los carteles de la droga mexicanos utilizan la Bitcoin como mecanismo para lavar dinero, ya que en el mundo no es una divisa reconocida ni controlada ni mucho menos vigilada, por lo cual los grupos delincuenciales la utilizan como forma de pagar pequeñas cantidades de dinero a sus colaboradores sin dejar rastro o huella de la transacción[64] y en países en vía de desarrollo como El Salvador la Ley del Bitcoin atraerá al crimen organizado en la medida que la población tengan confianza en la criptomoneda la cual dejará de ser tan volátil y brindará estabilidad, para crear una red de intercambio principalmente en las remesas familiares enviadas desde Estados Unidos, así como el anuncio del gobierno de que los extranjeros que inviertan en bitcoin tendrán exoneración de impuestos y tendrán residencia permanente en el país, lo que formaría un paraíso fiscal en Centroamérica.[65]

Lo cual vuelve urgente hacer un estudio jurídico, para determinar en qué medida el sistema penal de El Salvador está capacitado para investigar y probar la existencia de ciberdelitos a fin de proteger a la población de fraudes u otro tipo de acciones delictivas realizadas a través de las TIC´S que afecten a la seguridad jurídica nacional.

---

[63] https://www.elsalvador.com/noticias/nacional/fiscal-impuesto-rodolfo-delgado-reformas-delitos-informaticos-diputados/899117/2021/ consultado el 30 de noviembre de 2021.
[64] https://youtu.be/6E__nE3eSBI consultado el 16 de septiembre de 2021.
[65] https://youtu.be/8ThpWu_li6U consultado el 16 de septiembre de 2021.

CAPITULO II: LA INFORMÁTICA EN GENERAL Y UNA APROXIMACION A SU RELACIÓN CON EL DERECHO

SUMARIO: 2.1. Generalidades sobre la informática. 2.1.1. Funcionamiento de las maquinas basadas en las TIC´S. 2.1.1.1 Del Hardware. 2.1.1.2 Del Software. 2.1.1.3. Del Procesamiento de datos. 2.1.1.4 De los datos. 2.1.2. Sistema Informático y redes informáticas. 2.1.3. El Ciberespacio. 2.1.4. Redes Sociales. 2.1.5 Nuevas tecnologías. 2.1.6. Las páginas web y la Deep Web**.** 2.2. Visión general del derecho ante las TIC´S

RESUMEN:

En este capítulo se desarrollaran *latu sensu* temáticas referentes a la informática, definiéndola y resaltando sus aspectos más generales, así como los componentes de las computadoras y otras máquinas diseñadas en tecnología basada en las TIC´S que permiten la interacción o comunicación de las personas en el ciberespacio; pero no todo es color de rosa como se verá pues lo que se conoce como las nuevas tecnologías tiene un lado oscuro como lo es la "Deep Web" o "red profunda" de la cual se explicará su funcionamiento. Finalmente se hará una aproximación de la relación de la informática con el mundo jurídico, principalmente en lo relativo a las respuestas a los hechos ilícitos cometidos a través o sobre la información con las Tecnologías de la Información y la Comunicación.

2.1. GENERALIDADES SOBRE LA INFORMATICA.

La palabra "informática" deviene de la palabra francesa *"informatique"* que es la síntesis de origen francés de las palabras "información" y "automática"[66] que para TELLEZ su unión se traduciría en: Un "Conjunto de conocimientos

[66] Alberto Enrique Nava Garcés, *Delitos informáticos* (México: Porrúa, 2016). 7.

científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores[67]", ahora hablando en forma general como ciencia el mismo autor citado considera que la informática "es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones[68]"

El origen de la informática era conseguir la mecanización de cálculos matemáticos, de tal forma que se pudiesen llevar a cabo gran número de cálculos con poco esfuerzo humano, por ello concluye GONZALEZ HURTADO que la informática está basada principalmente en las matemáticas, como un resultado evolutivo de las mismas, pero también con la física de los materiales, el álgebra, la lógica y muchas otras ciencias teóricas que dan como resultado la ciencia aplicada que hoy se conoce como la informática.[69]

Lo dicho anteriormente tiene mucho sentido, pues como ya se dijo en el capítulo anterior fue durante la segunda guerra mundial que se pudo crear una maquina programable, que fue el antecedente de las computadoras actuales, pero desde ese momento a la actualidad se ha buscado la miniaturización de los componentes y lograr la máxima potencia de los mismos, por eso confluyen en el desarrollo de la informática otras ciencias.

La computadora es una "maquina electrónica" que funciona por medio de programas o aplicaciones adecuadas, con señales objeto de elaboraciones

---

[67] Julio Téllez Valdés, *Derecho informático*, 2. Ed, Serie jurídica (México: McGraw Hill, 1996). 5. Se debe de hacer notar que en Latinoamérica el concepto de ordenador no es usado para referirse a un equipo automatizado de datos, sino que el concepto utilizado es el de "computadora" para hacer referencia a aquella máquina electrónica capaz de almacenar información y tratarla automáticamente mediante operaciones matemáticas y lógicas controladas por programas informáticos.

[68] Ibid.

[69] González Hurtado, "Delincuencia informática". 21-22.

digitales conocidas como “bit”, elaborando los datos con base en un lenguaje lógico (o de computadora) basado en un sistema binario, que asume las situaciones 1 ó 0 en cada bit. A su vez la computadora se identifica en sentido estático con el ***“Hardware”*** que es físicamente la máquina y sus componentes, mientras que en el sentido dinámico opera por medio del ***“Software”*** que son los programas o aplicaciones que permiten en funcionamiento y la elaboración de datos, basadas sobre complejos grupos de instrucciones denominados ***“algoritmos”***. Según los objetivos de esta investigación se desarrollará los primeros dos conceptos que son utilizados en todas las TIC´S, ya que la explicación de los algoritmos escapa de los límites de esta investigación.

2.1.1. Funcionamiento de las maquinas basadas en las TIC´S

Se debe de entender que una computadora es una “máquina electrónica, analógica o digital, dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas informáticos”[70]

Se debe de hacer notar que la máxima expresión que una máquina que calcula, almacena, crea, transmite, recibe y toma decisiones sobre la información proporcionada por el ser humano es la computadora y la misma también es programable por el hombre o es tiene por objeto la utilización de programas y aplicaciones creadas o desarrolladas por grandes empresas tanto como por individuos independientes que inventan las mismas para resolver situaciones determinadas. No obstante esto, los teléfonos inteligentes, las tabletas, los reproductores de sonido e imágenes, los IPad, los IPod, los servidores, las máquinas que proporcionan las telecomunicaciones, entre

[70] González Hurtado, "Delincuencia informática". 31.

otros son sistemas informáticos que se basan en el mismo tipo de funcionamiento a que se hará referencia, con algunas particularidades especiales en atención al tipo de aparato.

2.1.1.1 Del "Hardware"

Se entiende como el conjunto de todas las unidades físicas que componen una computadora, es decir, el conjunto de los dispositivos materiales y técnicos que son necesarios para el desenvolvimiento del procesamiento de datos.

El Hardware puede distinguirse en dos ámbitos, que se encuentran unidos por canales: **a) La Unidad Central (CPU)**, que consiste en la unidad de control, en el mecanismo de cálculo y en el mecanismo de almacenamiento, es lo que se conoce como el cerebro de la computadora por ser el lugar donde se suma, se multiplica y se compara, así como son interpretadas las órdenes específicas de un programa o aplicación, ordenadas y ejecutadas las necesarias operaciones. En la actualidad los CPU usan microchips, por lo cual se habla de ***microprocesadores*** que han permitido reducir el espacio físico que utiliza una computadora y permiten la facilidad del transporte de las mismas; y **b) en Unidades periféricas**, que son aparatos de entrada (por ejemplo, el teclado), en aparatos de emisión o salida (p.e. la pantalla) y en contenedores externos o aparatos externos de almacenamiento de datos (p.e. discos duros, CD´s).[71]

2.1.1.2 Del Software

La RAE define software como el "conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora". Por software nos referimos al equipamiento lógico (en contraposición al

[71] Castillo González, *La estafa informática*. 21.

equipamiento físico) de un sistema informático y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de tareas específicas para las que están diseñados los elementos físicos del sistema (hardware)[72]

Se conoce como software o soporte lógico - formal de un sistema informático, que comprende el conjunto de los componentes lógicos, que incluyen tanto a las aplicaciones como a los datos, necesarios que hacen posible la realización de tareas específicas o que permiten que operen, en contraposición a los componentes físicos que son llamados hardware. En palabras de CASTILLO el Software es el balcón espiritual del procesamiento electrónico de datos[73].

Existe multitud de software con diferentes finalidades. El principal software presente en los sistemas informáticos actuales es el que realiza las funciones de sistema operativo, y es la base sobre la que el resto de los tipos de software trabajan; entre muchas otras aplicaciones informáticas, podemos señalar los procesadores de textos, los videojuegos, los programas de diseño gráfico o incluso las aplicaciones de programación del propio software. Debe además extenderse la idea de software a las aplicaciones que permiten la interacción hombre-máquina en cualquier sistema informático, es decir, el menú desde el que se gestiona un teléfono móvil, el de una videoconsola, un cajero automático, o una fotocopiadora electrónica suponen, con mayor o menor complejidad técnica, un software para su utilización.[74]

---

[72] González Hurtado, Delincuencia informática. 33.
[73] Castillo González, *La estafa informática*.26.
[74] González Hurtado, "Delincuencia informática". 33.

2.1.1.3. Del Procesamiento de datos

Se entiende un proceso que se realiza con la ayuda de una computadora, que consiste en almacenar datos y luego procesarlos, supone la existencia de objetos sobre los cuales ella se ejerce y cuyo cambio de condición es el objeto de la acción. La definición de "procesamiento de datos" es genérica que abarca todas las operaciones que pueden realizarse sobre el objeto, independientemente del contenido de la operación y de quien la haga, las cuales pueden distinguirse en tres grupos:

A) **Procesos de transformación:** Que son aquellas operaciones por las cuales se transfieren los datos de un contenedor de datos a otro, independientemente de que con ello se cambie el código originalmente asignado.
B) **Procesos de cálculo:** Son aquellos de transformación de datos en sentido estricto, porque se crea un nuevo objeto (un nuevo dato) por la conexión de un dato con otro.
C) **Procesos de orden:** Son todas las operaciones en las cuales no varían los objetos, pero si varía el orden o acomodo de ellos. P.e. Las operaciones de orden de mezclar, separar o clasificar los datos existentes[75].

2.1.1.4 De los datos

Hasta este momento en la investigación se ha hecho referencia en varias ocasiones al concepto "datos", pero no se ha determinado una definición de los mismos, por lo cual es necesario hacer una breve referencia a ellos, para que quede claro que debe de entenderse por este concepto.

[75] Castillo González, *La estafa informática*. 29-30.

En informática, los datos son representaciones simbólicas (vale decir: numéricas, alfabéticas, algorítmicas, etc.) de un determinado atributo o variable cualitativa o cuantitativa, es decir, es la descripción codificada de un hecho empírico, un suceso, una entidad; por ello los datos son la información (valores o referentes) que recibe la computadora a través de distintos medios, y que es manipulada mediante el procesamiento de los algoritmos de programación. Su contenido puede ser prácticamente cualquiera: estadísticas, números, descriptores, que por separado no tienen relevancia para los usuarios del sistema, pero que en conjunto pueden ser interpretados para obtener una información completa y específica.

En los lenguajes de programación, empleados para crear y organizar los algoritmos que todo sistema informático o computacional persigue, los datos son la expresión de las características puntuales de las entidades sobre las cuales operan dichos algoritmos. Es decir, son el input inicial, a partir del cual puede procesarse y componerse la información.[76]

Por su parte el Art. 1 litera “b” del convenio sobre la ciberdelincuencia, de Budapest del 23.XI.2001 define los “datos informáticos” de la siguiente forma: “Por datos informáticos se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función”[77]

Para CASTILLO el concepto de “dato” implica cualquier información codificada o codificable, que pueden ser representadas a consecuencia de una

[76] https://concepto.de/dato-en-informatica/#ixzz6sRh034Zv ; consultado el 02 de enero 2021.
[77] http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF consultado el 13 marzo de 2020.

convención semántica o de funciones (de manera sintáctica). Convención es cualquier acuerdo sobre el sentido de un signo o de una función, que son fijados o codificados. La codificación de la información es un elemento constitutivo del concepto de datos. No hay ninguna restricción respecto a determinada clase de codificación. P.e., en la codificación digital que se realiza por medio del Código binario pueden codificarse expresiones escritas y expresiones orales y otras características de un ser humano. Lo que guarda el inicio del proceso puede ser expresión escrita ("password"), puede ser una palabra de determinada persona (proceso que se inicia con la voz de una persona) o puede ser una característica individual (huella digital, el color del iris de los ojos de una persona).[78]

La amplia definición del concepto de datos que se ha relacionado en el párrafo anterior, puede verse que abarca al lado de los datos de entrada y de salida, también las informaciones, lo mismo que el programa o partes de un programa compuestos por los datos para el trabajo y dirección de programas, por lo cual puede verse que dicha definición siempre estará sujeta a cambios en la medida que avance el desarrollo de las TIC´S y de los sistemas informáticos que las soporten y desarrollen en el futuro; esta misma situación se presenta con la definición de información que será estudiada infra en este capítulo.

2.1.2. Sistema Informático y redes informáticas

En la actualidad hablar de sistemas de información o de sistemas informáticos es indistinto ya que ambos conceptos se utilizan como sinónimos, a pesar que para algunos autores no necesariamente debe existir tal similitud[79], así que se

---

[78] Castillo González, *La estafa informática*. 35-36.

[79] Ver la tesis doctoral de Jorge Alexandre González Hurtado citada en esta investigación que afirma, citando a LAPIEDRA "un sistema de información es algo más que un sistema computarizado (informático). El sistema de información es indisociable del sistema

que debe de tenerse en cuenta que una primera aproximación de un sistema de información debería de entenderse como un: "sistema o subsistema de telecomunicaciones o computacional interconectados y que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, transmitir o recibir voz y/o datos, incluyéndose en el mismo tanto los programas (software y firmware) como el equipo (hardware)" [80].

Por su parte el Art. 1 litera "a" del convenio sobre la ciberdelincuencia, de Budapest del 23.XI.2001 define un sistema informático de la siguiente forma: " Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento de datos en ejecución de un programa"[81] como puede apreciarse la definición apuntada en el primer párrafo de este apartado es más abarcadora del concepto objeto de estudio en este momento, por ello para fines de esta investigación será la utilizada en lo sucesivo.

Debe tenerse muy en cuenta que los sistemas informáticos no deben de confundirse con las redes informáticas, ya que estas últimas suponen una serie de sistemas informáticos (por tanto, no sólo computadoras) conectados entre sí por medio de dispositivos físicos que envían y reciben información a través de cualquier medio hábil para el transporte de datos, con la finalidad de compartir recursos y ofrecer servicios. Paradigma de las redes informáticas es Internet, una red informática de extensión global que conecta sistemas

---

organización-entorno, y en el proceso de adopción de decisiones no se puede pretender que toda la información necesaria sea predeterminada, formalizada e informatizada"

[80] González Hurtado, "Delincuencia informática". 34.

[81] http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF. Consultada el 13 de marzo de 2020.

informáticos en todas las partes del mundo. En relación con Internet habitualmente se utiliza el término ciberespacio, aunque no son del todo comparables, ya que a partir de este segundo concepto giran otras ideas relacionadas con campos más allá de la informática y las redes como pueden ser el político, el filosófico, el comercial o el jurídico[82]; esto es así porque el ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada.

2.1.3. El Ciberespacio.

La palabra ciberespacio fue popularizada por William Gibson en su novela de 1984 Neuromante aunque su origen es incluso anterior, utilizado en un cuento corto del mismo autor titulado *Johnny Mnemonic* de 1981, actualmente por ciberespacio debemos entender "es una infraestructura universal, a través de la cual se emite y recibe voz, texto e imágenes con origen y destino en cualquier lugar del mundo. Está instalado sin tener en cuenta las fronteras de los Estados porque supera el espacio físico sobre el que están constituidos los Estados. Estamos ante un territorio abierto, el Ciberespacio es un mundo sin fronteras"[83]. Se puede decir que el ciberespacio es una metáfora para describir el terreno no físico creado por los sistemas de computadoras[84].

Como puede apreciarse este aspecto general de la informática es clave para el estudio del ciberdelito, pues determinará el lugar de comisión o de producción del resultado dañoso ya que se analizará también los aspectos relativos a la territorialidad en la aplicación de la ley penal.

---

[82] González Hurtado, "Delincuencia informática". 37.
[83] Ver Hurtado Gonzalez. Delincuencia informática, y Nava Garcés. Delitos informáticos.
[84] Nava Garcés, *Delitos informáticos*, 2016. 10.

2.1.4. Redes Sociales.

Una realidad de inicios de la primera década del siglo XXI es la dependencia a la realidad virtual que generan las conocidas "redes sociales", que hacen que toda persona tenga una vida real y otra virtual, siendo que en esta última está en comunicación con personas que físicamente no conoce o que ni siquiera viven en su mismo país dándose el fenómeno que hay sujetos que prefieren esta realidad virtual al mundo real, por eso pasan horas utilizando las distintas redes sociales existentes en cualquier lugar: En su casa, en su trabajo, cuando van al servicio sanitario, en un autobús o caminan en las calles, siendo este último fenómeno titulado ***"zombiewalkers"*** que son individuos que están tan introducidas en el uso de su teléfono celular que olvidan el mundo real y sus riesgos p.e. hay personas que caen por gradas que no vieron o que son atropelladas por vehículos por no haber visto el cambio del semáforo, entre otros peligros.

En palabras de SANJURGO: "Las redes sociales son un servicio de comunicación en Internet que ha tenido una repercusión en la comunicación de todos nosotros, tanto en la vida personal como profesional" [85]; para NAVA GARCES las redes sociales cambiaron el modo de interrelacionar a las personas y pueden ser estudiadas desde diversos puntos de vista o desde diversas ciencias[86] por lo cual no escapan del estudio desde el punto de vista jurídico ya que como se verá más adelante por medio de ellas pueden cometerse ciberdelitos.

---

[85] Beatriz Sanjurjo Rebollo, *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, ecommerce, consumidores, marketing online y publicidad digital* (Madrid: Dykinson, 2015). 75.
[86] Nava Garcés, Delitos informáticos. 45.

Las redes sociales pueden definirse como espacios digitales que brindan a los ciudadanos la oportunidad de compartir información personal de especial interés, bien sea mediante el intercambio de imágenes y videos[87], para NAVA GARCES las redes sociales son grupos de personas que están interconectadas por uno o varios tipos de relaciones, intereses comunes o intercambio de conocimientos[88] esta última afirmación es importante ya que en materia de redes sociales cada uno de los usuarios crea un perfil, ingresando algunos datos personales e intereses en general (todo bajo el criterio de voluntariedad) y sobre esta base el sistema informático interconecta a las personas según esta información, pero cada usuario decide a quienes agregar a su red o grupo que puede conocer sus imágenes, publicaciones, notas de voz, mensajes de texto u opiniones.

La redes sociales han experimentado un auge acelerado en los últimos años y hoy en día se encuentran sumamente presentes en nuestras actividades diarias, ya que por un lado, todos los sujetos pueden acceder a ellas desde cualquier dispositivo electrónico, como aparatos celulares, tabletas u ordenadores y, por otra parte, debido a la gran cantidad de servicios y opciones que ofrecen, permiten el intercambio eficaz de gran cantidad de información a bajo precio (únicamente con una conexión a Internet) y de forma inmediata.[89]

El crecimiento en el uso redes sociales a través del uso de las TIC´S inclusive ha llevado a poder clasificar a las generaciones de seres humanos que las usan, de la siguiente forma: **a) En nativos digitales**: Que agrupa a aquellas personas que han nacido y se han desarrollado en el uso de las nuevas

---

[87] Gastón Enrique Bielli y Carlos Jonathan Ordoñez, *La prueba electrónica: teoría y práctica* (Ciudad Autónoma de Buenos Aires: Thomson Reuters La Ley, 2019). 587.
[88] Nava Garcés, *Delitos informáticos*, 2016. 47.
[89] Bielli y Carlos Jonathan Ordoñez, *La prueba electrónica: teoría y práctica*. 588.

tecnologías, pues las mismas son parte de su diario vivir, prescindiendo dicha generación del uso de manuales o instructivos para el uso de las redes y aparatos que utilizan las TIC´s y saben como desenvolverse en estos medios virtuales. También existe la generación conocida como **b) migrantes digitales:** Que tiene en su seno a las personas que no han crecido con aparatos que utilicen las nuevas tecnologías, sino que poco a poco se han ido adaptando a la misma conforme evolucionan, para esta generación existen manuales, tutoriales, libros necesarios para aprender a interactuar utilizando las TIC´S[90].

Se considera por las fuentes consultadas para esta investigación que ambas generaciones comparten los riesgos por igual ante los ciberdelincuentes, pues la falta de malicia en las personas de estas generaciones los puede llevar a confiarse para depositar en los aparatos electrónicos o difundir en redes sociales información sensible o significativa que puede ser utilizada para fines al margen de la ley que pueden dañar bienes jurídicos tutelados por los diversos Estados. No obstante, se es de la opinión que el grupo más vulnerable son los migrantes informáticos ya que desconocen en gran medida el uso de la Internet, de las redes sociales y las maquinas que utilizan las TIC´S por lo cual son presa fácil de la ciberdelincuencia.

Hasta este punto se ha dicho mucho sobre las redes sociales, pero no se han expuesto que debe ser entendido por las mismas, por lo cual se comparte la definición hecha por BIELLI y ORDOÑEZ, para quienes estas son: “espacios digitales que, según la función para las que están destinadas, reúnen a un grupo de personas con un interés común, para compartir información y experiencias vinculadas a ese ámbito. Ofrecen la posibilidad de intercambiar

[90] Nava Garcés, *Delitos informáticos*, 2016. 46.

múltiples contenidos, bien sea de forma pública o privada, lo que eleva las relaciones interpersonales a un nuevo plano en el que se mezclan e incorporan aspectos tecnológicos. A su vez, permiten la interacción en tiempo real, ya que a estas plataformas se puede ingresar desde cualquier dispositivo electrónico con acceso a internet.[91]

En la actualidad existen diversas redes sociales, de diversa índole o temática, siendo las más populares: Facebook, Twitter, Instagram, linkedin, Youtube, Myspace, Periscope, Tik Tok, etc que permiten a las personas intercomunicarse a través del uso de la Internet, pero que a la vez son vitrinas para la delincuencia.

2.1.5 Nuevas tecnologías.

Se hace necesario comprender la idiosincrasia del ciberdelincuente al vulnerar la seguridad de las redes informáticas y hacer un riguroso estudio jurídico – penal sobre su conducta, desde una perspectiva de política criminal sentar las bases de lo que se ha dado en llamar “la casa común” o “Aldea global” sobre la base del respecto a bienes jurídicos considerados universalmente o de reconocimiento general por la mayoría de los Estados del planeta, pues así se podrá determinar quiénes integrarán esa aldea y las conductas esperadas para la perfecta armonía de la misma.

No es fácil realizar una aproximación a lo que debe ser entendido como nuevas tecnologías y del impacto que estas suscitan en la vida de las personas. Similar al fenómeno estudiado supra sobre las redes sociales, la autora MORON al referirse a las nuevas tecnologías afirma que las sociedades se han visto modificadas, afectadas y reestructuradas por el advenimiento y la

[91] Bielli y Carlos Jonathan Ordoñez, *La prueba electrónica: teoría y práctica*. 588-589.

recepción masiva de unas tecnologías basadas en la convergencia de las telecomunicaciones con la informática.[92] La convulsión se centra en cómo se capta, transporta, almacena, procesa y se difunden los datos, información y conocimientos.

Información y comunicación aparecen, imbricadas, íntimamente ligadas e interrelacionadas. Su unión (tecnologías de la información) es considerada base de pensamiento e incluso de desarrollo, en el devenir de las relaciones sociales, así también la imbricación creciente entre las computadoras y las telecomunicaciones, denominada "telemática" ofrece una expectativa de prestaciones hasta hace poco tiempo insospechada[93] generando ciertas particularidades que se proyectan en el ámbito de la criminalidad ya que así como un individuo cualquier puede trabajar en tiempo real desde cualquier parte del mundo, un ciberdelincuente puede hacerlo también aprovechando la habilidad para no dejar huellas, cosa que hace difícil la detección, descubrimiento y persecución de ciberdelito.

Como lo expresa NAVA GARCES en la segunda edición de su libro *"Delitos Informáticos"* al referirse a las nuevas tecnologías lo hace en el sentido que estas son una nueva realidad que emerge con la criminalidad informática y la incertidumbre que plantean hechos socialmente considerados nocivos e incluso ilícitos desde una perspectiva general, hacen que se suscite la duda sobre la posibilidad de que tengan una consecuencia jurídico – penal. En estas circunstancias, los fenómenos que así se presentan deben ser abordados inicialmente desde la perspectiva de la Política Criminal y la

---

[92] Esther Morón Lerma, *Internet y derecho penal: Hacking y otras conductas ilícitas en la red* (Barcelona: Aranzadi, 1999). 90.
[93] Morón Lerma. Internet y derecho penal. 90-91.

Criminología como instrumentos de que dispone la ciencia del Derecho Penal.[94]

El procesamiento electrónico de datos se convierte en un factor criminógeno, ya que el delincuente con conocimientos especializados sobre las TIC´S ve una oportunidad de realizar hechos ilícitos utilizando como medio un aparato de estas nuevas tecnologías o teniendo por objeto de su actuación afectar ese procesamiento electrónico con un ataque hacía la computadora u otro dispositivo electrónico que contenga información, tanto en el seno de las instituciones estatales como en entidades privadas o en usuarios en general, especialmente cuando el ciberdelincuente ha obtenido información personal de la víctima a través de medios fraudulentos o utilizando información proporcionada en redes sociales.

Se debe de ser consciente que ante las nuevas tecnologías de la información y la comunicación, los gobiernos de distintos países – en especial los subdesarrollados – han reaccionado de una forma lenta, siendo sus reacciones muchas veces insuficientes, pues dictar una ley especial para tratar de resolver un problema que escapa de las fronteras nacionales es absurdo; así como los distintos países firman convenios, pactos o acuerdos internacionales que permiten el desarrollo y uso de la internet así como las telecomunicaciones de esa misma forma se debería reaccionar para regular la cibercriminalidad que ve una mina de oro en la existencia de las nuevas tecnologías y el potencial de estas para ser un factor criminógeno apenas emerge.

[94] Nava Garcés, *Delitos informáticos.* 11.

2.1.6. Las páginas web y la Deep Web

Una página **web** o página electrónica, es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, hipervínculos, entre otras funciones, adaptada para la llamada World Wide **Web** (www), y que puede ser accedida mediante un navegador **web** utilizando el internet. En estos portales se utilizan diversos recursos visuales o audiovisuales para presentar productos o servicios, pero hay mucho más que esto en este tipo de páginas[95] por tal razón tratar de controlar o regular lo que pasa en internet es una tarea imposible ya que la diversidad de contenidos y paginas es tan variado, así como su número es inimaginable que es lo que provoca la realización de hechos delictivos en el ciberespacio.

A pesar de lo dicho en el párrafo anterior ciertas legislaciones a nivel internacional están tratando de regular la responsabilidad por los contenidos de las páginas web, planteando en un principio como responsable a la persona que ostenta el "dominio real" de la página web y a su vez coincide con el que tiene el "dominio legal" de la misma. No obstante hay casos donde en las páginas web intervienen terceros en el desarrollo de los contenidos, p.e. Youtube en los cuales serán estos terceros los que responderán por los contenidos que suban al internet.[96] Sobre este punto de URBANO CASTRILLO expresa "ya sea por ostentar el dominio, ya por no haber ejercido el debido control *"culpa in vigilando";* cabrá en principio demandar junto con el autor material a quien ostenta el dominio de la página".[97]

---

[95] Ibid. 43.
[96] Ibid. 44.
[97] Eduardo de Urbano Castrillo, *La valoración de la prueba electrónica* (Valencia: Tirant lo Blanch, 2009). 66.

Otro aspecto importante que trata de regularse es lo referente a la prueba de los contenidos, ya que los mismos pueden cambiarse o borrarse tan pronto como su autor considere que está siendo vigilado o investigado por los mismos por la opinión pública o por las autoridades. Para este fin existen ciertas técnicas de investigación policial cibernética que permitirán identificar los contenidos, como por ejemplo "la técnica de localizar los logos permite hacer un rastreo de los cambios de la página principal. Y, con la máxima celeridad, sería especialmente interesante conseguir una certificación electrónica notarial de una concreta página, en un momento determinado, esto es en el día tal a la hora tal"[98].

En la actualidad existen tecnologías que permiten observar el comportamiento de las páginas web, así como su creación, modificación y eliminación, así como confrontar la misma con las bitácoras que guardan las computadoras.[99] Pero lo dicho en este apartado hasta el momento se refiere únicamente a la superficie del internet, a los lugares que comúnmente pueden ser visitados por cualquier persona, pero existe un submundo llamado ***"Deep Web"*** la ciberdelincuencia ha hecho de estos sitios, un espacio más para el desarrollo de sus actividades y en donde los delitos informáticos o electrónicos se caracterizan por ser conductas criminales altamente tecnificadas, para su comisión, la delincuencia organizada hace uso de las tecnologías de la información y la comunicación más actualizadas y de vanguardia, su mejor mecanismo de acceso a los cibernautas interesados en adquirir algún bien o servicio[100].

---

[98] Ibid. 67.
[99] Nava Garcés, *Delitos informáticos*, 2016. 44.
[100] Sandra Reza Reyes, "Uso ilícito de la red: 'El caso de la DEEP WEB'", en *Ciberdelitos* (México: Tirant lo Blanch - INACIPE, 2019), 181–96.

La ingeniería social[101] encuentra un medio eficaz para potenciar conductas nocivas, de modo tal que ha dado lugar al desarrollo de la Deep Web en la cual pueden encontrarse sitios de pornografía infantil, material censurado por cuestiones de decoro y ética periodística, sitios de comercio electrónico de efectos ilegales, pero también pueden encontrarse paginas satánicas, de grupos neo nazis e información clasifica o secreta de diversos gobiernos o páginas de grupos terroristas, las profundidades de la web presentan numerosos aspectos, como contenidos invisibles a los motores de búsqueda, transacciones comerciales a través de monedas electrónicas cifradas, acceso a través de navegadores que garantizan el anonimato, servidores en paraísos informáticos, es un alarmante inframundo virtual basado en un inframundo real.[102]

En la "red profunda" los volúmenes de información que se encuentra alojada supera la existente en la superficie de Internet, el tamaño de la Deep Web para el año 2019 era de 91,000 Terabytes versus 167 Terabytes que para el año 2000 se reflejaba oficialmente que tenía la superficie de internet[103] pero debe aclararse que cada día se cargan nuevos contenidos al internet y por lo cual no es posible determinar un dato certero del tamaño de cada una de ambas partes del Internet pueden tener a la fecha de esta investigación, pero las

---

[101] Entendida esta como el proceso de manipular a usuarios legítimos para obtener información confidencial, con el objetivo de divulgar información, cometer fraude u obtener acceso a un sistema informático. Son técnicas basadas en engaño que se emplean para dirigir o controla la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en determinados enlaces, introducir contraseñas, visitar paginas web, etc.) convenido de que está haciendo la correcto cuando realmente está siendo engañado por el ingeniero social. En el caso de las redes sociales los atacantes disponen de una gran cantidad de información tan solo con ver el perfil de sus victimas (sexo, fecha de nacimiento, aficiones, formación, carrera profesional, etc) lo que favorece el despliegue y empleo de estas técnicas.

[102] Nava Garcés, *Delitos informáticos*, 2016. 63-64.

[103] www.ladeepweb.blogspot.mx consultada el 28 de septiembre de 2020.

fuentes consultadas[104] determinan sin lugar a dudas que la Deep Web en tamaño a aquella.

Para REZA se debe aclarar que la Deep Web no es sinónimo de ***Dark web o Darknet,*** mientras que la primera se refiere a cualquier sitio al que no se puede acceder a través de un motor de búsqueda tradicional, bajo la superficie de la red, la segunda es una pequeña parte de Deep Web ubicada en lo más profundo de ella y en donde los sitios que se encuentran ahí han sido intencionalmente ocultos y que son inaccesibles con navegadores y métodos tradicionales, esta última es la verdadera red oscura en donde ocurren regularmente las transacciones y las actividades ilegales de la red, el mercado negro digital.[105]

Una de las características más importantes de la Deep Wep es que sus sitios están encriptados y la mayoría de ellos usan la terminación "*.onion"* así mismo usan el navegador TOR que es la abreviatura de ***"The Onion Router"*** que traducido al español es la "El Enrutador de Cebolla" haciendo referencia que para navegar en esta parte del internet es necesario hacerlo por capas similares a las que tiene una cebolla, solo que aquí las capas están cifradas o criptografíadas para proteger los datos contenidos en ella; cada una de estas capas protege de manera especial el contenido de la capa que le antecede. Nadie puede ser capaz de ver lo que hay dentro y en cada una de ellas a su interior y esto sirve para evitar que la información sea rastreada y así la conexión a la red se vuelve anónima.[106]

---

[104] Ibid; en Reza Reyes, "Uso ilícito de la red y en también en Nava Garcés, *Delitos informáticos.* 63.
[105] Reza Reyes, "Uso ilícito de la red: 'El caso de la DEEP WEB'".
[106] Ibid.

Cuando es ejecutado el sofware de TOR para acceder a la Deep Web, todos los mensajes y datos de la computadora son cifrados y rebotados de manera aleatoria, a través de una serie de "nodos" (servidores de transmisión o conexiones de las computadoras a la red), estos a su vez, se van retransmitiendo, atravesando una capa antes de retransmitirlo de nuevo, siendo que esta trayectoria cambia con frecuencia por lo que ninguno de los nodos está en posibilidad de descifrar los mensajes y solo conocen el siguiente nodo al que se pasará el mensaje, de modo que lo que se observa es una serie de conversaciones fragmentadas y cifradas.[107]

2.2.VISION GENERAL DEL DERECHO ANTE LAS TIC´S.

Se puede decir que las tecnologías de la información y comunicación giran en torno a tres medios básicos: 1. La informática, 2. La microelectrónica y 3. Las telecomunicaciones[108]; pero al afirmar que "giran" no debe de creerse que lo hacen de forma aislada, sino de manera interactiva e interconectadas, lo que permite conseguir nuevas realidades comunicativas"[109] que es lo que caracteriza el desarrollo tecnológico que desde los años ochenta del siglo pasado hasta la actualidad ha marcado la creación de dispositivos que en su funcionamiento utilizan a la vez los tres medios a que se ha hecho referencia.

Como dicen los eslogan más populares "se vive en plena era de la informática", pocas dimensiones de la vida del ser humano contemporáneo no se ven afectadas, dirigidas o controladas por el uso, directo o indirecto, de una

---

[107] Ibid.

[108] La función de la informática es almacenar, procesar y tramitar información que se convierte en datos digitales. La microelectrónica, son las reglas, normas, requisitos para una secuencia determinada, que eso permite obtener un producto final; y las telecomunicaciones, es toda transmisión y recepción de señales de cualquier naturaleza, típicamente electromagnéticas, que contengan , sonidos, imágenes o, en definitiva, cualquier tipo de información que se desee comunicar a cierta distancia.

[109] https://www.uv.es/~bellochc/pdf/pwtic1.pdf; consultado el 04 de diciembre de 2018.

computadora o de un dispositivo inteligente; por ello sectores como la banca, los seguros, los transportes, la educación, la bolsa, la administración pública, etc. dependen, en gran medida, del uso de dispositivos que utilicen las TIC´S al grado que se les encomienda, ya no solo el archivo y procesamiento de información sino, incluso, la adopción automática de decisiones, por lo que se ha convertido en el "caballo de trabajo del siglo XX"[110]

Pero la dependencia informática actual no es una exclusiva de sectores económicos privilegiados y con un elevado soporte financiero sino que el acceso a las nuevas tecnologías está al alcance de millones de personas. Ya en el presente siglo, las computadoras se encuentran encima de mesas y escritorios privados o de oficinas de trabajo alrededor del mundo. Y en una sociedad como la occidental las familias están equipadas con terminales de computadoras, como parte de su "ajuar doméstico", conectadas a una vasta gama de servicios, que llegaran a ser el centro de las comunicaciones y de otras muchas actividades familiares típicas.

Parafraseando a Pablo Palazzi el derecho puede tener dos respuestas con relación a las tecnologías: 1. Recurrir a las tradicionales instituciones de la ciencia jurídica y 2. Buscar renovar lo antiguo con una moderna visión de la realidad, proporcionada a la realidad actual, lo que se denomina "un nuevo Derecho" que busca adecuarse al siglo XXI[111] en cuanto a sus exigencias y los requerimientos que la Dogmática plantea para las leyes que pretendan regular la información, las tecnologías y el ciberespacio.

---

[110] María Luz Gutiérrez Francés, *Fraude informático y estafa: aptitud del tipo de estafa en el derecho español ante les defraudaciones por medios informáticos* (Madrid: Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, 1991). 37.
[111] Palazzi, *Delitos informáticos*. 25.

El mundo jurídico de inicios de siglo XXI se mantiene a la expectativa ante el gran reto que hoy plantean a las ciencias jurídicas las nuevas tecnologías de la información. El principal problema se traduce en buscar fórmulas efectivas de control, respecto a las cuales el derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social, que se adecue en cada momento histórico, según los valores prevalentes[112]; por ello se ve paulatinamente como ha correspondido al Derecho Penal el papel protagónico en cuanto a la regulación y mantenimiento del orden en lo que corresponde al uso de las TIC´S, poniéndose de manifiesto a través de los países que han regulado este aspecto en su Código Penal o en leyes especiales.[113]

En efecto, la información se presenta sobre todo como un factor criminógeno, ya que si bien el ordenamiento jurídico en su conjunto está llamado a encauzar en todas las manifestaciones sociales, esta transformación de la sociedad, con sus logros, sus nuevas perspectivas y con sus riesgos implica que el Derecho Penal ha de reaccionar solo ante las manifestaciones delictivas que surjan en la misma, esto es, ante la utilización pervertida y abusiva de lo que,

---

[112] Gutiérrez Francés. Fraude informático y estafa. 41.

[113] Se debe de hacer notar, que al inicio de la utilización de las TIC´s se pensaba que bastaba la aplicación de lo que se conocía como la informática jurídica como una herramienta que permitía el estudio de la creación, transmisión, procesamiento y almacenamiento de la información, de la cual se hicieron sub ramas como: a) la *informática jurídica documental* orientada a la búsqueda y compilación de documentos jurídicos; b) la *informática jurídica administrativa o de gestión* que es una herramienta que ayuda en los procedimientos administrativos rutinarios, de mantener actualizada la información de un despacho y que se haga un buen control de la información; y c) la *informática jurídica decisional* que aún no ha sido desarrollada más que en aspectos teóricos, buscando que un programa informático sustituya al hombre en la aplicación del derecho. Con el tiempo se fue viendo la necesidad de hacer otra sub rama en la informática jurídica que se dedicará al estudio, regulación y control de las conductas ilícitas realizadas por medio de las TIC´S o con la finalidad de dañar los sistemas que permiten el uso de las mismas y es donde nace el derecho penal informático, como otra forma de expandir el derecho penal a su aplicación en el ciberespacio y en las nuevas tecnologías de la información y la comunicación.

originariamente se concibió como factor de progreso como lo es la tecnología, por lo que difícilmente podía quedar inmune frente al impacto de la nueva tecnología informática en el campo de lo criminal, si afecta prácticamente a todas las manifestaciones humanas[114], tanto las de la vida real como las de lo que se podría llamar la realidad virtual[115].

El papel del Derecho en el avance y aparición de novedades tecnológicas es el de servir como elemento disciplinador del proceso. Aunque se pueda afirmar que en el siglo XXI se ha confirmado aún más el aforismo de Adán Smith *"Dejar hacer y dejar pasar"* superlativamente manifestado en las relaciones y libertades que nos permite el internet, como lo afirma Nava Garcés: Debe existir un coto a esa libertad, un límite que evite la degeneración y la destrucción de otras libertades y de otros bienes jurídicamente tutelados[116].

La cuestión que hoy debe ser tratada es, pues directamente la de cómo debe intervenir el Derecho Penal en relación con las aplicaciones y procedimientos informáticos y las redes de transmisión de datos e internet. Ello, en un triple sentido: (1) sobre que premisas valorativas debe apoyarse la intervención, lo que conduce a la determinación de los bienes jurídicos que deben ser protegidos; (2) que tipos de ataques deben ser considerados penalmente relevantes, y (3) que instrumentos de técnica legislativa resultan preferibles para articular la tutela penal[117] de los dos primeros temas se hablará más

---

[114] Paraf. Gutiérrez Francés. Fraude informático y estafa. 42.

[115] Se debe de hacer notar que con esta palabra compuesta lo que se pretende dar a entender es que actualmente el ser humano desarrolla su personalidad en dos mundos paralelos, el real u objetivo que es el que percibimos con nuestros sentidos y el virtual al cual tenemos acceso por medio de las redes sociales y el internet, siendo que las conductas delictivas buscan dañar bienes jurídicos protegidos en la realidad objetiva esto no obsta a que un ataque informático -que es de tipo virtual- afecte también esa realidad objetiva.

[116] Alberto Enrique Nava Garcés, *Delitos informáticos* (México: Editorial Porrúa, 2007).5.

[117] Juan José González Rus, *Cuadernos Penales José María Lidón*, 4 (Bilbao: Universidad de Deusto, 2007).13.

adelante en este capítulo y el tercer tema será objeto de un capítulo en particular de esta investigación.

De las anteriores tres cuestiones, la primera, sin duda, la de mayor importancia. Solo cuando se defina con la suficiente precisión que debe ser protegido en relación con los intereses que se desenvuelven en internet y en las redes de transmisión de datos podrá efectuarse de manera certera la determinación de los riesgos que resultan admisibles y, consecuentemente, de las conductas que deben ser mandadas o prohibidas. Como en tantos otros ámbitos del derecho penal actual, la identificación y delimitación de los bienes jurídicos que deben ser eventualmente protegidos resulta, pues, la cuestión central[118].

La afirmación del párrafo precedente es importante, ya que en el Código Penal vigente desde 1997 no fue tomado en cuenta como un bien jurídico la información o el tratamiento de la misma o de los sistemas que la soportan; debe tenerse en cuenta que el contexto en el cual se puso en vigencia el C.P. era un periodo de post guerra civil y cumplimiento de los acuerdos de paz que implicaba la búsqueda de la sumisión del poder del Estado a la vigencia de los derechos fundamentales consagrados en la Constitución y en los Derechos Humanos vigentes en la normativa internacional ratificada por El Salvador. No obstante, la realidad del siglo XXI ha implicado que el Legislador salvadoreño haya tenido que buscar, entre otros bienes jurídicos, la protección de la información con la LECDIC.

Cuando se hace referencia al Derecho penal hay que tomar en cuenta: i) a la dogmática penal y ii) A la política criminal, en el caso de la dogmática se hace

[118] Ibid.

necesario comprender el precepto jurídico en cuanto a su conformación y fundamentos del mismo y la política criminal como *"el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción".*[119]

Algo similar se puede decir del delito informático: Su existencia, su prevención y hasta su persecución depende de muchos factores, entre otros de la recepción de los cambios tecnológicos en el Derecho sustancial también el Derecho formal y en las organizaciones judiciales y fuerzas de prevención. [120] Así que en caso de no prestar la debida atención a esto puede ocurrir, parafraseando a NAVA GARCES, que la ausencia de ley en este espacio de la información, permite la distribución de material normalmente prohibido, la inyección de costumbres ajenas que pueden romper con los patrones de vida existentes en una población. La agresión que puede sufrir cualquier ente mediante el uso sin límites de esta tecnología, el peligro que puede padecer un agente debido al uso indiscriminado de estos aparatos, es decir, el caos[121].

[119] ¿qué es política criminal? http://www.politicacriminal.gov.co/Portals/0/documento/queespoliticacriminal-ilovepdf-compressed.pdf?ver=2017-03-09-180813-317 (consultado el 05 de diciembre de 2018)
[120] Ibídem.
[121] Nava Garcés, *Delitos informáticos*, 2007. 53.

CAPITULO III:TRATAMIENTO DOGMÁTICO DEL CIBERDELITO

SUMARIO: 3.1. Definición de Ciberdelito. 3.1.1. De la Información. 3.1.2. El Ciberdelito. 3.2. Teoría del Delito aplicada al Ciberdelito. 3.2.1. Tipo Penal. 3.2.1.1. Tipo Objetivo. 3.2.1.1.1 Bien jurídico protegido. 3.2.1.1.2. Acción. 3.2.1.1.3. Medios. 3.2.1.1.4. Resultado. 3.2.1.1.5. Elementos Normativos y Descriptivos. 3.2.1.1.6. Sujeto Activo del Delito. 3.2.1.1.7. Víctima. 3.2.1.1.8. Circunstancias de tiempo, espacio y desarrollo tecnológico. 3.2.1.2 Tipo Subjetivo. 3.2.1.2.1. Dolo. 3.2.1.2.2. Elementos Especiales de Autoría. 3.2.1.3 Tipo Culposo o imprudente. 3.2.2. La Antijuridicidad en el Ciberdelito. 3.2.3 La Culpabilidad en los Ciberdelitos. 3.3. Clasificación de los Ciberdelitos.

RESUMEN

En el presente capitulo se pretende desarrollar los aspectos generales de lo que debe ser considerado por el lector como “el Ciberdelito” excluyendo esta figura de otras parecidas y estableciendo la definición que en esta investigación se tendrá por tal. Así mismo se desarrollará un breve análisis de la teoría del delito aplicada a los ciberdelitos, ya que como se pondrá en evidencia existen ciertos aspectos que en la doctrina tradicional no han revestido mucha importancia, pero en el tema de la delincuencia por medio de las TIC´S presenta una nota muy característica y esencial para dicha temática.

3.1.DEFINICION DE CIBERDELITO.

En este apartado se pretende estudiar las diferentes definiciones y conceptos acuñados por la doctrina para este tema; pero para llegar a ese punto se principiará por determinar que debe entenderse por información desde un punto penalmente relevante.

3.1.1. De la información.

"La palabra "información" parece conformarse de dos partes: "in" – "formatio". En latín "formatio" se refiere a la acción de formar o de dar forma, de generar algo. Por su parte el prefijo "in" indica dirección hacia dentro. Generar algo hacia adentro, algo que proviene desde afuera".[122] "Información, es un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y reestructurarlos de una manera determinada, de modo que le sirvan como guía de su acción.[123]

El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después.

En opinión de AZOLA CALDERON[124] no existe una definición exacta del concepto "información" ya que a lo largo de la historia han existido diversos acontecimientos que han venido determinando el curso de la humanidad, ya que algunas personas, en un momento dado, obtuvieron y aprovecharon distintos datos para utilizarlos para un fin determinado.

Así mismo ABOSO[125] considera que una definición abstracta del concepto "información" se encuentra en discusión, que sea abarcadora,

---

[122] https://definiciona.com/informacion/ (consultado el 06 de diciembre de 2018)
[123]http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/capitulo1.pdf (consultado el 05 de diciembre de 2018)
[124] Luis Azaola Calderón y Instituto de Formación Profesional (México), *Delitos informáticos y Derecho penal* (México: Editorial UBIJUS, 2010). 12.
[125] Gustavo Eduardo Aboso, *Derecho penal cibernético: la cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la información* (Buenos Aires: B de F, 2017). 72.

multidisciplinaria y estrictamente lógico-formal o si, por el contrario, la idea es que hay tantas definiciones de conceptos de información como disciplinas a las que él sea aplicable.

La teoría de la información se origina con el famoso artículo de Claude Shannon de 1948 (*"The Mathematical Theory of Communication"*[126]*),* por su ubicación dentro de la matemática, se ha considerado a la misma un nuevo capítulo de la teoría de la probabilidad que ha sido aplicada en diversas áreas como la radio, la televisión, la telefonía y la economía entre otras, lográndose un completo desarrollo en el campo de la ingeniería. Esta teoría expone que la información parte de una situación de comunicación que queda definida por una fuente, un receptor y un canal[127] de transmisión de la misma.

Según Lombardí, considera que la información es un concepto totalmente formal sin alusión a la transmisión o recepción de señales, ya que es una medida del modo en que se modifica el estado del conocimiento humano; para Gallo el conocimiento contemporáneo está marcado por una excesiva compartimentación que es el fruto de la disciplinariedad, que tiene un doble sentido: Induce tanto a la delimitación de un campo especifico como a la jerarquización y al ejercicio del poder; por ello la propuesta interdisciplinaria surgió para proporcionar el tránsito entre varios compartimentos del saber contemporáneo.[128]

---

[126] Que traducido al español debe entenderse como "Teoría Matemática de la Comunicación"
[127] Aboso, *Derecho penal cibernético*. 72.
[128] Tanto Aboso como Nava Garces autores que han sido citados en este trabajo expresan esta idea, solamente que sus posturas han sido determinadas a su mínima expresión a fin de no desbordar los fines de esta investigación.

La información puede ser codificada, lo que significa la conversión en símbolos de determinada información con el fin de ser comunicada, es el emisor que convierte las ideas en signos que sea más fácil para los usuarios que buscan esa información, según el autor Mazuelos Coello,[129] señala que la criminalidad no operara mediante asaltos a las bóvedas de los bancos sino que recaerá sobre las bases de datos de la empresa, como puede ser su cartera de clientes, sistemas de cobranzas, contabilidad, balances, estrategia de mercado, desarrollo de tecnología, etc.

Para el caso de esta investigación se denominará información a aquel conjunto de datos de que el sujeto activo tiene como fin de un ataque cibernético o como un medio para la comisión de un ciberdelito.

3.1.2. El ciberdelito

Para poder definir el ciberdelito es necesario delimitar y determinar el papel que juegan las computadoras o las maquinas basadas en las TIC´S en la realización de hechos ilícitos, ya que prácticamente cualquier delito puede cometerse con la utilización de aparatos electrónicos, pero debe verificarse cuando de forma principal estas máquinas forman parte del tipo del injusto para clasificarlo como un ciberdelito o un delito común. En palabras de Palazzi "sin establecer una regla genérica, podemos afirmar que una computadora puede constituir un *medio* para cometer un delito o el *objeto* sobre el cual recaiga el mismo"[130] lo cual será visto más delante al plantear una diferencia entre ciberdelitos y delitos informáticos, por lo que acontinuación se verán unas definiciones de estos últimos.

---

[129] Mazuelos Coello, Julio. "Protección jurídico penal de la información como valor económico de la empresa". En Revista Legal del Estudio Muñiz, Forsyth, Ramírez, Pérez, Taíman y Luna-Victoria Abogados, marzo de 1999, p.38.
[130] Palazzi. *Delitos informáticos.* 33.

La denominación **"delitos informáticos"**, proviene de las expresiones inglesas *computer crime* y *computer-related crim.*[131] En el Manual sobre la prevención y control de los delitos informáticos la ONU se señala que, a pesar del largo debate entre los expertos sobre que constituyen exactamente los "*computer crimes" o "computer-related crim"*, no hay una definición reconocida internacionalmente de estos términos.[132] La definición propuesta en 1983 por la OCDE, según la cual constituyen delitos informáticos "las conductas antijurídicas, no éticas o no autorizadas que impliquen el procesamiento automático de datos y/o la trasmisión de datos"[133], es sin lugar a dudas vaga e imprecisa sobre el fenómeno estudiado.

Durante los últimos años, la noción de *"computer crime"* o delincuencia informática ha sido un importante tema de debate, particularmente en los países en los que se ha presentado mayor atención a los problemas que las nuevas tecnologías presentan al derecho penal como Estados Unidos y Alemania. Los esfuerzos a nivel legal y doctrinal por alcanzar un consenso sobre dicha cuestión han sido ineficaces y llegado el momento de tomar postura[134] a fin de que se puedan concentrar los esfuerzos para afrontar la lucha contra este tipo de criminalidad.

Para Davara Rodríguez el delito informático es "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea

---

[131] Gutiérrez Francés, *Fraude informático y estafa*. 51.
[132] http://conventions.coe.int/Treaty/EN/projets/cybercrime27.html). Consultado el 21 de enero de 2020.
[133] Javier Cremades, Miguel A. Fernández Ordóñez, y Rafael Illescas Ortiz, eds., *Régimen jurídico de Internet*, Colección Derecho de las telecomunicaciones (Las Rozas, Madrid): La Ley, 2002). 259.
[134] Gutiérrez Francés, *Fraude informático y estafa*. 54.

llevada a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea *hardware o software*".[135] En cambio para Bramont-Arias no existe un concepto único sobre el delito informático: "ello debido a que la delincuencia informática se basa en una cantidad de conductas que son difíciles de agrupar en un solo significado"[136] por su parte Matellanes, considera que el delito informático comprende aquellas conductas que constituyen agresiones a las funciones de procesamiento, transmisión y ejecución de programas propios de sistemas informáticos.

La definición de delito informático comprende aquellas conductas que constituyen agresiones a los funciones de procesamiento, transmisión y ejecución de programas propios de sistemas informáticos, por lo que completando la anterior definición NAVA GARCES considera que los delitos informáticos son actividades criminales que, en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo o hurto, fraude, falsificaciones, daños, estafa, sabotaje, etc. Sin embargo debe destacarse que el uso de las computadoras ha propiciado, a su vez, le necesidad de regulación por parte del Derecho, para sancionar conductas como las señaladas.[137]

Es muy importante tomar en cuenta que el fenómeno objeto de estudio ha sido conocido como "delito informático" pero debe tenerse en cuenta que un correcto análisis jurídico del mismo implica enraizar el estudio de las ***maquinas cibernéticas*** las que pretenden reproducir funciones

---

[135] Citado por Azaola Calderón e Instituto de Formación Profesional (México), *Delitos informáticos y derecho penal*. 14.
[136] Ibid.
[137] Nava Garcés, *Delitos informáticos*, 2007. 25.

específicamente humanas.[138] Se debe hacer notar que la existencia de las computadoras es lo que ha permitido el tratamiento automatizado de la información y que la misma fue concebida con la idea de emular una de las principales partes del cuerpo humano, el cerebro. La cibernética busca enlazar la teoría de los sistemas informáticos con el sistema jurídico para dar solución a los problemas de la realidad que involucran tanto a la tecnología como al derecho creando elementos y conceptos convergentes.

En este punto es importante acentuar, como lo hace POSADA MAYA, que la doctrina penal persiste en la idea de asimilar los delitos informáticos en sentido amplio (o delitos computacionales) con los ***cibercrimenes*** (delitos informáticos en sentido estricto), agrupándolos en una misma categoría, es decir, todos los comportamientos que de manera directa o indirecta se encuentran vinculados con medios u objetos informáticos. Se trata de una postura que extiende el ámbito de esos ilícitos especiales al ámbito de los delitos clásicos, al definirlos como *delitos de relación o por conexidad objetiva o conexidad medial* con el tratamiento de datos que afectan la seguridad de la información, el patrimonio o la intimidad, etcétera.[139]

Si se piensa en el supuesto de que las maquinas basadas en las TIC´S son ***el medio*** para cometer delitos, se produce una ampliación de las formas de comisión, es adaptar la figura penal a los avances de la teoría de los sistemas, lo cual es razonable ya que sería imposible e infructuoso que se le exigiera al legislador determinar un catálogo de medios para cometer ilícitos sino que debe tenerse en cuenta cuando el legislador previó específicamente un medio

---

[138] Morón Lerma, *Internet y derecho penal: Hacking y otras conductas ilícitas en la red*. 26.
[139] Ricardo Posada Maya, *Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del título VII bis del Código penal colombiano*, Colección Ciencias penales (Bogotá, D.C., Colombia: Universidad de los Andes : Grupo Editorial Ibáñez, 2017). 99-100.

determinado en el que tenga cabida el uso de una maquina basada en las TIC´S o se permita expresamente el uso de cualquier medio y el supuesto permita que se realice con ayuda de computadoras o cualquier dispositivo de última generación, pero ello no *per se* determinará el carácter de informático, sin perjuicio que pueda catalogarse como un delito relacionado con la informática.

Otro supuesto muy diferente lo encontramos en el caso en que el delito se comete teniendo ***por objeto*** el aparato basado en las TIC´S, haciendo la diferencia entre el *hardware* y el *software*, ya que el primero no puede generar mayor trascendencia de un delito común, piénsese p.e. en un hurto, robo, daño, apropiación del aparato, esto generaría a lo más un delito común; en cambio si la acción recae sobre el *software,* es decir, el lugar donde se encuentra la información, donde están los programas y las aplicaciones que son formas intangibles creadas por la teoría de los sistemas informáticos ahí si no habría cabida a una forma tradicional de delincuencia.

No obstante lo dicho, la doctrina penal no está de acuerdo en esta distinción en cuanto a si el medio de comisión o el objeto de ataque será lo determinante para catalogar a un delito de informático o de cibercrimen pues la forma de realización de los hechos y la complejidad que puede llevar su entendimiento hace que puedan mezclarse estas ideas en cuanto a esta especialidad de delitos, piénsese que puede haber casos en que la computadora se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva P.e. la destrucción de datos mediante un programa o un virus informático, que es una combinación de las dos modalidades dichas, es utiliza un programa (medio) para dañar una maquina (objeto) que es sobre la que recae la acción típica.

En consonancia con lo anterior se puede decir que *los delitos informáticos vinculados a la red (pero que no dependen de la red)* también llamados delitos computacionales o *informáticos en sentido amplio* son todas aquellas conductas punibles tradicionales de medios ejecutivos abiertos, que tienen una relación modal objetiva – aunque circunstancial – con el tratamiento de datos e información y los sistemas informáticos (utilizado elementos incorporales).[140] Son delitos que directamente lesionan o ponen en peligro bienes jurídicos tradicionales, ya que esos son los objetos de protección y no buscan proteger las funciones informáticas.

En cambio, para los delitos que buscan proteger los sistemas informáticos, lo datos y la información utilizados como medios concretos y la afectación de los bienes jurídicos protegidos por delitos clásicos debe existir una relación modal concreta desde la fase ejecutiva hasta el agotamiento del respectivo delito, cuando sea necesario. Esta relación modal comporta, por consiguiente, un mayor *desvalor de acción objetivo* en la realización de los delitos informáticos en sentido amplio o delitos vinculados a delitos comunes[141]. Se trata de delitos en los cuales los cibercriminales utilizan como medio adicional métodos de *ingeniería social* que implican la disposición en la web de mecanismos o técnicas lógicas dirigidos a inducir o a mantener en error, mediante manipulaciones psicológicas o persuasiones engañosas a usuarios que bajo error realizan actividades voluntarias que afectan su patrimonio en beneficio de los criminales, suministrando datos o información confidencial (como contraseñas o pines) entre otras conductas.[142]

---

[140] Posada Maya. *Los cibercrimenes.* 100.
[141] Ibid. 101.
[142] Ibid. 102.

Por el contrario, a lo dicho en los dos párrafos precedentes, la doctrina especializada ha dicho que los cibercrímenes (o delitos informáticos en sentido estricto o propio) son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos sin el consentimiento o con abuso del mismo. La finalidad usual de estos comportamientos es lesionar o poner en peligro de manera ilícita la seguridad de las funciones informáticas, esto es, la confiabilidad, confidencialidad, integridad, la disponibilidad, el no repudio de los datos y los sistemas informáticos protegidos y la recuperación de información; sin perjuicio de que esto implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados.[143]

Para la presente investigación la definición anterior es la que se considera más apegada al fenómeno objeto de estudio, por lo cual será a esta a la que se haga referencia. No obstante, la misma se aplica a "Cibercrimen" concepto con el que no se está de acuerdo, ya que según el Código Penal se califican de hechos punibles los delitos y las faltas, los primeros a su vez se sub clasifican en atención a su penalidad en graves y menos graves (Art. 18 C.P.) por lo cual en la realidad salvadoreña no se está a la costumbre de llamar "crimen" a los delitos graves, pues esta clasificación es más de sistemas jurídicos como el francés o el inglés donde los hechos punibles se clasifican en: Crímenes, delitos y faltas o contravenciones. Por ello, el termino a utilizar en lo sucesivo será el de "**ciberdelitos"** para estar en armonía con el sistema penal salvadoreño y a la vez con la normativa internacional de combate a estos ilícitos a la que se hará referencia en los próximos capítulos.

[143] Ibid. 103-104.

3.2. TEORIA DEL DELITO APLICADA AL CIBERDELITO

Para Bacigalupo la teoría del delito tiene por objeto proporcionar los instrumentos conceptuales que permitan establecer que un hecho realizado por un autor es precisamente el mismo hecho que la ley prevé como presupuesto de una pena.[144] Parafraseando a MUÑOZ CONDE la teoría general del delito estudia las características comunes que debe tener cualquier conducta (acción u omisión) para ser considerada delito, pues hay rasgos que son comunes a todos los delitos y otros por las que se diferencian los tipos penales unos de otros[145] sin olvidar que un hecho solo puede ser penado cuando su punibilidad haya sido establecida en una ley anterior a su comisión.[146]

Considera CHOCLAN que este tema debería llamarse "Teoría jurídica del delito o teoría del hecho punible" la cual tiene por cometido explicar los presupuestos generales de la acción punible deducidos de los tipos concretos de la Parte Especial. Esta tarea corresponde realizarla a la dogmática jurídico – penal que tiene por objeto, precisamente, la interpretación, sistematización y elaboración conceptual de las categorías penales.[147] Por su parte PEREZ DEL VALLE considera que en la actualidad es mejor hablar de una "Teoría de la imputación" que tiene por objeto determinar qué persona o personas han de ser castigadas con una pena, porque mediante su comportamiento delictivo

---

[144] Enrique Bacigalupo, *Lineamientos de la teoría del delito*, 2a ed., corr. actualizada, Colección Escuela Libre de Derecho (San José, Costa Rica: Editorial Juricentro, 1985), 13.
[145] Francisco Muñoz Conde, *Teoría general del delito* (Bogotá, Colombia: Temis, 2018), 7.
[146] Harro Otto y José R Béguelin, *Manual de derecho penal: Teoría general del Derecho* (Barcelona: Atelier Libros, 2017), 21.
[147] Ángel Calderón Cerezo y José Antonio Choclán Montalvo, *Derecho Penal. Tomo I. Parte General* (Barcelona: Bosch, 1999), 71–72.

han mostrado su desprecio por las normas esenciales para la subsistencia de la comunidad política y, por tanto, por el bien común.[148]

Independiente de la denominación que se emplee por parte de la doctrina para el tema sujeto de este apartado, es importante resaltar que debe hacerse un estudio profundo por parte de la dogmática para explicar la teoría del delito aplicada a los Ciberdelitos como lo ha intentado hacer el autor Alberto Nava Garcés que su obra “delitos informáticos” aborda brevemente este tema, por lo que, a continuación, se pretende lacónicamente desarrollar este tema aclarando que será en sus aspectos más relevantes y generales, adecuándolos al ciberdelito, ya que hacerlo de una forma pormenorizada escapa de los fines de esta investigación.

El delito debe observarse como un ente propio de la ciencia del derecho que contendrá aquellas conductas humanas tachadas de antisociales en un tiempo y espacio determinados. Para la lógica quedan las tareas de definir y dividir al delito como tal, entendiendo que al definir y de dividir al delito como tal, entendiendo que al definir, establece cuáles son sus aspectos esenciales y al dividir, clasifica al delito por dichos caracteres.[149]

De una forma simple se puede definir el delito de acuerdo a sus elementos y dependiendo el orden en el cual se coloquen dichos elementos se puede determinar el sistema penal al que responde dicha definición, asi se puede decir que “x” o “y” autor tiene una visión causalista, finalista o funcionalista. El hecho de formular un concepto general del delito con una serie de elementos, divididos a su vez en subelementos y sub categorías, y que este concepto

[148] Carlos Pérez del Valle, *Lecciones de derecho penal: parte general* (Madrid: Dykinson, 2016), 75.
[149] Nava Garcés, *Delitos informáticos*, 2016, 77.

general sea válido para todas y cada una de las figuras de la parte especial es un avance muy importante de la historia jurídico penal, pues tiene una consecuencia trascendental: Garantizar la seguridad jurídica del ciudadano.[150] Existe acuerdo en determinar que los elementos de toda conducta punible es una acción *típica, antijurídica, culpable* y que en ocasiones cumple especiales presupuestos de punibilidad.[151]

3.2.1. TIPO PENAL

La necesidad de recurrir al tipo penal como primer estrato sistemático del delito, es un imperativo constitucional del Art. 15 Cn y de los Tratados de Derechos Humanos suscritos por El Salvador, tal como la Convención Americana sobre Derechos Humanos que prescribe el mismo mandato en su Art. 9 [152] ya que deriva del principio constitucional de legalidad penal. Como solo es posible aplicar una pena como consecuencia de la realización de una acción, es indispensable que el sistema provea de una herramienta apta para individualizarla y el único instrumento que puede llevar a cabo esa tarea de forma efectiva y sin ambigüedades es el tipo penal.[153]

El tipo penal es la descripción hecha por la ley del comportamiento humano socialmente relevante y prohibido (acción u omisión), en su fase subjetiva y objetiva[154]; al referirse al tipo penal la doctrina utiliza otras expresiones tales como: Tipo del delito, tipo del injusto, tipo total, tipo de garantía o tipo

---

[150] Diego-Manuel Luzón Peña, *Derecho penal: parte general* (Montevideo; Buenos Aires: Editorial B de F, 2018), 213.
[151] Calderón Cerezo y Choclán Montalvo, *Derecho Penal. Tomo I. Parte General*, 72.
[152] Así también lo prescriben: El Pacto Internacional de Derechos Civiles y Políticos, Art. 15; Declaración Universal de Derecho Humanos, Art. 11.2
[153] Mariano H. Silvestroni, *Teoría constitucional del delito*, 2. ed., actual (Buenos Aires: Eds. Del Puerto, 2007). 237.
[154] Mario Garrido Montt, *Derecho penal*, Segunda edición actualizada (Santiago, Chile: Editorial Jurídica de Chile, 2016).45.

sistemático, pero las mismas van referidas a la misma definición antes anotada, solo que resaltándola en un contexto determinado, como lo pone en evidencia GARRIDO MONTT *"al enunciar el concepto de tipo penal se ha hecho referencia a lo que normalmente se califica como tipo sistemático, a la descripción de la conducta prohibida. El denominado tipo de garantía se vincula con el principio de la legalidad, presupone la comprensión de todos los presupuestos requeridos para la imposición de una pena"*[155]

SILVESTRONI al referirse al tema objeto de este apartado manifiesta que hay una diferencia entre tipo penal que es el instrumento abstracto que describe la conducta penalmente relevante; es la descripción concreta y material de la conducta prohibida, el tipo es la herramienta que utiliza el legislador para individualizar aquellas conductas a las que amenaza con una pena; en cambio la tipicidad es la adecuación de la conducta a esa descripción y la subsunción es el resultado positivo del juicio de adecuación.[156]

El vocablo tipicidad -del latín *"typus"* y este , a su vez, del griego *"Turos"* en su acepción trascendente para el derecho penal significa símbolo representativo de una cosa figurada o figura principal de alguna cosa a la que suministra fisonomía propia, típico es todo aquello que incluye en si la representación de otra cosa, y a su vez, es emblema o figura de ella.[157] Se puede definir el tipo penal como la abstracta descripción que el legislador hace de una conducta humana reprochable y punible. La abstracción se refiere al contenido general

[155] Garrido Montt. 45-46.
[156] Silvestroni, *Teoría constitucional del delito*. 237.
[157] Mariano Jiménez Huerta, *La tipicidad* (México D.F.: Porrúa, 1955), 11.

y amplio de la conducta normada, para que dentro de su marco el singular y concreto comportamiento.[158]

El tipo penal es la expresión jurídica mediante la cual el legislador expresa la conducta antisocial y la tipicidad el proceso mediante el cual podemos adecuar una conducta al tipo[159] un comportamiento es típico cuando puede afirmarse que está comprendido en el grupo de casos que describe la ley penal y que se denomina tipo, por su parte se dice que la tipicidad cumple una función de garantía, ya que es la manifestación del principio de legalidad como *lex stricta* por ser el presupuesto de la imposición de una pena. De acuerdo con esta función de garantía de la tipicidad, no es posible considerar un comportamiento como incluido en el tipo del delito cuando se considera que cae fuera del tipo legal.[160]

En el caso de El Salvador la LECDIC contempla los diversos tipos penales en abstracto que son conductas reprochables que van a generar, en caso que un sujeto las realice una o más de los distintos supuestos contemplados en la ley en referencia, en la medida que su conducta se adecue a la descripción típica, se estará en presencia de uno o varios ciberdelitos que deben ser investigados por la PNC y procesados luego por la FGR a fin de imputar su conducta al sujeto activo lo cual solo puede hacerse a través de la articulación de los actos probatorios y medios de prueba pertinentes y útiles para ese fin.

No debe perderse de vista que el tipo de injusto no está compuesto solo de elementos objetivos de naturaleza descriptiva o normativa. La gran aportación

---

[158] Alfonso Reyes Echandía, *Tipicidad*, 2.reimpr. de la 6. ed (Santa Fe de Bogotá: Temis, 1999), 7.
[159] Nava Garcés, *Delitos informáticos*, 2016, 71.
[160] Pérez del Valle, *Lecciones de derecho penal*, 113.

de la teoría final de la acción consistió en demostrar que la acción u omisión subsumible en el tipo no es un simple proceso causal ciego, sino un proceso causal dirigido por la voluntad hacia un fin. De ahí se desprende que, en el ámbito de la tipicidad, deba tenerse en cuenta el contenido de esa voluntad (determinación de un fin, selección de medios, previsión de los efectos concomitantes, etc). Por eso el tipo de injusto tiene tanto una vertiente objetiva (el llamado tipo objetivo) como una subjetiva (el llamado tipo subjetivo). Esta última vertiente es más difusa y difícil de probar, ya que refleja una tendencia o disposición subjetiva que se puede deducir, pero no observar.[161] Estas dos vertientes será estudiadas a continuación.

3.2.1.1. Tipo Objetivo

Al hacer referencia al tipo objetivo del tipo penal se habla de la descripción de la conducta antijurídica desde un punto de vista externo, pero eso no quiere decir que sea únicamente una descripción externa, ya que siempre que se describe una conducta humana habrá que tomarse en cuenta el elemento subjetivo[162], esta separación obedece a razones de técnica legislativa, ya que la ley incriminadora describe la acción externa y, cuando ello es relevante, sus consecuencias materiales o resultado, y la parte subjetiva se restringe a las formas de culpabilidad, lo cual no debe entenderse como que el tipo objetivo sea autónomo con respecto al tipo subjetivo ya que solo la conjunción de ambos se puede derivar la existencia de una acción jurídico penal conforme al tipo[163] pero para fines didácticos y de mejor comprensión se explican por separado; el tipo objetivo se identificará con la manifestación de la voluntad en el mundo físico que es requerida por el tipo penal. Por tal motivo a

[161] Muñoz Conde, *Teoría general del delito*, 51.
[162] Parraf. Eduardo López Betancourt, *Teoría del delito* (México: Porrúa, 2015). 129.
[163] Juan Fernández Carrasquilla, *Derecho penal fundamental*, 2. reimpresión de la 2. ed (Santa Fe de Bogotá, Colombia: Editorial Temis, 1989). 130.

continuación se detallarán los elementos que se encuentran inmersos en el tipo objetivo relacionado con el Ciberdelito.

3.2.1.1.1. Bien Jurídico Protegido

La norma penal tiene una función protectora de bienes jurídicos, para cumplir esta función protectora eleva a la categoría de delitos, por medio de su tipificación legal, aquellos comportamientos que más gravemente lesionen o ponen en peligro los bienes jurídicos protegidos. El bien jurídico es, por tanto, la clave que permite descubrir la naturaleza del tipo, dándole sentido y fundamento. Todo tipo penal debe incluir un comportamiento humano capaz de provocar la puesta en peligro o lesión de un bien jurídico. Lógicamente se espera que, de acuerdo con el principio de intervención mínima, el legislador sólo utilice el Derecho penal proteger bienes jurídicos verdaderamente importantes y tipifique aquellos comportamientos verdaderamente lesivos o peligrosos para esos bienes jurídicos.[164]

A la fecha de la redacción de esta investigación la Doctrina Jurídico Penal no es unánime en determinar si los Ciberdelitos tienen un solo bien jurídico susceptible de lesión o de puesta en peligro, o por el contrario son muchos y distintos los bienes jurídicos que se hayan vinculados a la hora de realizarse la conducta típica prevista por el legislador, pero la toma de postura sobre este tema se hace con base a la vigencia de la LECDIC y sobre el contexto de la misma como se verá a continuación.

Las características del Ciberespacio, hace que la seguridad cibernética juegue un papel central en su aplicación en el contexto de un Estado de Derecho, así

[164] Francisco Muñoz Conde, *Derecho Penal. Parte General*, 4 Edición (Valencia: Tirant lo Blanch, 2000), 296.

como en el juego de relaciones internacionales, llegando a ser una constante, presente, de una u otra forma, en todos los intereses en juego del nuevo ámbito relacional cibernético. Esta omnipresencia de las relaciones cibernéticas, en todos sus aspectos, técnicos, sociológicos, jurídicos, económicos y políticos, hace emerger al Ciberespacio –y las relaciones electrónicas que lo sustentan- como un nuevo valor, un nuevo bien jurídico digno de protección –barrera de protección jurídica anticipada- , de carácter universal, que deberá servir para configurar nuevos tipos penales, con independencia de los ya existentes y, entre los que destaca por su importancia para hacer viable el bien principal, la seguridad cibernética y el derecho al uso seguro de Internet.[165]

Concordando con POSADA MAYA a pesar de la compleja discusión doctrinal sobre el bien jurídico protegido por los ciberdelitos, la LECDIC, ha creado un conjunto de tipos penales que protegen un nuevo bien jurídico autónomo, intermedio o de referente individual con independencia de los demás intereses protegidos de forma conexa que se concreta en ***la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos***[166] los demás bienes jurídicos tradicionales que se pueden ver afectados se hacen de forma "conexa" por eso el nombre de la normativa vigente.

La seguridad cibernética es un bien jurídico que adquiere una dimensión institucional y supraindividual, cuyo objeto jurídico de protección inmediato es la seguridad colectiva, lo que no impide que determinados bienes jurídicos

---

[165] José Maria Molina Mateos https://www.abogacia.es/publicaciones/blogs/blog-nuevas-tecnologias/la-ciberseguridad-como-bien-juridico-protegido/ Consultada el 01 de enero de 2021.

[166] Posada Maya, *Los cibercrímenes*. 113.

individuales constituyan un objeto inmediato de protección, en una situación valorativa en relación al bien supraindividual. La seguridad cibernética es una entidad nueva de protección, referida a los procesos y funciones que ha de cumplir el sistema, para que estén aseguradas las bases y condiciones, esencialmente los bienes jurídicos individuales.[167]

Por su parte **la información**, tal como lo señala el Art. 3 lit. b) de la LECDIC, es el bien jurídico protegido expresamente en dicha ley especial, para garantizar y proteger el ejercicio de derechos fundamentales, lo cual no debe significar criminalizar el medio, sino la ingeniería social o técnica con la que se utilizan las computadoras o las máquinas basadas en las TIC´S para cometer ilícitos penales *"on line",* protegiendo secundariamente los datos informáticos en sí mismos o los sistemas y redes informáticas y de telecomunicaciones, ya que aquellos son una representación electrónica, incluso digital, de la información, con un valor variable, en cambio los sistemas y redes son mecanismos materiales de funciones automáticas de almacenamiento, tratamiento, transferencia y transmisión de información.

No obstante, lo dicho en el párrafo anterior a pesar de ser una toma de postura de parte del legislador salvadoreño no implica su acertada determinación doctrinaria ya que para MAYER LUX deben ser criticadas las tesis que pretenden asumir que los ciberdelitos tutelan un bien jurídico especifico, propiamente informático e individual, pues considera que la funcionalidad informática es el presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su servicio en un Estado democrático de Derecho, que posibilitan que los sistemas

[167] José Maria Molina Mateos https://www.abogacia.es/publicaciones/blogs/blog-nuevas-tecnologias/la-ciberseguridad-como-bien-juridico-protegido/ Consultada el 01 de enero de 2021.

informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos dentro de un marco tolerable de riesgo que implica a su vez el uso de las redes computacionales, lo que justifica que los ciberdelitos deban tener como bien jurídico protegido **la funcionalidad informática como un bien jurídico instrumental de carácter colectivo**[168] que implica tanto la defensa del derecho humano a la identidad digital individual como a la defensa de la sociedad en sus relaciones o actividades en redes computacionales.

Se debe considerar, que en concreto para un ciudadano, la ***confianza publica en el correcto funcionamiento de los sistemas y redes computacionales*** es el objeto de tutela penal de los Ciberdelitos; partiendo que la confianza es la expectativa que una persona tiene del comportamiento que tendrá otra persona en las relaciones hechas a través del uso de las TIC´S que se hace indispensable para el normal desarrollo de las relaciones sociales, pues en ella se apoyarían tanto las actividades de los consumidores como de los entes públicos y privados[169], es decir, que la confianza en la operatividad de los sistemas informáticos resulta relevante para el libre desarrollo del individuo en un Estado democrático de Derecho.

3.2.1.1.2. Acción

De modo general se puede decir que toda acción u omisión es delito si infringe el ordenamiento jurídico (antijuridicidad) en la forma prevista en los tipos penales (tipicidad) y puede ser atribuida a su autor (culpabilidad), siempre que no existan obstáculos procesales o punitivos que impidan su penalidad.[170]

---

[168] Laura Mayer Lux, “El bien jurídico protegido en los delitos informáticos” en Revista Chilena de Derecho, volumen 44, número uno, año 2017. pp. 235 – 260.
[169] Ibid.
[170] Muñoz Conde, *Teoría general del delito*, 37.

Para que un delito exista es indispensable que se realice una conducta, NOVOA sostiene que el delito es fundamentalmente una conducta humana, término que comprende tanto el comportamiento positivo (acción propiamente tal) como el negativo (la omisión)[171]; por su parte ROMO MEDINA considera que por "conducta" entiende que el comportamiento humano voluntario, positivo o negativo, la acción *strictu sensu,* es un hacer voluntario, positivo, un movimiento del organismo del hombre capaz de ser percibido por los sentidos[172], por ello se afirma que todo comportamiento dependiente de la voluntad humana es penalmente relevante y esa voluntad implica siempre una finalidad, **"una acción final, una acción dirigida a la consecución de un fin"[173]**

No obstante lo anterior no debe perderse de vista que para el derecho penal es importante estudiar la conducta no sólo desde un hacer positivo sino que se debe ir más allá y analizar también la omisión como una forma de realización de ilícitos, ya que la acción y la omisión son los dos únicos modos que reviste la conducta incriminable, la acción en el aspecto positivo o *strictu sensu* y en el aspecto negativo, la omisión concebida como una acción *latu sensu* ya que en esta se realiza una conducta negativa se deja de hacer lo que se debía de hacer, se omite la obediencia a la norma.[174]

---

[171] Eduardo Novoa Monreal, *Curso de Derecho Penal Chileno. Parte General* (Santiago: Jurídica de Chile, 2010), 265.
[172] Miguel Romo Medina, *Criminología y derecho*, 2. ed, Serie J--Enseñanza de derecho y material didáctico, num. 10 (México: Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, 1989), 46.
[173] Muñoz Conde, *Teoría general del delito*, 9.
[174] Raúl Carrancá, *Derecho Penal Mexicano, Parte General* (Ciudad de México: Porrúa, 2016), 276.

Las conductas perseguibles o bien susceptibles de reproche social en el ámbito de la computación son muy variadas, pero tienen en común que la expresión de dichas conductas se realiza teniendo por objeto o por medio de un sistema electrónico utilizando una computadora o máquina basada en las TIC´S que son empleadas con el fin de producir un ciberdelito.

Para NAVA GARCES la expresión de la conducta se puede ejercer de manera directa, sin embargo cabe la posibilidad de que ésta se realice a través de la omisión, citando de ejemplo la revisión de un sistema de cómputo donde el encargado de la misma verifica la existencia de un defecto, pero asegura que no existe ningún defecto en ese sistema y este es irrumpido por un Hacker, por lo cual si el encargado de dar soporte al sistema hubiera hecho bien su trabajo no hubiera existido el delito, pero como no lo hizo cabría responsabilidad penal por "comisión por omisión". Sobre esta última afirmación del autor citado no se está de acuerdo ya que según el Art. 20 del C.P. sería bastante excesivo equiparar el deber jurídico de obrar o que la omisión se viera como equivalente al resultado pues se estaría violando el principio de legalidad según la redacción de los tipos en la LECDIC pareciera que el legislador no tomo en cuenta la omisión como una forma negativa de comisión de los mismos.

Lo dicho en el párrafo precedente es muy importante ya que en la actualidad, como se mencionó en el capítulo I, el sistema bancario nacional ha sido objeto de ciberataques que a todas luces tienen que ver con fallas en la seguridad electrónica, que podrían traer responsabilidad para los empleados bancarios encargados de la misma si en la investigación se llegará a determinar que su comportamiento omisivo fue generador o facilitador de los ciberdelitos cometidos contra las entidades bancarias.

Se debe considerar a la acción en los Ciberdelitos como un concepto normativo desde el punto de vista de manifestación de la personalidad que aporta por si mismo un aspecto valorativo decisivo para imputar una conducta anímico – espiritual a un sujeto que renuncia a buscar lo que conceptualmente tienen en común en la unidad del sustrato material (voluntariedad, corporalidad, finalidad, no evitación o similar)[175] que atiende a una decisión jurídica del sujeto activo que incide en las otras categorías rectoras de la teoría del delito.

3.2.1.1.3. Medios

En ocasiones el tipo hace referencia a un objeto material sobre el cual recae la conducta del sujeto activo del delito, pudiendo ser este objeto una persona o una cosa, entendiendo por esta última toda entidad ya sea corporal o incorporal, natural o artificial sobre la que recae directamente el delito, por ello puede ser objeto: El sujeto pasivo, las cosas animadas o inanimadas (virtuales para el caso de los ciberdelitos). Así mismo existen casos en los cuales los tipos exigen determinados medios, que da nacimiento a los ***delitos con medios legalmente determinados o limitados,*** es decir, que para que pueda darse la tipicidad deben concurrir los medios que exija el tipo correspondiente, por lo que debe entenderse que este tipo de delitos la tipicidad de la acción se produce, no mediante cualquier realización de resultado último, sino sólo cuando éste se ha conseguido en la forma en que la ley expresamente determina.[176]

[175] Claus Roxin, Derecho penal parte general, tomo I, fundamentos, la estructura de la teoría del delito (Madrid: Civitas, 2007). 265

[176] Paraf. Nava Garcés, *Delitos informáticos*, 2016.

Es común confundir al medio comisivo con el verbo núcleo del tipo pues en ocasiones el código penal sanciona de manera directa el medio empleado o el uso de algún objeto[177] P.e. El caso de hurto agravado empleando violencia sobre las cosas (Art. 208 Nº 1 C.P.) o el robo agravado esgrimiendo o utilizando armas de fuego o explosivos (Art. 213 Nº 3 C.P.) por citar algunos tipos legales donde se da esta situación. Aplicando lo dicho a los ciberdelitos se tiene que el uso de las computadoras con el fin de cometer hechos penalmente sancionables, deben considerarse como los medios comisivos de las conductas principales, actualmente castigadas y, en ese tenor, se debe sancionar dicho uso de manera autónoma y concurrente.[178]

Se debe tener en cuenta que para el caso de El Salvador la LECDIC sanciona el uso de las TIC´S que tiene por **objeto** la realización de conductas típicas y antijurídicas para la obtención, manipulación o perjuicio de la información P.e. los tipos jurídico penales de los Arts. 4 al 9 de dicho cuerpo normativo encajan en este supuesto, pero también en este cuerpo legal penal especial hay casos donde la realización de conductas ilícitas requieren la utilización de las TIC´S como **medio** o siguiendo el concepto propuesto de ***delitos con medios legalmente determinados*** se vuelve indispensable que la realización de la tipicidad deba darse con los medios fijados por el legislador, P.e. los Arts. 10 (estafa informática) 11(Fraude informático) 13 (hurto por medios informáticos) 14 (técnicas de Denegación de servicio) 16 (manipulación fraudulenta de tarjetas inteligentes o instrumentos similares) todos de la LECDIC entre otros tipos ahí prescritos requieren el uso de computadoras o maquinas que permitan el uso de las TIC´S para perpetrar dichos ilícitos.

[177] Ibíd. 89.
[178] Ibíd. 90-91.

3.2.1.1.4. Resultado

En la Teoría del delito se suele considerar el resultado como consecuencia de la acción en sentido estricto, es decir, como modificación del mundo exterior producida o causada por un movimiento corporal dependiente de la voluntad humana. Entendido el resultado como cambio causado por la conducta y distinto de la misma, da lugar, cuando es requerido por la descripción legal, a los tipos de resultado, mientras que los tipos o delitos de mera conducta (activa u omisiva) se conforman con la actividad o pasividad sin exigir un resultado distinto de la misma.[179]

Para imputar a un sujeto activo de un delito la producción de "un resultado como su obra" debe determinarse si se ha producido un menoscabo al bien jurídico descrito en el tipo y si el mismo puede atribuírsele al autor como su obra antijurídica. Sobre la idea anteriormente dicha OTTO acentúa: "*La constatación de que el resultado se ha producido y la imputación objetiva del mismo se refieren al* ***tipo de la ley****; la constatación del injusto realizado con ello, a la* ***antijuridicidad*** *de la conducta*" [180] así mismo LUZON PEÑA manifiesta que desde la perspectiva jurídico penal el resultado (jurídico) se pone en conexión con la afectación del bien jurídico y puede consistir en la lesión (destrucción o menoscabo) o la puesta en peligro (probabilidad de lesión) del mismo prevista en cualquier tipo, en la consumación o en fases anteriores, pero advierte que tal lesión o peligro pueden ser una consecuencia subsiguiente a la acción y distinta de ella (P.e. en el caso de la estafa informática o el fraude informático, Arts. 10 y 11 LECDIC respectivamente), pero también puede la propia conducta suponer una lesión o un peligro abstracto para el bien jurídico (P.e. la posesión de Equipos o prestación de

[179] Luzón Peña, *Derecho penal*. 322-323.
[180] Harro Otto, *Manual de derecho penal: teoría general del derecho penal*, 7.a edición reelaborada (Barcelona: Atelier, 2017). 102.

servicios para la vulneración de la seguridad, Art. 8 LECDIC); también cuando la teoría del tipo habla de delitos de resultado lesivo o de delitos de resultado de peligro concreto, se alude a tipos que requieren un resultado distinto de la propia acción[181] (P.e. la utilización de datos personales, Art. 24 LECDIC).

Finalmente el resultado como cambio del mundo exterior: real, sensorial o intelectualmente perceptible y distinto de la propia acción causado por la manifestación de la voluntad que tiende a revelarse en los ciberdelitos por la lesión o puesta en peligro -concreto o abstracto- de los bienes jurídicamente protegidos que como se ha dicho supra son la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos, que es lo que permite realizar la imputación al o los sujetos activos del injusto.

3.2.1.1.5. Elementos Normativos y Descriptivos

Según Donna cuando el legislador tipifica una conducta, se ve en la obligación de realizar una enumeración de elementos que la componen, realizando, aunque sea de manera implícita, un juicio de valoración sobre esos elementos[182] que se clasifican en descriptivos y normativos; los primeros son todos aquellas construcciones del lenguaje, incluidas en una definición típica, que cualquiera puede conocer y apreciar en su significado, sin mayor esfuerzo ("daños", "lesiones", "muerte" etc.), pudiendo ser percibidos por los sentidos, ya que el legislador se refiere a ellos como seres, objetos o actos que se encuentran en el tipo penal[183] P.e. el concepto de manipulación de Registros, Art. 15 LECDIC o el hurto de la identidad, Art. 22 LECDIC, o los conceptos de

---

[181] Parraf. Luzón Peña, *Derecho penal*. 323.

[182] Edgardo Alberto Donna, *Teoría del delito y de la pena. 2: Imputación delictiva* (Buenos Aires: Depalma/Astrea, 1995). 81.

[183]file:///Users/lucioarias/Downloads/elementos_descriptivos,_normativos_y_subjetivos_del_tipo_penal.pdf consultada el 27 de julio 2021.

niño, niña, Adolescente o persona con discapacidad de la que se habla en el Art. 29 LECDIC que no requieren mayores explicaciones pues están en acervo de conocimientos generales de la población.

Por el contrario, los elementos normativos son aquellos conceptos que implican siempre una valoración, y por ende, un cierto grado de subjetivismo ("documento", "honor", "buenas costumbres", etc.); o bien se trata de remisiones directas a otros órdenes valorativos, que obligan al juzgador a realizar o a aceptar un juicio sobre un comportamiento. No se trata de una valoración personal, sino que está subordinada a normas judiciales, normas sociales y criterios ético-jurídicos de comportamiento socialmente reconocido y conocido por su carácter público y notorio. En algunos casos se refiere a una comprensión del sentido técnico del concepto, comparado con el vocablo utilizado de manera corriente en el lenguaje popular[184] o valoraciones de tipo jurídico inmersas en el tipo penal p.e. cuando incluye vocablos como “indebidamente” (porque requiere la valoración de si la acción fue realizada dentro de lo debido o no), “ilícitamente” (porque se debe hacer el examen sobre la licitud)[185] que en el caso de la LECDIC se encontraría en las definiciones establecidas en el Art. 3 de dicho cuerpo penal especial por ejemplo, que son explicadas en el contexto de la ley que regula los ciberdelitos o en el caso de los tipos penales del mismo cuerpo normativo que establecen formas de cometer los hechos delictivos que hacen referencia a valoraciones subjetivas o jurídicas.

[184] Ibíd.
[185] Nava Garcés, *Delitos informáticos*, 2016. 95.

3.2.1.1.6. Sujeto Activo del Delito

La ciberdelincuencia es un mal que no conoce de fronteras y que avanza a pasos agigantados, afectando al 65% de los adultos que usan Internet y al 40% de los menores; no es un hecho desconocido que en los medios de comunicación se brindan noticias internacionales de detención de integrantes de redes dedicadas a la falsificación de tarjetas de crédito o que accedían a las cuentas de los bancos vía Internet para realizar fraudes en la banca electrónica o bien se dedicaban a la duplicación de tarjetas o conseguían el acceso a ficheros no autorizados de empresas o particulares para descargar u obtener bases de datos o documentos[186], pero cabe preguntarse: ¿existe algún tipo de perfil para el ciberdelincuente? Si bien determinarlo corresponde a la criminología en este apartado se hará una breve reseña de este tema.

Según la información consultada se dice que el ciberdelincuente es generalmente una persona poco sociable, que actúa preferentemente en la noche son auténticos genios de la informática que entran sin permiso en computadoras y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita[187]. Se les engloba con el nombre de “Hackers” que constituyen la última avanzada de la delincuencia informática de finales del siglo pasado. El joven hacker Kevin Mitnik, de 16 años fue un pionero, impuso su lema "La información es pública, es de todos, y nadie tiene derecho a ocultarla" y cuando fue detenido sostuvo que no se creía un delincuente y

[186] Parraf. Sanjurjo Rebollo, *Manual de Internet y redes sociales*, 211.

[187] Tal cual se presenta en el personaje principal de ficción de la película “The Matrix”, estelarizada por Keanu Reeves quien en la película en el mundo real era Thomas Anderson, pero en la realidad virtual se denominaba “Neo” quien realizaba clonación de programas, accesaba a bases de datos y tenía comunicación con otras personas que se dedicaban al mismo rubro, todas las cuales se realizaban en altas horas de la noche y tenía problemas para interrelacionarse con sus compañeros de trabajo.

decía "Un Hacker es solo un curioso, un investigador", [188] pero no siempre es así también lo puede ser el trabajador de una empresa que en este caso la empresa seria la víctima, como por lo general pasa en los bancos donde muchas veces sus mismos empleados son los que realizan estafas informáticas a los clientes y al mismo banco.

Lo anteriormente expuesto se basaba en estudios criminológicos que consideraban al ciberdelincuente, como un joven entre 18 a 25 años, muy preparado, introvertido, con retos intelectuales y que formaba parte de grupos aislados[189]

Para Palazzi no es necesario el delincuente informático deba forzosamente tener muchos conocimientos profundos de la materia, ya que en la actualidad la computación es cada vez más fácil de manejar por las personas que rápidamente adquieren conocimiento de ella y cuando tengan acceso a una computadora, por lo cual existe la posibilidad de una persona decida desde la comodidad de su casa realizar un ciberdelito. El caso más típico es el cajero que desvía fondo mediante el ordenador que usa para contabilizar el dinero que recibe o ingresa falsamente un monto en una cuenta, o el del empleado de seguridad que conoce los códigos de acceso al sistema y los utiliza en su provecho. En esta facilidad de cometer delitos por medio de computadora

[188]http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf (consultada el 07 de diciembre de 2019)
[189] Gustavo Balmaceda Hoyos, *El concepto de perjuicio en el delito de estafa análisis dogmático* (Bogotá, Colombia: Leyer, 2009), 59.

han tenido un papel muy importante la expansión de acceso a cualquier sistema informático debido a las redes informáticas.[190]

No obstante, lo dicho, es muy atinada la critica que hace BALMACEDA al establecer que las posturas antes apuntadas parten de errores de concepción sobre el ciberdelincuente, considerándolos como *"nerds"* o personas inadaptadas, pero que no son violentas y que todos encajan en un "perfil" cuando más que un perfil lo que existe son *"estereotipos",* sin que se tenga presente que un perfil criminal es complejo. De esta forma, se ha demostrado que los autores de este tipo de conductas suelen ser primarios u ocasionales, que los hechos de mayor connotación económica son cometidos por empleados de empresas (denominados "insiders"); que no siempre poseen conocimientos informáticos especiales.[191]

En el ámbito de la ciberdelincuencia existe una clases *sui generis* de sujeto activo que se sitúa entre el delincuente de cuello blanco y aquel delincuente habitual del derecho penal clásico, presentándose con frecuencia el delito por la acción de autores ocasionales, que no precisan conocimientos específicos e incluso por la intervención de jóvenes a título de mera diversión o por mera curiosidad intelectual, es decir, sin afán de lucro, sino más bien empujados con ambición de fama o simplemente de respuesta al desafío constante de la inteligencia que representa la computadora y normalmente sin conocimiento de estar procediendo contra derecho.[192]

---

[190] Palazzi, *Delitos informáticos*. 67.
[191] Balmaceda Hoyos, *El concepto de perjuicio en el delito de estafa análisis dogmático*, 60.
[192] José Antonio Choclan Montalvo, *El delito de estafa*, 2. ed (Barcelona: Bosch, 2009), 1070.

Una parte de la doctrina cataloga al ciberdelincuente, a fin de no englobarlos a todos como “Hackers”, aclarando que las denominaciones utilizadas son en idioma ingles ya que no tienen equivalente en español; por lo cual se reproduce a continuación el esquema elaborado por Azaola Calderón[193] en el que se plantean también aspectos criminógenos para cada uno.

Hackers	Es una persona muy interesada en el funcionamiento de los distintos sistemas operativos; por lo general suelen tener mucho conocimiento en lenguajes de programación. Además conocen la mayoría de los agujeros de un sistema operativo o de los protocolos de Internet, y los que no conocen los busca, y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor.
Crackers	Son personas que se introducen en sistemas remotos con la intensión de destruir datos, denegar el servicio a usuarios legítimos, y general a causar problemas a los sistemas, procesadores o redes informáticas. A los crackers también se les conoce con el nombre de piratas informáticos.
Cyberpunk	El termino Cyberpunk vándalos cibernéticos se refiere a las conductas tendientes a causar daños en toda el área vinculada a la informática, esto es, afectando a los datos, programas o soportes informáticos, fundamentalmente a través de Internet.
Phreaker	Posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles, puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general móviles o celulares. Construyen equipos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular de percate de ello.

[193] Azaola Calderón y Instituto de Formación Profesional (México), *Delitos informáticos y derecho penal*. 30.

3.2.1.1.7. Víctima

De forma general se piensa que la víctima "por excelencia" de estos comportamientos es la *persona jurídica* y sobre todo aquéllas con un potencial económico muy elevado. Así mismo es frecuente que el *sujeto pasivo* sea "plural", muchas veces en cantidad muy elevada y con incertidumbre sobre su cuantía e identidad. No obstante, como se dijo con el ciberdelincuente no todas las *victimas* pueden encajar perfectamente en una determinada "clase" y algunas pueden superponerse[194]

No puede negarse que a nivel mundial son los bancos y las entidades financieras las victimas por excelencia de los ciberdelitos ya que el uso creciente de trasferencias de fondos en forma electrónica códigos autorizados electrónicamente de dígitos únicos que identifican a cualquier banco con el fin de autorizar una transferencia monetaria, pero los problemas surgen porque los códigos caen en manos incorrectas; se debe llamar la atención a lo que establece BALMACEDA, que en los inicios de estas conductas contra el sector bancario o de seguros los mismos preferían no denunciar los ciberdelitos que detectaban, con el propósito de evitar una imagen negativa, pero al día de hoy estos hechos ya se suelen denunciar por dichas entidades.[195]

Adicional a lo dicho en el párrafo anterior, también el Estado puede llegar a ser víctima de esta novedosa criminalidad[196] ya que las Instituciones Estatales manejan muchos datos personales de los ciudadanos y el actuar doloso contra

---

[194] Ver Balmaceda Hoyos, *El concepto de perjuicio en el delito de estafa análisis dogmático*, 61. Y https://www.unifr.ch/ddp1/derechopenal/articulos/a_20100831_02.pdf (consultado el 08 de diciembre de 2019)

[195] Gustavo Balmaceda Hoyos, *El delito de estafa informática* (Bogotá, D.C., Colombia: Leyer, 2009). 62.

[196] Palazzi, *Delitos informáticos*, 70.

dichas entidades estaría lesionando la seguridad de estos datos personales como bien jurídico que debe proteger el Estado.

Las víctimas de los ciberdelitos pueden ser individuos -personas naturales-, así como gobiernos, Instituciones estatales, Bancos, Fundaciones, Sociedades, etcétera, en otras palabras cualquiera puede ser víctima de un ciberdelito, pero para serlo es indispensable que las mismas usen sistemas automatizados de información, generalmente conectados a internet o que operen utilizando una computadora o aparato basado en las TIC´S.

Las características comunes o más habituales de este tipo de víctimas, -cuando son personas naturales- son las siguientes: Son personas nuevas en la red (novatos en de internet) o como se dijo antes *migrantes digitales,* son sujetos inocentes por naturaleza individuos "desesperados" que son codiciosos, solitarios, o que tienen necesidades de carácter emocional, con frecuencia existen "pseudo víctimas", es decir, personas que informan haber sido atacadas pero en verdad no lo han sido, y en último lugar, en la mayoría de los casos, se trata de personas que simplemente son desafortunadas por estar en el lugar (virtual) equivocado en el momento equivocado.[197]

La víctima de un ciberdelito padece lo que se conoce como impotencia aprendida, un sentimiento que se adquiere según los psicólogos cuando no se sabe suficiente de un problema o no se sabe cómo resolverlo. Esta sensación es idéntica a la que existe fuera de Internet; pero, agravada porque se cree por la víctima que ha desarrollado nuevas capacidades en la Red y se siente especialmente defraudada por ese fracaso, les irrita el haber sido engañadas,

[197] Balmaceda Hoyos, *El delito de estafa informática*. 62.

pero lo malo es que acepta la situación como una consecuencia por el uso de las TIC´S.[198]

En las personas existe una idea que ante los ciberdelitos existe impunidad y que no se puede hacer nada, en contraposición a lo que ocurre con los delitos en la vida real donde la gente sabe que puede acudir a una delegación de policía o a la fiscalía a interponer una denuncia, por eso ante los delitos *"on line"* la mayoría de la población no sabe que hacer o cómo reaccionar, se crea un stress emocional y se cree erróneamente que acudir a las autoridades es una pérdida de tiempo porque tiene "la idea de que internet otorga impunidad a las actividades ilegales, pero en la Red todo deja rastro"[199]

Por esto, se reconoce que para conseguir una prevención efectiva a los Ciberdelitos se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la ciberdelincuencia presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como su forma de encubrimiento que pueden representar las mismas dentro de la ingeniería social a las que muchas veces está sometido.

3.2.1.1.8. Circunstancias de tiempo, espacio y desarrollo tecnológico

Los temas enunciados en el epígrafe anterior están relacionados con modalidades de realización del tipo objetivo como: *El tiempo* en el que se ejecuta la acción, su *forma* de perpetración, el ***lugar*** o espacio donde se concreta y el nivel de dominio de las TIC´s que se tenga por los sujetos activos o pasivos del tipo del ciberdelito. Como lo afirma GARRIDO MONTT en

[198] Parraf. Sanjurjo Rebollo, *Manual de Internet y redes sociales*, 230.
[199] Ibid. 231.

principio, no siempre tales circunstancias tienen importancia para el tipo objetivo, por ello sólo de modo excepcional la ley las considera, pero en determinadas situaciones ofrecen interés.[200] En estas circunstancias modificativas del delito, que como elementos adicionales que se contienen en los tipos penales y que según su descripción típica atenúan o agravan la conducta[201] tiene especial importancia la agravante, ya que es la circunstancia de tiempo, lugar, modo, condición y estado que acompañan a algún hecho ilícito para aumentar la gravedad del mismo y por consiguiente la pena con la que debe ser castigado el delincuente.[202]

Respecto de las circunstancias del lugar, en ocasiones se hace referencia a que el delito en cuestión "ocurra en el país, a bordo de aeronave, etc" , esto es que se especifica el lugar donde debe ocurrir la conducta para que satisfaga la hipótesis normativa, pero en el caso de los ciberdelitos estas conductas se realizan a través de la Internet, un ente atopológico que sirve de medio a los delincuentes para buscar la impunidad de sus actos[203]. No obstante lo dicho, se considera que la internet no solo es el medio, sino el espacio "virtual" donde se cometen los ciberdelitos, que muchas veces implican también la extraterritorialidad en su realización, pues la red de redes no conoce de fronteras ni de límites geográficos, como lo dice FLORES PRADA: *"Sobresale sin duda la configuración anárquica y supranacional de la red -internet- como un espacio transfronterizo que carece de centro de decisión"*[204] que es una de las críticas que se le hace a la LECDIC que no va acompañada de acuerdos

---

[200] Garrido Montt, *Derecho penal*. 59.
[201] https://archivos.juridicas.unam.mx/www/bjv/libros/5/2379/5.pdf consultado el 20 de julio 2021.
[202] Ibid.
[203] Parraf. Nava Garcés, *Delitos informáticos*, 2016. 97.
[204] Ignacio Flores Prada, *Criminalidad Informática. Aspectos Sustantivos y Procesales"* (Valencia, España: Tirant lo Blanch, 2012). 49.

multilaterales ni bilaterales con otras naciones que permitan el esclarecimiento de los hechos delictivos, como se verá más adelante.

En cuanto al desarrollo tecnológico se ha dicho que este depende del dominio de las TIC´s en mayor o menor medida, para el caso de la LECDIC está ha tomado como una circunstancia agravante el tener facilidad o conocimiento sobre sistemas o programas informáticos, p.e. el caso de la estafa agravada informática Art. 10 inc. 2 LECDIC por ser empleado de la entidad o en el caso de la divulgación no autorizada Art. 23 inc. 3 LECDIC donde se pone en evidencia que los conocimientos cualificados de los sujetos activos de dichos delitos generarán para ellos en caso de hacer encontrados responsables, de penas más severas que las del tipo básico.

3.2.1.2 Tipo Subjetivo

Según ROXIN frente a la objetividad del tipo autores como MAYER Y MEZGER descubrieron que en muchos casos, no ya la culpabilidad, sino ya el injusto del hecho depende de la dirección de la voluntad del autor[205], en la actualidad se ha impuesto la concepción de que hay un dolo subjetivo y que éste se compone del dolo y en su caso de otros elementos subjetivos del tipo adicionales al dolo[206] En palabras de SILVESTRONI: El tipo subjetivo es la descripción subjetiva de la conducta penalmente relevante; es la descripción del conocimiento y la voluntad de la acción que interesan para individualizar dicha conducta[207]. Este tipo subjetivo está compuesto del dolo y otros elementos especiales de autoría que serán estudiados a continuación de una forma breve.

---

[205] Claus Roxin, *Derecho penal. Parte general* (Madrid, España: Editorial Civitas, 1997). 280.
[206] Roxin. 307.
[207] Silvestroni, *Teoría constitucional del delito*. 258.

3.2.1.2.1. Dolo

Dentro del tipo subjetivo del tipo se encuentra como elemento del mismo “el dolo”, el cual es el conocimiento y voluntad que tiene el sujeto activo de un delito de la realización del tipo objetivo, por ello se dice que ante una conducta una persona obra con dolo, en consecuencia, él sabe lo que hace y hace lo que quiere. El dolo es la subjetividad referenciada a la descripción objetiva del tipo[208] Los componentes de dolo son: a) El componente cognitivo: Que es el conocimiento del tipo objetivo del injusto; y b) El componente volitivo: Que es la voluntad que tiene el sujeto de realizar el injusto. Para el caso de los ciberdelitos que requieren ciertos conocimientos de informática por parte del sujeto activo, debe considerarse que la realización del tipo objetivo de cualquiera de los delitos contenidos en la LECDIC ha sido realizado con dolo directo, pues el sujeto quiere realizar los elementos del tipo y adecua su conducta a la norma, es decir, realiza su conducta a fin de generar la tipicidad de su acción.

3.2.1.2.2. Elementos Especiales de Autoría

Sobre este tema, relacionado con los Ciberdelitos -que en España son englobados en la expresión “delitos informáticos”- se comparte la opinión de ACURIO quien citando al profesor ROMEO CASABONA señala que: “Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características

[208] Ibíd. 259.

semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados)"[209].

Es de hacer notar que SANCHEZ BARAHONA considera necesario crear perfiles del ciberdelincuente, en el cual es importante la participación de la criminología ya que el estudio y análisis de las motivaciones que influyen en el ciberdelincuente no hace distinción en cuanto a si el delito informático ha sido el medio (sustracción de secreto de empresa) o el objetivo (destrucción de un registro informático relacionado con el secreto empresarial). Según las investigaciones llevadas a cabo por Kranenbarg Weulen han expuesto es que en ambos casos podemos extraer motivaciones intrínsecas o extrínsecas que guían las acciones delictivas de los infractores.[210]

Las **motivaciones intrínsecas** surgen como las más relevantes puesto que la mera actividad ilícita se convierte en la verdadera recompensa para el infractor, es el beneficio principal de su acción. El infractor se nutre de la curiosidad, del autoaprendizaje, del reto para romper barreras informáticas, lo hace por aburrimiento o porque está de moda. En cambio, **las motivaciones extrínsecas** tienen que ver con los resultados de sus acciones: al infractor le motiva actuar por venganza, movido por la ira o por hacer bullying contra la víctima, por causar impresión en otras personas o para enviar un mensaje determinado al objetivo, porque actúa motivado por el lucro personal o porque

[209] https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consultada en 20 de julio 2021.

[210] https://www.camjol.info/index.php/DERECHO/article/download/12223/14276/44901 consultado el 17 de septiembre de 2021.

sus acciones son actos políticos dirigidos, y en ocasiones la guía es una posición de poder que únicamente puede lograrse en forma virtual[211].

Según lo dicho es muy difícil englobar elementos especiales de autoría para los distintos tipos de ciberdelitos, ya que como se dijo en este capítulo se ha podido determinar que el bien jurídico protegido con base a la LECDIC es la información y la seguridad informática, por lo cual en la realización de estos hechos ilícitos en conexión se dañan otros bienes jurídicos, lo cual puede permitir fijar algunos elementos especiales de autoría, tales como:

-**Ánimo de Lucro:** Este elemento especial de autoría está relacionado con aquella circunstancia que sirve de motivación al sujeto activo para realizar la acción típica, naturalmente el ánimo de lucro, ampliamente interpretado, incluye cualquier tipo de ventaja o beneficio patrimonial que el sujeto se proponga conseguir mediante el apoderamiento de alguna cosa mueble ajena[212]; en relación con la LECDIC este elemento motivacional se ve requerido en los delitos de Estafa Informática (Art. 10), el Fraude informático (Art. 11), hurto por medios informáticos (Art. 13) y los comportamientos relacionados a tarjetas inteligentes: tales como la manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (Art. 16), obtención indebida de bienes y servicios por medio de tarjetas inteligentes o medios similares (Art. 17) y la provisión indebida de bienes y servicios (Art. 18)

-**Motivación Egocentrista**: Este elemento es el que lleva a los sujetos activos a realizar las conductas de intrusismo o allanamiento informático pues este se comete cuando **una persona con ciertos conocimientos y habilidades**

[211] Ibíd.
[212] Miguel Alberto Trejo et al., eds., *Manual de derecho penal. Parte Especial*, 2º Edición (San Salvador: Centro de Información Jurídica, Ministerio de Justicia, 1999). 764.

informáticas viola las medidas de seguridad de un sistema utilizando su experiencia y conocimientos informáticos. Por lo tanto, el sujeto activo o autor del delito siempre será un especialista informático, ya que se entiende que un usuario medio carece de las habilidades necesarias para cometer este delito[213]; en la regulación de dicho tipo penal se hace referencia a la persona que, sin la correspondiente autorización, utiliza cualquier medio o procedimiento para vulnerar las medidas de seguridad establecidas para evitar ataques o accesos que no estén permitidos en un sistema de información. El especialista informático procurase **el acceso para él o facilitárselo a un tercero**, y el delito se perfecciona tanto con el mero acceso como el impedimento de uso de la persona con derecho legítimo de uso.[214]

El sujeto activo busca acceder a un sistema informático, por puro ego o por demostrar a sus contemporáneos generacionales que es capaz de vulnerar la seguridad de un sistema informático, circunstancia que lo hace acreedor de un delito doloso de comisión por lo que no puede realizarse por mero descuido o imprudencia. No obstante, para que el hecho sea delito **basta con el mero acceso al sistema informático**, por lo que no se requiere que el especialista abra los archivos, datos o programas que se encuentran en dicho sistema, es decir, que los hackers que entran por mera curiosidad a un sistema informático para buscar vulnerabilidades y comunicarlas están cometiendo este ilícito penal[215], pero pueden además divulgarlo, transferirlo o utilizarlo para algún fin ya en esos casos se está en presencia de un intrusismo más invasivo a la víctima.

---

[213] https://iurisnow.com/es/articulos/delito-intrusismo-informatico/ consultado el 2 de agosto de 2021.
[214] Ibíd.
[215] Ibíd.

En la LECDIC la figura del intrusismo se pueden clasificar y manifestar en ilícitos así: a) Acceso Indebido: a sistemas informáticos (Art. 4) y a programas o datos informáticos (Art. 5); b) Formas complementarias: Violación a la seguridad del sistema (Art. 9) y posesión de equipos u ofrecimiento o prestación de servicios para la vulneración de la seguridad (Art. 8); c) Obtener o interceptar información, que se manifiesta en los siguientes ilicitos: Interceptación de transmisiones entre sistemas de las tecnologías de la información y la comunicación (Art. 21); Espionaje informático (Art. 12); y la obtención y transferencia de información de carácter confidencial (Art. 25); d) divulgar o transferir información, que se manifiesta en los iliictos de: Divulgación no autorizada de contraseñas y claves de acceso (Art. 23) y en la revelación de datos o información personal (Art. 26); y e) Utilización indebida de la información, que se expresa en los ilícitos de Hurto de identidad (Art. 22) y la utilización de datos personales (Art. 24).

-**Ánimo de Dañar:** Es toda conducta típica realizada por el sujeto activo que destruye una cosa, sin lucro ni transferencia dentro del patrimonio de la misma víctima, no puede tener más propósito que el de perjudicar al titular del derecho, de ahí que sea necesario identificar como, elemento especial del ánimo, el propósito definido de causar daño en perjuicio de otra persona; ello porque el dolo de este delito no es un dolo común ya que se produce un daño injuriosamente producido, causado por el autor a sabiendas de su injusticia y adrede que no se enmarcar dentro de una estructura típica de naturaleza culposa.[216] Dentro de este elemento se puede encuadrar el sabotaje o daño informático que atenta contra la integridad de un sistema de tratamiento de información o de sus componentes, su funcionamiento o de los datos contenidos en él, que se encuentra clasificado de la siguiente manera: a)

[216] Trejo et al., *Manual de derecho penal. Parte Especial*. 942.

Sobre el sistema informático: Que se representa a través de los siguientes ilícitos de la LECDIC: Interferencia del sistema informático (Art. 6), las técnicas de denegación de servicios (Art. 14) y los daños a sistemas informáticos (Art. 7); y b) Sobre datos o registros: Que se representa a través de los siguientes ilícitos: Alteración, daño a la integridad y disponibilidad de los datos (Art. 19) y la interferencia de datos (Art. 20).

-**Motivación Política:** Este elemento es uno de los más alarmantes en la actualidad y que han generado la realización de distintos Ciberdelitos alrededor del mundo, como lo puso en evidencia en el Diario "La Razón" de España al indicar: En 2016 se produjo un «alarmante aumento» de ciberataques con motivaciones políticas y **se detectó una «tendencia creciente» al ciber sabotaje para intentar influir en la política** y sembrar conflicto en otros países, según la compañía de seguridad Symantec, que ha hecho público que las amenazas a la seguridad en internet, destaca que **el año 2016 estuvo marcado por ciberataques «extraordinarios»**, por campañas diseñadas para **desestabilizar organizaciones y países,** como sucedió durante el proceso electoral de Estados Unidos. «Los ciberdelincuentes, en ocasiones **«patrocinados por gobiernos»**, han demostrado «nuevos niveles de ambición», son «ataques devastadores desde el punto de vista político, en un movimiento que pretende socavar a un nuevo tipo de objetivos»[217] ya que lo que se busca es difundir un discurso de odio hacia una corriente política o hacia un adversario político siendo factores extrínsecos que motivan al sujeto activo para que realice los Ciberdelitos, los cuales pueden ser muy variados según el tipo de coyuntura que se este

[217]https://www.larazon.es/tecnologia/los-ciberataques-con-motivacion-politica-se-disparan-LG15028672/ consultada el 18 de septiembre de 2021.

viviendo y el grado tecnológico de la población para determinar si cumplirá el objetivo o los objetivos que buscan los ataques.

3.2.1.3 Tipo Culposo o Imprudente

Para SILVESTRONI la culpa es un elemento subjetivo del tipo que consiste en la representación del riesgo que amenaza a un bien jurídico, a diferencia de lo que ocurre con el dolo, el conocimiento que caracteriza a la culpa no recae sobre el resultado típico ni sobre los elementos objetivos del tipo doloso; hay culpa cuando se tiene conocimiento del riesgo y se desconoce que éste desembocará en el resultado, aunque este suceso sea previsible.[218]

No obstante lo dicho, se comparte la idea de MUÑOZ CONDE en el sentido de considerar la culpa más que un elemento del tipo subjetivo del tipo, como un verdadera clase de tipo, que debe ser llamado "tipo culposo o imprudente" pues la observancia del deber jurídico de cuidado, también llamada "diligencia debida" constituye el punto de referencia obligado del tipo de injusto del delito imprudente, ya que éste es la realización imprudente de los elementos objetivos de un tipo de delito, no se castiga siempre pues el principio de intervención mínima obliga a una doble restricción, seleccionando por un lado aquellos comportamientos imprudentes que afectan a bienes jurídicos fundamentales y castigando de entre todos ellos los comportamientos que llegan a producir realmente un resultado lesivo para dichos bienes jurídicos.[219]

En el caso de la LECDIC se puede apreciar que solo un comportamiento fue definido por el legislador que puede catalogarse como delito culposo o imprudente, el cual es **"los daños a sistemas informáticos"** regulados en el

[218] Silvestroni, *Teoría constitucional del delito*. 270-271.
[219] Parraf. Muñoz Conde, *Teoría general del delito*. 66.

Art. 7 inc. 2 que literalmente establece: *"Si el delito previsto en el presente artículo se cometiere de forma culposa, por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, será sancionado con prisión de uno a tres años."* Fuera de esta disposición todas las otras conductas reguladas en la LECDIC deben ser realizadas con dolo, por ello en El Salvador en materia de ciberdelitos solo los daños informáticos fueron tomados por el legislador como tipo de injusto que puede realizarse bajo la clasificación de culposo o imprudente.

3.2.2. LA ANTIJURIDICIDAD EN EL CIBERDELITO

Siguiendo con el análisis dogmático, una vez afirmada la tipicidad, del caso real concreto, es decir, una vez comprobado que el caso es subsumible en el supuesto de hecho del tipo del delito previsto en la norma penal, el siguiente paso, en orden a la averiguación de si ese caso puede engendrar responsabilidad penal, es la determinación de la antijuridicidad, es decir, la constatación de que el hecho producido es contrario a derecho. El término antijuridicidad expresa la contradicción entre la acción realizada y las exigencias del ordenamiento jurídico. El derecho penal no crea la antijuridicidad sino que selecciona, por medio de la tipicidad, por consistir en ataques muy graves a bienes jurídicos muy importantes, conminándolos con una pena.[220]

Para REYES ECHANDIA la antijuridicidad es el juicio negativo de valor que el juez emite sobre una conducta típica en la medida en que ella lesione o ponga en peligro, sin derecho alguno, el interés jurídicamente tutelado en el tipo penal, se habla de un juicio desvalorativo porque la naturaleza de la conducta lleva a un enjuiciamiento negativo de la misma, desde el momento en que ella

[220] Muñoz Conde, 82.

se pone en contradicción con el ordenamiento jurídico penal y se hace referencia al juez como la persona que emite el juicio respectivo porque es él quien en nombre del Estado declara el desvalor de la conducta enjuiciada. Finalmente la expresión "sin derecho alguno" hace referencia que cuando se lesiona o se pone en peligro un interés jurídicamente tutelado en circunstancias que justifiquen la lesión, llamadas "causas de justificación" tal conducta a pesar de ser típica no es antijurídica.[221]

Lo dicho en los párrafos precedentes es aplicable al ciberdelito, pues este elemento se encuentra dentro de los elementos del delito tradicional y la LECDIC no escapa de la aplicación de este elemento en sus tipos penales, por ello es posible que estudiando las particularidades que rodean una determinada conducta cometida teniendo por objeto o mediante el uso de las TIC´S se pueda establecerse un juicio de reproche o por el contrario determinar si existe una o varias causas de justificación aplicando las reglas generales del Código Penal.

3.2.3 LA CULPABILIDAD EN LOS CIBERDELITOS

La comprobación de la realización de un hecho ilícito (típico y antijurídico o no justificado) y atribuible al autor no es todavía suficiente para determinar la responsabilidad penal de éste, es decir, la obligación de responder ante el ordenamiento jurídico, por ello se dice que la culpabilidad es la reprochabilidad jurídico penal, por ende culpable es aquél que, pudiendo, no se ha motivado ni por el deber impuesto por la norma, ni por la amenaza penal dirigida contra la infracción de la misma.[222]

---

[221] Alfonso Reyes Echandía, *Antijuridicidad*, cuarta edición (Santa Fe de Bogotá: Temis, 1999), 23.
[222] Paraf. Bacigalupo, *Lineamientos de la teoría del delito*, 85.

Para CHOCLAN la culpabilidad, como categoría sistemática del delito, es una culpabilidad jurídica y no una culpabilidad ética, es decir, el objeto del reproche es una acción disconforme con el Derecho no con la Moral. Además, la culpabilidad lo es por el hecho individual y no por el género de vida, pues el juicio de reproche tiene por objeto el hecho cometido por el autor y no el desarrollo de su personalidad. La culpabilidad por el hecho es reconocida hoy por la posición dominante no sólo como presupuesto de la pena sino también como medida de la pena, esto es, como conjunto de determinados elementos que poseen relevancia para la magnitud de la pena en el caso concreto.[223]

De acuerdo con el concepto normativo de la culpabilidad ésta es, desde un punto de vista formal, la reprochabilidad personal por el hecho cometido. Desde un punto de vista material se pretende dar respuesta a la interrogante de *"por qué ello se le reprocha al sujeto"* [224] para poder reprochar la conducta es indispensable determinar la capacidad de culpabilidad del sujeto o si el mismo era inimputable, el conocimiento que el mismo tenga de la antijuridicidad de su comportamiento y la exigencia de que debe actuar conforme a las normas jurídicas.

Como se pone en evidencia, la culpabilidad conforma una categoría de la sistemática de la teoría general del delito es fácilmente trasladable a la figura del ciberdelito, ya sea que este tipo de hechos se encuentre regulados en el Código Penal o en una ley especial penal, como es el caso de El Salvador con la LECDIC, por lo cual no se presenta ninguna particularidad especial que requiera atención.

---

[223] Calderón Cerezo y Choclán Montalvo, *Derecho Penal. Tomo I. Parte General*, 200.
[224] Ibíd. 201.

3.3. CLASIFICACION DE LOS CIBERDELITOS

En este apartado se pretende estudiar las clasificaciones de ciberdelitos existentes más importantes expuestas por la doctrina y las opiniones que al respecto diversos autores tienen de los mismos, así como Organizaciones internaciones a fin de tener un panorama general de cómo están catalogados, partiendo de la visión que se utilizará como criterio la actividad que realizan los sujetos activos más que el espacio utilizado para cometer los ilícitos.

En el apartado anterior se estudió a profundidad la clasificación con base a estos dos criterios: como instrumento o medio, o como fin u objetivo, que es expuesta tanto por Tellez como por Palazzi[225] la que, para no caer en repeticiones indebidas se resume en ver que los ciberdelitos pueden visualizar:

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

b) Como fin u objetivo, se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Para Lima Malvido,[226] clasifica lo que ella llama “delitos electrónicos” en tres categorías a saber:

1. Los que utilizan la tecnología electrónica como método
2. Los que utilizan la tecnología electrónica como medio y

[225] Ver Téllez Valdés, *Derecho informático*; Palazzi, *Delitos informáticos*.
[226] Citada por Nava Garcés, *Delitos informáticos*, 2016. 110.

3. Los que utilizan la tecnología electrónica como fin.

En otras palabras, dicha autora agrega una forma más de realizar los ciberdelitos, el cual es el criterio como método que consiste en utilizar la información o un sistema informático como procedimiento para realizar los ilícitos. Aunque a todas luces puede apreciarse que no hay mayor diferencia entre utilizar las TIC´S como medio para realizar conductas ilícitas que utilizándolo como método, por lo cual esta autora no expresa una mayor precisión o fundamentación de su criterio de clasificación.

Para Davara Rodríguez,[227] indica que la manipulación mediante la informática puede provenir de dos vertientes diferentes: a) acceso y manipulación de los datos, y b) manipulación de los programas. Y así también el mismo autor realiza una clasificación de seis acciones de acuerdo al fin que persigue:

- Manipulación en los datos e informáticos contenidas en los archivos o soportes físicos informáticos ajenos,
- Acceso a los datos y utilización de los mismos por quien no está autorizado a ello,
- Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas,
- Utilización del ordenador y/o los programas de otra persona sin autorización, con el fin de obtener beneficios propios y en perjuicios de otro,
- Utilización del ordenador con fines fraudulentos y
- Agresión a la “privacidad” mediante la utilización y procesamiento de datos personales con fin distintos al autorizado.

[227] Nava Garcés, *Delitos informáticos*, 2007. 41

La OCDE fue la primera organización de carácter internacional que elaboró un informe con los diferentes tipos de delitos ciberdelitos existentes; en su informe "Delitos de informática: análisis de la normativa jurídica" de 1986 [228], clasificación que no ha modificado, a pesar de haber realizado sendos informes de directrices para la seguridad de sistemas y redes de información en los años 1992 y 2002.

En este informe de 1986 la OCDE estableció las que debería ser las líneas generales de las políticas legislativas para prevenir la delincuencia informática y realizó una primera clasificación de cuáles eran las conductas que debían recogerse en las legislaciones penales a fin de atacar frontalmente el fenómeno de los Ciberdelitos. Las cinco acciones que señalaba el informe como merecedoras de reproche penal eran:

1.-La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de computadora con la intención de cometer una transferencia ilegal de fondos o de otra cosa de valor.

2.-La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de computadora con la intención de cometer una falsificación.

3.-La introducción, alteración, borrado y/o supresión deliberada de datos informáticos y/o programas de computadora, u otra interferencia con sistemas

[228] https://grupo4nri.wordpress.com/2-normativa-internacional/ consultada el 24 de abril de 2021.

informáticos, con la intención de obstaculizar su funcionamiento y de las telecomunicaciones.

4.-La infracción del derecho exclusivo del titular de un programa de computadora protegido con la intención de explotar comercialmente el programa y ponerlo en el mercado

5.-El acceso o la interceptación de un sistema informático o de telecomunicaciones producido sin conocimiento y sin la autorización de la persona responsable del sistema, ya sea: i) infringiendo las medidas de seguridad o ii) con intenciones deshonestas o dañinas.

Cabe señalar que las acciones primera, segunda y cuarta utilizan el sistema informático como medio para conseguir sus fines delictivos, en cambio el tercer y quinto tipo de conductas el sistema informático o su contenido se sitúan como los objetos sobre los que recae la acción delictiva del ciberdelincuente.

Para la Organización de las Naciones Unidas (en lo sucesivo ONU) durante el 8º Congreso de las Naciones Unidas para la Prevención del Delito y Justicia Penal celebrado en La Habana, Cuba, del 27 agosto a 7 septiembre de1990[229], la Asamblea General de Naciones Unidas adoptó una resolución relativa a la legislación de delitos informáticos que debían realizar internamente, es decir, por cada Estado parte de esta Organización, basándose en dicha resolución, en 1994 publicó un Manual de delitos informáticos que realiza la siguiente clasificación[230]:

229 Informe general del 8º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, La Habana, Cuba, 27 de agosto a 7 de septiembre de 1990, pp. 149 y ss

230 ONU: "Manual de las Naciones Unidas sobre prevención y control de delitos informáticos" en Revista Internacional de Política Criminal, Ed. Naciones Unidas, nº 43 y 44, 1994. En http://www.uncjin.org/documents/irpc4344.pdf Consultado el 09 de marzo de 2020.

1.-Fraude por manipulación informática: Consiste en modificar los programas informáticos del sistema para conseguir un beneficio patrimonial. La manipulación puede realizarse desde sistemas ajenos, desde el mismo sistema o a través de aparatos electrónicos capaces de engañar al sistema informático atacado. En todos los casos el objetivo de las acciones es conseguir un beneficio patrimonial gracias a la manipulación.

2.-Falsificaciones informáticas: Se produce cuando se alteran de forma ilícita los documentos electrónicos. La ONU también incluye en este apartado los delitos relativos a la utilización de sistemas informáticos para realizar falsificaciones de documentos.

3.-Daños o modificaciones de programas o datos informáticos: Es el acto de borrar, suprimir o modificar sin autorización datos o programas informáticos con la intención de obstaculizar el funcionamiento normal del sistema. Generalmente son producidas por virus informáticos.

4.-Acceso no autorizado a sistemas: Se trata de acceder a sistemas ajenos sin necesidad de estar físicamente presente en donde se encuentra el sistema atacado, a través del uso del Internet.

5.-Reproducción no autorizada de programas informáticos con derechos de autor: Se refiere en general a la reproducción o difusión no autorizada a través de medios informáticos de programas de computadora u otros materiales con derechos de autor.

Como se desprende de la clasificación realizada por la ONU en 1994 se puede afirmar que sigue una línea muy pareja a la realizada por la OCDE en 1986. Con descripciones algo más vagas y con una mayor vocación generalista que

la clasificación anterior, parece reconocer la necesidad de regular penalmente las mismas acciones: fraudes usando computadoras, falsificaciones, daños informáticos, accesos ilícitos y acciones que vulneran la propiedad intelectual. Por ello se puede concluir, al igual que en la clasificación anterior, que los sistemas informáticos pueden situarse en dos vertientes, aquella en la que los sistemas son el objeto sobre el que recae la acción delictiva y aquellos en los que son medios para conseguir los fines ilícitos.

Según el **Convenio sobre la Ciberdelincuencia de Budapest**, de 23 de noviembre de 2001, es otra de las herramientas fundamentales del Derecho internacional para la homogenización de las legislaciones penales respecto de los delitos ciberdelitos[231], estos se clasifican así:

1.-Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: En esta categoría engloba el acceso ilícito (no autorizado) a un sistema informático (art. 2), la interceptación ilícita de transmisiones de datos entre sistemas informáticos o dentro del mismo (art. 3), los ataques a la integridad de los datos (art. 4) o los sistemas (art. 5) y el abuso de dispositivos, es decir, la producción, venta, obtención, difusión u otra puesta a disposición de dispositivos o programas informáticos adaptados para la comisión de los delitos anteriores o de contraseñas o códigos de acceso que permitan acceder a otros sistemas informáticos (art. 6).

2.-Delitos informáticos: Dentro de esta categoría se encontraría la falsificación informática (art. 7) y el fraude informático (art. 8) en la misma línea que las clasificaciones anteriores de la OCDE y la ONU.

---

[231] El texto completo del Convenio se puede encontrar en: http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF consultado el 13 de marzo de 2019.

3.-Delitos relacionados con el contenido: Sanciona la producción de pornografía infantil para su distribución, la oferta, la puesta a disposición, la difusión, la transmisión, la adquisición o la mera posesión en o a través de sistemas informáticos (art. 9).

4.-Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10), de forma similar a las clasificaciones anteriores En esta nueva clasificación destaca sobremanera el nivel de detalle y la inclusión de nuevas acciones. Aparece por primera vez como acción merecedora de reproche penal aquella relacionada con el abuso de dispositivos, que se suma a las anteriores, que además sufren una notoria restructuración y un mayor nivel de detalle en su definición. Además, en comparación con las listas anteriores, cabe destacar que la realizada en este Convenio se hace desde una perspectiva de lógica legislativa, entre otros puntos reflejada en que se estructura sobre la base de un articulado y en que apremia a los Estados a acometer las reformas oportunas en sus ordenamientos penales. La aplicación del mismo deja de ser una mera recomendación, como en el caso de la lista de la OCDE o el Manual de la ONU, o una declaración de intenciones como la Comunicación de la Unión Europea, para convertirse en una norma imperativa de Derecho internacional para aquellos países que ratifiquen el Convenio.

CAPITULO IV: LA INVESTIGACIÓN Y PRUEBA DEL CIBERDELITO

SUMARIO: 4.1. Investigación del delito. 4.2. Crítica a la Investigación Delictiva Tradicional. 4.3. Hacia una Investigación Delictiva Moderna. 4.3.1. Resultados de Investigaciones de ciber crímenes realizadas a nivel internacional. 4.3.1.1 Fraude y Hurto de identidad. 4.3.1.2 caso DarkSide. 4.3.2. Técnicas de Investigación Tecnológica. 4.3.2.1. Obtención de una IP. 4.3.2.2 Mensajes de Datos. 4.3.2.3. El Correo Electrónico. 4.3.2.4 El Chat o Conversaciones en Línea. 4.3.2.5. Redes Sociales. 4.3.2.6. Registro Remoto sobre Equipos Informáticos. 4.3.2.7. El Agente encubierto Informático. 4.3.2.8.Identificación de IMEI, IMSI y MAC. 4.3.2.9. Otros programas que son utilizados para la investigación. 4.4. Actos de investigación. 4.4.1. Actos Urgentes de Comprobación. 4.4.2. Proceso de cadena de custodia de la evidencia digital. 4.5. Prueba de los Ciberdelitos. 4.5.1 Prueba Electrónica. 4.5.2. Prueba Pericial.

RESUMEN

En este capítulo se pretende analizar las técnicas de investigación policial del ciberdelito y como sus resultados pueden ser presentados como prueba en el correspondiente proceso penal. La temática será examinada en forma general y no enfocada a un determinado ciberdelito, a fin de que el lector pueda encontrar una guía fácil para verificar las técnicas más convenientes para cuando tenga un caso en concreto o en su caso pueda analizar si la misma requiere o no autorización judicial para su realización ya que en la investigación puede que en ciertos casos afectarse derechos fundamentales del investigado.

4.1. INVESTIGACION DEL DELITO

Las funciones estatales encomendadas a la Fiscalía General de la Republica, por mandato constitucional del Art. 193, son fundamentales para el mantenimiento del Estado de Derecho principalmente la de defender los intereses del Estado y la sociedad, así dirigir la investigación del delito con la colaboración de la PNC suelen ser consideradas no solo una facultad, sino también como un deber propio del Estado, para combatir la delincuencia o la criminalidad; esta función debe cumplirse en forma necesaria, obligatoria y ser, además, auto limitativa. El Estado logra su función penal, a partir del "ius puniendi", es decir, un poder jurídico que el Derecho objetivo concede al ente estatal para garantizar el mantenimiento del orden jurídico y restablecerlo cuando ha sido perturbado. Desde ese punto de vista, el derecho de castigar es la facultad que tiene el Estado para actuar de conformidad con las normas del Derecho, que son su límite; pero a ese Derecho Penal subjetivo, visto como función penal del Estado, se la ha señalado una doble característica; al mismo tiempo que un poder, es también un deber.[232]

La investigación criminal se constituye como el proceso tendiente a comprobar la existencia de un hecho o conducta delictiva, identificar o por lo menos individualizar a sus autores y participes, así como recolectar las evidencias que permitan definir la responsabilidad de los mismos, encaminado a que la Fiscalía promueva el ejercicio de la acción penal[233] de conformidad con la ley.

En atención a lo dicho la Constitución de la Republica, Art. 193 Ord 3º, establece que el encargado de la función punitiva el Estado es el Fiscal

---

[232] Armando Antonio Serrano et al., eds., *Manual de derecho procesal penal.* (San Salvador: Centro de Información Jurídica, Ministerio de Justicia, 1998), 27.
[233]https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/ManualUnicoInvestigacion.pdf consultado el 28 de abril de 2021.

General de la Republica, a través de sus auxiliares ya que le corresponde dirigir la investigación del delito con la colaboración de la policía nacional civil en la forma que la ley determine, siendo esta forma la establecida en el Art. 270 CPP que tiene por fin recoger los elementos que pueden servir como prueba, tanto de cargo como de descargo, en el eventual proceso penal que pudiera formarse en caso de constatar que existe un hecho delictivo y la participación de uno o varios sujetos en el mismo, así mismo el Fiscal General por medio de sus auxiliares coordinaran la investigación del delito junto con la Policía Nacional Civil, según lo prescrito en el Art. 272 CPP.

Por ello la investigación de todo hecho ilícito principia con los actos iniciales de investigación, que constituyen los diferentes canales por los cuales se tiene conocimiento por la FGR de la comisión de un hecho delictivo, los cuales son aplicables a los ciberdelitos ya que estos pueden llegar a conocimiento a través de un aviso, una denuncia, o una querella, según lo prescrito en los Arts. 260 y ss del CPP, siendo que estas deber ser interpuestas en la FGR; para el caso de las denuncias o querellas la ley habilita a que las mismas sean interpuestas en la PNC o en un Juzgado de Paz, para luego ser remitidas a Fiscalía y al ser asignado un auxiliar para llevar dicho caso éste deberá girar la respetiva ***"dirección funcional"*** que es la orientación técnica jurídica que el Auxiliar del Fiscal General que llevará el caso debe proporcionar al investigador policial, para establecer la comisión de un hecho punible y determinar la responsabilidad de quien lo cometió, siendo así que inicia la fase de investigación administrativa.

.

Lo dicho hasta este momento, es tan aplicable a la delincuencia tradicional como a la ciberdelincuencia, por eso a continuación se hará una crítica a la aplicación de la forma tradicional de investigación al tema del ciberdelito hasta

llegar a las formas y técnicas actuales de investigación de los mismos y su tratamiento probatorio.

4.2. Critica a la investigación delictiva tradicional

La investigación, desde la perspectiva del proceso penal, viene integrada por el conjunto de actos encaminados a averiguar la existencia de un hecho conocido que tuviere apariencia de delito, de sus circunstancias y de sus posibles autores; se trata, en todo caso, de una investigación para el proceso, una actividad previa y práctica, que busca proporcionar una información relevante y que se constituye como presupuesto del ejercicio del *ius puniendi* del Estado[234] La investigación genera elementos probatorios, tanto de cargo como de descargo, que deben ser evaluados por sus autores conforme los van obteniendo a fin de proceder a su aportación, pero ello es algo distinto, y no debe confundirse, a su valoración, ya que la apreciación de la prueba, es tarea exclusiva del órgano enjuiciador. Y así, el juez adopta un papel de controlador de las garantías, velando, desde una posición de imparcialidad, porque en la investigación se respeten las garantías procesales, pero sin que sea el órgano judicial el que directamente deba implicarse en la investigación.[235]

Por lo que se refiere al contenido de la investigación penal, su legitimidad requiere "que se identifique un objeto fáctico"', pues son inconstitucionales las investigaciones sobre una persona, o las indagaciones generales o prospectivas, no concretadas en un objeto fáctico determinado.[236] En cuanto a los actos de investigación, dentro de este apartado se inscriben las técnicas de investigación tecnológica, entre las cuales desempeñan un papel

---

[234] María del Carmen Ortuño Navalón, *La Prueba Electrónica Ante los Tribunales* (Valencia: Tirant lo Blanch, 2014), 17.
[235] Ortuño Navalón, 53.
[236] Ortuño Navalón, 53.

primordial, las técnicas de video vigilancia y la obtención de información a partir de soportes electrónicos documentales, de voz o de imagen.[237]

Como ya fue expresado, supra, la investigación tiene en el sistema penal salvadoreño dos fases: a) La administrativa y b) la de Instrucción formal dentro del proceso. En la primera lo que se busca es preparar la presentación del caso ante el juez competente para que se inicie el proceso o determinar que no existe la posibilidad de presentar un caso al órgano jurisdiccional, pero para eso el fiscal en coordinación con la policía debe de emplear técnicas investigativas reguladas en el CPP o en caso que no exista en este cuerpo normativo una técnica o procedimiento de investigación buscar una solución dentro del ordenamiento jurídico nacional, según lo establece el principio de libertad probatoria (Art. 176 CPP), teniendo en cuenta el respeto a las garantías fundamentales de las personas.

En el caso de la investigación de los ciberdelitos el CPP vigente prescribe la realización, dentro de los actos urgentes de comprobación, de operaciones técnicas por parte de la PNC (Art. 186) y la obtención y resguardo de información electrónica (Art. 201); en las diligencias iniciales de investigación, el Fiscal puede ordenar con el consentimiento de la víctima la grabación por cualquier medio electrónico de las comunicaciones telefónicas, radiotelefónicas o que utilicen el espectro electromagnético (Art. 281) y fuera de dichos artículos el legislador guardo silencio en cuanto a técnicas o medios de prueba que pudieran facilitar la labor de investigación, tanto en la etapa administrativa como en la instrucción, por lo cual siguiendo el ejemplo de España, que mientras no se habían hecho reformas a la ley en enjuiciamiento criminal para admitir prueba electrónica los jueces debieron suplir esa vacío

[237] Ibid.

con las normas de la Ley de Enjuiciamiento Civil que era más reciente y contenía prescripciones al respecto de esta tipo de pruebas; por esa razón a la realidad de El Salvador se debe de recurrir al Código Procesal Civil y Mercantil, específicamente a los Arts. 396 y siguientes, que regula los medios de reproducción de sonido, voz, imagen y almacenamiento de información para tratar de llenar el vacío que existe.

Resulta evidente que la regulación de técnicas y prueba novedosos en El Salvador es deficiente e insuficiente para tratar de dar respuesta al problema de la ciberdelincuencia, por lo que sobre medios de prueba tradicionales debe tratar de aplicarse las técnicas policiales de investigación, tales como la intervención de las comunicaciones electrónicas, ADN, pruebas videográficas, documentos electrónicos o pericias informáticas. Ello obliga a operar sobre cada medio de investigación, aplicando el principio de libertad probatoria para aplicar el régimen legal más semejante y doctrina jurisprudencial existente, junto con las reglas que resulten de su naturaleza especifica.[238]

En la investigación tecnológica, las piezas de convicción alcanzan una gran importancia porque constituyen un soporte fundamental de aquella; su papel es relevante para la acreditación del hecho delictivo, por lo que deben extremarse las medidas para su obtención, custodia y presentación o practica en el juicio. Por ello, resulta indispensable cuidar "la cadena de custodia" y su debida identificación, debiendo contarse con una guía de la pista (track) o lugar concreto del soporte, en que se encuentren los contenidos importantes para la causa con el fin de localizar el que interese y así lograr su rápida operatividad.[239]

---

[238] Ortuño Navalón, *La Prueba Electrónica Ante los Tribunales*. 55.
[239] Ortuño Navalón, 56.

Por eso se comparte la opinión de QUEVEDO al comentar la realidad de España antes de que se hicieran reformas a la ley de enjuiciamiento criminal, que es la misma que se vive en la actualidad en El Salvador: “Los instrumentos de investigación tradicionales se muestran claramente insuficientes para investigar los ciberdelitos, la normativa procesal no contaba con una regulación aplicable a muchas de las técnicas de investigación necesarias para el esclarecimiento de conductas ilícitas ligadas al uso de las nuevas tecnologías. Ley de Enjuiciamiento Criminal no regulaba técnicas específicas para la investigación tecnológica, por lo que se suplía la insuficiencia legal mediante la aplicación de disposiciones genéricas de la propia Ley procesal, mediante la aplicación analógica de los preceptos que regulaban las intervenciones telefónicas, entradas y registro en lugares cerrados, registro de papeles y efectos.”[240]

LLAMAS FERNÁNDEZ y GORDILLO LUQUE[241], advierten de la casuística tan amplia que impera en esta materia de la investigación tecnológica, dado que resulta imposible contemplarla a través del marco normativo vigente, por la vertiginosa progresión de la tecnología sobre la que se apoya y que da pie a una vastísima problemática de orden jurídico-práctico sobre el correcto empleo legal de tales medios. El evidente retraso en la acomodación del Derecho al uso de los medios técnicos, ha provocado que sea frecuente que se tenga que esperar a que por la vía jurisprudencial se consiga validar el uso de los mismos; de otro lado, advierte que las decisiones "ad hoc" de cada órgano jurisdiccional, respecto de la problemática que se le plantee en esta temática

[240] Josefina Quevedo González, “Investigación y prueba del ciberdelito”, 169.
[241]Ortuño Navalón,*La prueba electrónica ante los tribunales.* 56 en el que la autora citando a LLAMAS FERNÁNDEZ, MANUEL Y GORDILLO LUQUE, JOSE MIGUEL. "Medios técnicos de vigilancia'. En Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia. CGPJ. Cuadernos de Derecho Judicial, 2. 2007.

dentro de las causas que conozca, no siempre están revestidas del conocimiento técnico necesario y suficiente, para evitar dar al traste con arduas y rigurosas investigaciones policiales.

La actual legislación procesal nacional no regula de forma clara la actuación del investigador policial de los ciberdelitos, que le permita conocer los límites y atribuciones en la utilización de los medios tecnológicos empleados en el seno de las investigaciones penales, así como cuando será necesario la autorización judicial para realizar ciertas diligencias de cara a la presentación de un proceso ante los tribunales.

4.3. Hacia una investigación delictiva moderna.

Al iniciar este apartado, debe establecerse desde ya que los ciberdelitos son más difíciles de investigar que los delitos tradicionales, porque son novedosos, lo que hace que escapen de los cánones tradicionales, lo que hace que los cuerpos policiales y de los tribunales no estén preparados para investigar y detectar las técnicas novedosas que los delincuentes utilizan para realizar los mismos. Como lo afirma Palazzi en el ambiente digital no quedan huellas visibles a simple vista, y si éstas existen es muy difícil imputarlas a una determinada persona.[242] Sumado a ello, como se ha dicho, que las leyes adjetivas no contengan regulaciones de qué técnicas emplear para investigar y formar luego la prueba para acreditar la conducta hacen que el panorama sea desolador.

Hay que reconocer que en cierta medida, la investigación tradicional incidirá sobre la investigación moderna, es decir, aquella sentará algunas bases de

[242] Palazzi, *Delitos informáticos*, 70.

ésta, ya que la evidencia física y la evidencia digital comparten en la actualidad los mismos fundamentos del modelo de la criminalística en lo que se refiere a minimizar la contaminación en el lugar del hecho, documentar todo lo que se haga, utilizar los principios y los estándares establecidos y tener presente que el objeto primario es la admisibilidad de la evidencia[243] o fuente de prueba que será llevada al juez de la causa a través de los distintos medios de prueba existentes y admisibles en el ordenamiento jurídico.

Los fiscales en relación a la actividad policial, deberán respetar las disposiciones administrativas internas y la cadena de mando, la cual es ejercida exclusivamente por las autoridades jerárquicas respectivas, sin embargo es necesario señalar que entre el criterio administrativo y jurídico debe de prevalecer el jurídico, el fiscal no debe entrar en conflicto con el investigador en aspectos administrativos, y si esto afecta el trabajo técnico lo informará a sus superiores para que estos resuelvan observando de conformidad con la política de persecución penal vigente en su Art. 42.

Los fiscales deben de partir de un plan de investigación, el cual consiste en los diferentes pasos que sirven para investigar y con ello construir la teoría para cada caso, partiendo de una hipótesis criminal preliminar hasta culminar con la conclusión que permita ejercer con éxito la acción penal ante el órgano jurisdiccional. El plan de investigación debe contener tres componentes: 1. **Componente jurídico**: Constituye el encuadramiento jurídico de los hechos dentro las disposiciones legales pertinentes 2. **Componente fáctico**: El mismo se construye confrontando los hechos de las diligencias de investigación con los elementos del delito cometido. 3. **Componente probatorio**: Se determinan

[243] Leopoldo Sebastián Gómez, “Evidencia digital en la investigación penal”, en *Cibercrimen* (Buenos Aires: B de F, 2017), 619–37.

los medios de prueba con los que se cuenta para probar cada elemento fáctico y se determina quién será la persona responsable de obtenerlo y el tiempo que se requerirá para ello.

En este nuevo escenario de la ciberdelincuencia es necesario seguir ciertas técnicas que recaerán sobre ciertos elementos informáticos, que si bien no están reguladas dentro de un cuerpo normativo adjetivo en el país, se encuentran desarrollados en la doctrina y servirán para conformar el componente probatorio al que se ha hecho referencia en el párrafo anterior para que el Agente Auxiliar del Fiscal pueda determinar si hay lugar a formar o no una imputación delictiva. Las cuáles serán analizadas las más representativas a continuación.

4.3.1. Resultados de Investigaciones de cibercrimenes realizadas a nivel internacional.

En este apartado se presentan dos casos, en los que existen 10 años de diferencia entre cada uno, ocurridos en los EE.UU. en los cuales se puede determinar el nivel de avance y tecnificación de las autoridades para la persecución de los Ciberdelitos, su acreditación y la forma de dar con el o los responsables de los mismos, así como a grandes rasgos la forma en la que se cometieron los ilícitos.

4.3.1.1 Fraude informático y Hurto de identidad

Un joven estadounidense Albert Gómez acusado de haber pirateado millones de tarjetas de crédito fue condenado, en el año 2010, a 20 años de prisión por un tribunal federal de Boston (Massachusetts). El joven 'cracker', término que alude a los 'hackers' o piratas informáticos mal intencionados, ha sido inculpado por complot, fraude informático y hurto de identidad. En total, habría

hurtado los datos de más de 130 millones de tarjetas bancarias desde 2006, año que en el cual desde comienzos del mismo el 'cracker' y sus cómplices (dos personas de nacionalidad rusa) "inventaron un medio sofisticado" para infiltrarse en las redes de los supermercados y organismos financieros para hurtar las coordenadas bancarias de sus clientes.[244] A continuación, las enviaban a servidores que operaban en varios Estados Estadounidenses, así como a los Países Bajos y Ucrania.

Los piratas informáticos habían encontrado el modo de borrar su rastro en los sistemas informáticos pirateados. Los piratas utilizaban una técnica que permite acceder a las redes informáticas deseadas sorteando el cortafuegos. Durante el proceso, González ha aceptado devolver a sus víctimas —mediante la confiscación de bienes— lo defraudado, "más de 2,7 millones de dólares" que había utilizado para comprar un apartamento en Miami, un BMW y varios Rolex.. Asimismo, ha reunido un millón de dólares en efectivo que había enterrado en el jardín de sus padres.[245]

4.3.1.2. Caso DarkSide

Este año 2021 el mundo ha conocido del peor intento de extorsión cibernética que obligó a cerrar un importante oleoducto estadounidense, este ciberdelito fue perpetrado por un grupo delictivo conocido como DarkSide, el cual cultiva una imagen de Robin Hood de robarles a las grandes empresas y donar un porcentaje del botín a caridad, según revelaron dos personas al tanto de la investigación; el gobierno del presidente estadounidense Joe Biden señaló que se está trabajando con “todos los recursos disponibles” para restaurar las

[244] https://www.elmundo.es/elmundo/2010/03/25/navegante/1269554529.html consultado en mayo de 2021.
[245] Ibíd.

operaciones y evitar interrupciones en el suministro de combustible, el cual fue detenido por más de tres días y a la fecha es considerado el peor ataque cibernético contra infraestructura vital estadounidense y debería servir de llamada de atención a las compañías sobre las vulnerabilidades que enfrentan[246] ante los ilícitos cometidos a través del Internet.

El oleoducto, operado por **Colonial Pipeline**, compañía con sede en Georgia, EE.UU. transporta gasolina y otros combustibles desde Texas hasta el noreste del país que entrega casi el 45% de la gasolina que se consume en la costa este, según la empresa, fue afectado por lo que Colonial describió como un ataque de ***"ransomware"***[247], en el que los hackers suelen encriptar información para bloquear el acceso a los sistemas de cómputo, lo cual paraliza las redes, y luego exigen un cuantioso rescate para liberar la red.

El responsable de dicho ciberataque, según el FBI, fue el grupo de Hackers conocidos como "***DarkSide" [248]*** que surgió como uno de los principales equipos de *ransomware* en agosto del año 2020; se cree que es un equipo experimentado de delincuentes en línea que opera desde Rusia. La compañía de ciberseguridad *CrowdStrike*, con sede en Silicon Valley, rastreó los orígenes de DarkSide hasta el grupo de hackeo criminal conocido como Carbon Spider, que "reformó drásticamente sus operaciones" el año pasado

---

[246] https://www.latimes.com/espanol/eeuu/articulo/2021-05-09/eeuu-ciberataque-a-oleoducto-esta-ligado-a-grupo-criminal Por Mae Anderson y Frank Bajak Associated Press. 9 de mayo de 2021, consultado el 05 de Agosto de 2021.

[247] Ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo que es infectado por el programa y los ejecutores de este programa piden un rescate a cambio de quitar la restricción que tiene secuestrados los datos.

[248] Que traducido al español significa "lado oscuro" que es una franca alusión a la pelicula "Star wars" (Guerra de las Galaxias) donde se ve una clara batalla entre El lado Oscuro de la Fuerza y el lado justo de la fuerza representado por los caballeros Jedy, muy similar en lo que se encuentra un experto en computación que puede utilizar sus conocimientos para esclarecer hechos delictivos, Hacker Ético o puede dedicarse a realizar hechos delictivos como los conocidos Hackers de este grupo.

para enfocarse en el campo de rápido crecimiento[249] de los programas que funcionan como *ransomware.* Los ataques de ransomware involucran a hackers que toman el control de los datos o sistemas de software de una organización, bloqueando a los propietarios con cifrado hasta que se realiza un pago, que generalmente se hace con criptomonedas para evitar el rastreo, prácticamente es una forma de realizar una extorsión por medios de la Internet, para recuperar el control de los sistemas informáticos de la compañía.

El señor Brett Callow, analista del grupo de seguridad cibernética Emsisoft, referente al ataque que se comenta dijo: "DarkSide no ataca en Rusia, ya que comprueba el idioma que se utiliza en el sistema y, si es ruso, se cierra sin encriptar";[250] por eso se cree que su centro de operaciones se encuentra en dicho país y como forma de conservar el anonimato, ni enfrentar a las autoridades rusas evitan los realizar Ciberdelitos en esa jurisdicción; también se ha investigado que el grupo alquila sus servicios en la web oscura (Deep web), ya que DarkSide es una operación de ransomware como servicio y el mismo ha llevado a determinar el grado de profesionalismo de la *ransomware.*

El sitio web de DarkSide afirma que evitará atacar instituciones médicas como hospitales, asilos, desarrolladores de vacunas, proveedores de servicios funerarios, escuelas, universidades y organizaciones sin fines de lucro y gubernamentales, ya que aunque parezca contradictorio sus administradores manifiestan que el grupo tiene un carácter ético pues el resto de grupos de la industria del ransomware, para quienes los proveedores de atención de salud y el sector público se encuentran entre los principales objetivos. Colonial

---

[249] https://www.milenio.com/negocios/financial-times/hackers-lamentan-dano-a-sociedad-por-oleoducto consultado el 05 de agosto de 2021.
[250] Ibíd.

Pipeline es una empresa privada propiedad de inversionistas como Shell, KKR y Koch Capital.[251]

Se conoce que la compañía víctima “Colonial Pipeline” **pagó en mayo de 2021 la cantidad de 4,4 millones de dólares** en bitcoins a DarkSide a cambio de que desencriptaran los sistemas informáticos de la empresa para poder reiniciar sus operaciones, según ha explicado el Gobierno estadounidense ellos mismos localizaron una cartera de bitcoins asociada al grupo criminal y, **tras pedir una orden judicial**, requisaron 2,3 millones de dólares en forma de 63,7 bitcoins esto generó que la cotización del Bitcoin cayera en un 7% de su valor. Sobre esto se especuló que las agencias de investigación criminal de los Estados Unidos de América habían podido Hackear la Blockchain de la Bitcoin, pero lo que en verdad sucedió fue que al pagar la compañía víctima por liberar sus sistemas, el FBI hizo un rastreo de la parte publica del Blockchain de la Bitcoin, que determina a qué dirección va a parar cada cripto moneda y se determinó que la gran mayoría de los Bitcoins pagados fueron a parar a una dirección que estaba almacenada en un servidor que había sido alquilado por DarkSide, en donde al tomar el FBI el control de dicha dirección pudo controlar la billetera y las claves de acceso a las Criptomonedas a fin de evitar el daño patrimonial original.[252]

La incautación de parte del rescate fue llevada a cabo por **un nuevo grupo de trabajo** del Departamento de Justicia, de los EE.UU. creado para luchar contra "el chantaje digital" y los ataques con 'ransomware'. Esta es la primera operación de este tipo por parte del grupo de trabajo[253]. Con lo dicho en este

---

[251] Ibíd.
[252] https://youtu.be/sEEmY7SFvtg consultado el 05 de agosto de 2021.
[253] https://www.milenio.com/negocios/financial-times/hackers-lamentan-dano-a-sociedad-por-oleoducto consultada el 05 de agosto de 2021.

apartado se puede constatar que los Estados Unidos de América se encuentran en la vanguardía de las investigaciones criminales de los Ciberdelitos, que poseen los equipos y los técnicos necesarios para realizar estas investigaciones: Documentándolas, determinándolas a través de peritajes y logrando esclarecer quienes son sus responsables, lo cual se ha logrado con una investigación delictiva moderna que ha determinado los protocolos de actuación en diferentes casos o que cuentan con analistas debidamente acreditados que pueden determinar las líneas de investigación a seguir en múltiples situaciones.

4.3.2. Técnicas de Investigación Tecnológica

La obtención de elementos de convicción se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.[254]

Para iniciar el estudio de las técnicas de investigación de los ciberdelitos es conocer el proceso de acceso al internet, el cual es el primer paso para realizar cualquier tipo de escrutinio que se haga en sistemas informáticos que hayan sido objeto de ataque cibernético o que sirvan para llegar a los realizadores de los ilícitos cometidos a través de las TIC´s.

Todo usuario que tiene acceso a internet necesita de servicios llamados proveedores de servicios de internet, que dan acceso a la “red de redes”; los

[254] Santiago Acurio del Pino, Manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0 en https://www.oas.org/juridico/english/cyb_pan_manual.pdf

usuarios son identificados cada vez que se conecta a internet, comienza lo que desde el punto de vista informático se denomina una sesión de acceso. Las sesiones de acceso son controladas por los servidores del proveedor de servicios (ISP), que registran en bitácoras (logs), siendo estos dos elementos esenciales para la investigación de los hechos informáticos. Cuando la conexión a internet se hace vía telefónica, el servidor correspondiente del ISP registra el número de teléfono desde el cual se está haciendo la conexión, lo que sirve a su vez para ubicar la sede física o lugar desde el cual se realizó el acceso para navegación, envío de mensajes de datos, etc. Los computadores relacionados con hechos informáticos también poseen la información y configuración de acceso a los proveedores, para que se pueda establecer contacto entre proveedor y los usuarios.[255]

En este proceso de acceso al internet, se puede hacer un rastreo de las páginas de internet visitadas, cuales IP lo han hecho y si se ha compartido información o no, hasta ese momento solo son números no sujetos debidamente individualizados, pero bajo esta forma de actuación es como los investigadores de la policía inician una investigación sobre ciberdelitos.

4.3.2.1. Obtención de una IP

Es el primer paso para desarrollar cualquier investigación sobre un ciberdelito es esta técnica policial. La dirección IP es una etiqueta numérica que identifica a una interfaz (elemento de comunicación/conexión) de un dispositivo (Computadora, móvil, iPad, televisión, consola de videojuegos, etc) dentro de una red que utiliza el protocolo IP. Las direcciones IP son asignadas por los

[255] Juan Carlos Zapata Marcó, “El delito de estafa en la modalidad ‘phishing’ a través de internet y sus medios probatorios en Venezuela,” (Venezuela, Universidad de Carabobo, 2009), 49.

ISP, compañías proveedoras de acceso a Internet[256] (TIGO, CLARO, MOVISTAR, etc.)

Cada vez que se tiene acceso a internet, se asigna al usuario un número de identificación único a nivel mundial, denominado dirección IP, los proveedores de servicios de internet poseen un gran rango de números de identificación disponibles, que son asignados a los usuarios durante las diversas sesiones de acceso." La dirección IP asignada al usuario es guardada también en las bitácoras de los servidores del proveedor y es capturada por la mayoría de los programas de telecomunicación informática, tales como programas o aplicaciones Web de correo electrónico servidores de internet navegadores. De lo antes expuesto podemos deducir que al enviarse y recibirse los mensajes de datos, la dirección IP del emisor puede ser extraída de estos mensajes.[257]

Existen proveedores de servicios de internet, que asignan direcciones IP fijas a sus usuarios. Es común que estos casos sean los de servicios de televisión por acceso combinados de televisión por cable. El servicio de acceso a internet por banda ancha (ADSL), por sus características técnicas, hace posible que un mismo usuario emplee o detecte una sola dirección IP, por días o meses, lo que hace posible una identificación rápida de los usuarios. Las direcciones IP en estos casos pueden variar en un mismo día.[258]

---

[256] Paraf. Josefina Quevedo González, "Investigación y prueba del ciberdelito", 173.
[257] Ligia Maribel García Juárez, "La investigación de delitos emergentes en internet, su detección y control" (Guatemala, Universidad Rafael Landivar, 2014), 46.
[258] Ibid.

4.3.2.2. Mensajes de Datos

Un mensaje de datos es toda información inteligible en formato electrónico similar que pueda ser almacenada o intercambiada por cualquier medio. La característica principal del mensaje de datos es la posibilidad de intercambio de información. Dentro de este concepto amplio entrarían las páginas web, toda vez que el propietario, administrador y muchas veces los usuarios de páginas web, pueden publicar información subiéndola al servidor web, una vez que se encuentra la información en el servidor y que por ende la misma es pública, terceros pueden acceder a ella, con lo que se configuraría el intercambio.[259] Según QUEVEDO un principio básico en la jurisprudencia Española es que "no se precisa autorización judicial para conseguir lo que es público" [260] por lo que en este tipo de casos es posible que un investigador de la policía se encuentre monitoreando ciertas páginas a fin de verificar la activad de las mismas y sus contenidos para prevenir o detectar la realización de hechos delictivos.

4.3.2.3. El Correo Electrónico

El correo electrónico es uno de los medios de comunicación usual hoy día, y los concretos mensajes a través del mismo son genuinos actos de comunicación. Cuando un mensaje se envía es transmitido por el proveedor de servicios del remitente al proveedor de servicios del destinatario, quien una vez recibido lo almacena en su buzón hasta su apertura. El destinatario tiene acceso al mensaje y determina cuánto tiempo permanecerá en el buzón. Los mensajes del buzón están por consiguiente bajo el control tanto del destinatario como del proveedor y generalmente las autoridades encargadas

[259] Ibid.
[260] Quevedo González, "Investigación y prueba del ciberdelito". 173.

de aplicar la ley podrían tener acceso ejerciendo medidas coercitivas[261] contra cualquiera de ellos. Normalmente preferirán ejercerlas contra el proveedor de servicios de internet, dado que de ese modo no alertarían al destinatario sobre la existencia de la investigación.[262]

Desde un punto de vista técnico cabe diferenciar dos partes en un correo electrónico: el cuerpo y las cabeceras. El cuerpo está formado por el contenido del mensaje en sí (incluyendo posibles adjuntos, previamente tratados por el programa de correo para poderse transmitir), y por tanto depende por completo de lo que el usuario haya decidido incluir en dicho mensaje. Mientras que las cabeceras contienen información tanto facilitada de una u otra forma por el usuario (asunto, destinatario, emisor...) como añadida por el servidor o servidores por los que pasa el mensaje hasta llegar a su destino.[263]

Los mensajes de datos vía correo también pueden ser generados por programas que se activan desde los navegadores web, tales como el Explorer, Chrome, Firefox y otros. En la actualidad diversos sitios web permiten que se generen mensajes de datos tipo correo electrónico, se envíe a otra cuenta de este mismo tipo que posteriormente puede ser visto por otro usuario en un mismo computador.

En España el tema de la investigación policial a los correos electrónicos ha generado mucho debate, pero con ciertas reformas hechas a la Ley de

---

[261] En este caso en concreto no es posible utilizar la ley especial para la intervención de las telecomunicaciones en vista que de conformidad con el Art. 5 de la misma los Ciberdelitos sujetos a la LECDIC no se encuentran previstos para la utilización de dicha ley especial, salvo que existieran delitos conexos entre los previstos en esta última y la LECDIC por así habilitarlo el supuesto del número 16 del Art. 5 de la ley especial para la intervención de las telecomunicaciones.
[262] Ibid. 214.
[263] Ibid. 215.

Enjuiciamiento Criminal se ha equiparado éste a la intervención telefónica y telemática otorgándole las mismas garantías procesales. A estos efectos debe aplicarse el mismo régimen a las diversas modalidades de mensajería instantánea (instant messaging) cuyo uso generalizado ha colocado a este medio en pieza esencial en las comunicaciones interpersonales (ej: WhatsApp Telegram, o Messenger).

El acceso a un correo electrónico que aún no ha sido leído por su receptor, con independencia del momento concreto del proceso de comunicación en que se encuentre (ya esté escrito y almacenado en la computadora personal, o en el terminal telefónico pendiente de ser enviado a su destinatario final, o enviado y recibido pero aún no leído), supone sin duda una injerencia en el secreto de las comunicaciones, de ahí es donde se recalca que al realizar investigaciones policiales sobre este tipo de tecnología es necesario contar con autorización judicial pues es una injerencia a la intimidad del investigado.
El principal problema radica en que gran cantidad de ISP tienen su sede en el extranjero, principalmente en EEUU, y sobre todo en que los datos que poseen se encuentran ubicados en servidores informáticos fuera del territorio español, para cuya consecución es prácticamente obligado solicitarlos mediante la oportuna comisión rogatoria internacional, lo que generalmente ralentiza, si no inutiliza, la investigación.[264]

El envío de un mensaje de correo electrónico por técnicas universalmente aceptadas implica la captura de la dirección IP del usuario que lo envía, la hora en que se realiza el envío, y la hora en que el mensaje pasa por los agentes de transferencia de los mensajes de datos, estos últimos juegan un papel fundamental probatorio, por cuanto van agregando datos de horas de envío y

[264] Quevedo González, “Investigación y prueba del ciberdelito”, 216–217.

recepción a las llamadas cabeceras de los mensajes de datos, que se pueden comparar imaginaria y analógicamente con los sellos que van colocando las oficinas de correo postal a los sobres que procesan.[265] Con esto los investigadores de la policía pueden seguir un rastro para verificar y constatar la autoría de quien realizó el correo electrónico o el mensaje instantáneo que ha realizado la conducta prevista para un ciberdelito.

Pruebas de origen de destino, identidades del emisor y receptor, existencia de una cuenta de correo determinada, para establecer si una cuenta de correo existe o si la misma ha sido falsificada o inventada, se dispone de la posibilidad de dirigirse al administrador servidor o de la empresa encargada del mismo a efectos de que se suministren los datos del usuario; si no se tiene acceso directo a ella, se pueden realizar pruebas de experticia o de experimentos, en los cuales se pueden enviar mensajes de prueba y establecer el comportamiento del sistema para determinar si son retornados o no para demostrar la actividad o vigencia de una cuenta de correo determinada, lo que se puede indicar o se indica de la posibilidad de emisión de un mensaje de datos.[266]

El hecho de que un mensaje de prueba rebote de una cuenta no significa que la cuenta no ha existido, las cuentas de correo electrónico pueden ser creadas y borradas por los administradores de los servidores de correo, es por ello que pueden obtener pruebas dentro del servidor como ejecutor de este tipo de comandos. También puede haber indiciarias que indiquen la existencia de direcciones de correo determinadas y la relación con sus presuntos autores.

---

[265] Ligia Maribel García Juárez, “La investigación de delitos emergentes en internet, su detección y control”, 47.
[266] Ibid. 48.

La configuración del programa de correo hace que cuando se configura un programa para el uso de una cuenta de correo, se coloque el nombre de usuario lo cual constituirá un indicio de la titularidad de la cuenta. El nombre de usuario de la cuenta puede ser también otro indicio de hecho, al igual que la coincidencia de iniciales o de sílabas que formen parte del nombre y apellido de una persona, o bien la combinación de números. En un caso donde no se impugne o desconozca un mensaje de datos debe tenerse como acepta la existencia de la cuenta del emisor.

Cuando se investiga una cuenta de correo relacionada presuntamente con un dominio o nombre web tipo www.dominio.com, pueden realizarse estudios periciales a efectos de establecer si efectivamente ese dominio está apuntando a un servidor con servicios de correo activos. La tecnología permite que exista nombres de dominio activos que apunten o dirijan el navegador a un servidor sin que necesariamente se tenga activado el servicio de correo en el mismo. Esto es posible gracias a que los propietarios de dominio pueden utilizar servicios de re direccionamiento, que hacen por ejemplo que cualquier correo electrónico enviado a una dirección propia y determinada se reenvíe automáticamente a otra cuenta de correo, funcionando de modo similar a un servicio telefónico de transferencia de llamadas.[267]

Existe gran cantidad de variables desde el punto de vista técnico que deben ser verificados por expertos o peritos a efectos de que se establezca el origen o procedencia de los mensajes de datos, su emisor y destinatario.

[267] García Juárez, “La investigación de delitos emergentes en internet, su detección y control”. 49.

4.3.2.4 El Chat o Conversaciones en Línea

La mensajería instantánea (instant messaging) difiere del correo electrónico ya que las conversaciones son en tiempo real (Skype, Line, Telegram…). Las comunicaciones mediante el tráfico de voz sobre IP (VoIP), se trata de una conversación entre dos interlocutores, cada uno de ellos desde su teléfono, sin que estemos en absoluto ante una "comunicación telefónica". El ejemplo paradigmático es el "WhatsApp" que es una aplicación de mensajería multiplataforma de gran arraigo que permite enviar y recibir mensajes y efectuar llamadas VoIP. Esta aplicación utiliza el plan de datos de los teléfonos móviles para su funcionamiento e intercambio de información.[268]

La información que se envía a través de este servicio se almacena en los servidores de WhastsApp, que están localizados en el Estado de California (EEUU), circunstancia de la cual los usuarios son advertidos de que su uso lleva implícito la aceptación de la política de privacidad y las condiciones del servicio, que están bajo las leyes del Estado de California y que toda la información que se trasmita mediante el servicio de WhatsApp es transferida a los EEUU, y por tanto muestran su consentimiento a que sean amparadas bajo las leyes de del Estado de California.[269] No obstante, también se les notifica que su información está cifrada de extremo a extremo lo cual significa que está garantizada que no habrá injerencia de terceros que intenten interceptar las comunicaciones.

Cuando se utiliza WhatsApps los servidores del mismo registran automáticamente, la siguiente información:

---

[268] Paraf. Quevedo González, "Investigación y prueba del ciberdelito", 222.
[269] Ibid.

- La petición web.
- La dirección IP.
- La versión del sistema operativo (Android, Apple iOS)
- El idioma utilizado.
- El tipo de plataforma desde el que se accede al servicio.
- Nombre de dominio del que se accede al servicio.
- El número de mensajes.
- Fecha y hora de cada mensaje.
- Número de teléfono origen del mensaje.
- Número de teléfono destino del mensaje.

WhatsApp no registra nombres, direcciones de correo u otra información de contacto de las listas de los dispositivos, ni el contenido de los mensajes. Tampoco registra los datos de localización de los dispositivos, a menos que los usuarios quieran compartir voluntariamente su localización con otros usuarios utilizando el servicio de WhatsApp.[270]

Desde que se ha activado el cifrado E2EE (end-to-end), que se conoce como un "protocolo severo", sólo el emisor y el receptor pueden leer los mensajes, no pueden acceder a ellos ni siquiera los proveedores de telecomunicaciones, los proveedores de internet o los dueños de la aplicación. Esto quiere decir que la compañía no tiene ninguna capacidad para acceder a los mensajes de sus clientes, ni siquiera por orden de las autoridades. WhatsApp no mantiene los registros de los mensajes en sus servidores una vez han sido enviados y recibidos. Lo mismo sucede con las llamadas de WhatsApp, cualquier llamada realizada con la aplicación, incluyendo si es al extranjero, está cifrada de extremo a extremo para que ningún tercero pueda escucharla y no puedan ser

[270] Ibid. 223.

intervenidas de ninguna manera, ya que ni la aplicación, ni el servidor ni el proveedor de datos conoce la clave de cifrado, que es creada por el propio dispositivo.[271]

Por ello, ante el uso de estas nuevas técnicas de encriptación, será necesario acudir a otras sofisticadas medidas de investigación tecnológica, como pudiera ser el registro remoto de equipos informáticos, para acceder al contenido forma remota mediante la introducción de un malware en el equipo a intervenir, sin que sea necesario así solicitar la colaboración del ISP.[272]

4.3.2.5. Redes Sociales

La investigación multidisciplinar ha mostrado que las redes sociales operan en muchos niveles, desde las relaciones de parentesco hasta las relaciones de organizaciones a nivel estatal (se habla en este caso de redes políticas), desempeñando un papel crítico en la determinación de la agenda política y el grado en el cual los individuos o las organizaciones alcanzan sus objetivos o reciben influencias. El análisis de redes sociales estudia esta estructura social aplicando la teoría de grafos e identificando las entidades como nodos o vértices, y las relaciones como enlaces o aristas. La estructura del grafo resultante es a menudo muy compleja. En su forma más simple, una red social es un mapa de todos los lazos relevantes entre nodos; se habla en este caso de redes socio céntricas o completas.[273]

También la doctrina se suele referir a las redes sociales como las plataformas en Internet, las cuales tienen como fin o propósito hacer de la comunicación y

---

[271] Ibid. 224
[272] Ibid.
[273] http://www.slideshare.net/mariaelenasotojara/las-redes-sociales-son-estructuras-sociales-compuestas-de-grupos-de-personas consultada el 28 de abril de 2021.

temas sociales algo más fácil y accesible para la comunidad cibernética, para que la misma se mantenga informada o pueda fácilmente emitir opinión sobre temas de la realidad nacional o internacional.

Conviene destacar que las empresas dedicadas a mantener las páginas web de las redes sociales, en cuanto a la introducción de contenidos en internet de sus usuarios no pueden controlar (pues técnicamente solo son intermediarios de la circulación de información) lo que cada una de las personas sube a la red, y sería exacerbado imponerles una vigilancia sobre esto; pero se les ha exigido un carácter de custodia pasiva, de modo que responderán penalmente, en su caso, no por no haber detectado en sus páginas la existencia de contenidos ilícitos, sino si una vez hecho, notificado, ordenado o sabido, éstos no los retiran (comisión por omisión), además de en los supuestos en que ellos sean los propios creadores directos o cooperadores necesarios en la difusión del contenido ilícito o asuman el papel de moderadores o gestores responsables, por ejemplo de foros de debate.[274]

4.3.2.6 Registro remoto sobre equipos informáticos

En la investigación de los ciberdelitos, una de las diligencias más plausibles la constituye la posibilidad de acceder a un equipo informático mediante el registro remoto del mismo. Esta diligencia consiste en la utilización de programas que permiten de forma remota y telemática el examen a distancia del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o bases de datos. Obviamente, toda esta operación tiene lugar sin conocimiento de su

[274] Josefina Quevedo González, “Investigación y prueba del ciberdelito”, 225.

titular o usuario, accediendo a la información del dispositivo electrónico que se controla a distancia mediante el empleo de un malware o virus informático.[275]

Tradicionalmente el registro se realizaba in situ, pero en la actualidad la implantación de los denominados “programas espía”, ya sean “registros de teclado” (Keyloggers), programas troyanos, o cualquier otro software o hardware que permita la apertura de una “puerta trasera” (backdoor), facilita el acceso de forma remota. A través de estos procedimientos se toma el control del dispositivo anfitrión, posibilitando el descubrimiento y captura de cualquier información alojada físicamente en él o, en su caso, virtualmente (en la nube) con ocasión de su acceso al repositorio correspondiente, o incluso la propia intervención de sus comunicaciones.[276]

La técnica electrónica en estudio servirá para conocer la información que el investigado almacene o transcurra por el sistema informático de manera continuada durante un tiempo determinado, por lo que suponen una afectación de elevada intensidad en los derechos a la intimidad, al secreto de las comunicaciones y, en general, al propio entorno virtual de la persona investigada, por lo cual se considera que es necesario que sea controlada por un juez o mejor dicho que la misma sea autorizada por un Juez que autorice la misma, así como la información a controlar y la duración de esta diligencia de investigación.

Instalado el correspondiente programa espía con orden judicial, o conseguido el acceso por claves, las posibilidades para la policía son infinitas, ya que no

---

[275] “El registro remoto de equipos informáticos” en http://www.internautas.org/html/8833.html consultado el 28 de abril de 2021.
[276] Quevedo González. *Investigación y prueba del ciberdelito.* 264.

solo se puede acceder a la información que se almacena en el disco duro sino a toda la información obrante en el mismo.[277]

4.3.2.7. El agente encubierto informático

Es el agente de autoridad que conoce o tiene noticias de la existencia de una actividad delictiva y se infiltra entre quienes la llevan a cabo en busca de información y pruebas que permitan impedir o sancionar el delito. Agente encubierto sería entonces el policía especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la ley y bajo el control del juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos son manifiestamente insuficientes para su descubrimiento y permite recabar información sobre su estructura y *modus operandi,* así como obtener pruebas sobre la ejecución de hechos delictivos[278]

En la actualidad los grandes avances y descubrimientos tecnológicos han aportado al ámbito de la investigación criminal nuevas técnicas para la averiguación de los delitos y la identificación de las personas que participan en los mismos. El agente informático es una modalidad de agente encubierto, pero, al contrario del carácter presencial de este último, se llevará a cabo a través de canales cerrados de la comunicación. Tanto en la figura del agente encubierto como en la del agente encubierto informático se exige que la introducción en la organización criminal tenga un carácter totalmente voluntario, es decir, el funcionario que se infiltre a través de internet para la investigación de hechos delictivos, deberá proceder a ello por deseo propio,

[277] Ibid. 265.
[278] Flavio Cardoso Pereira, *El agente encubierto. Desde el punto de vista del garantismo procesal penal* (San Salvador, El Salvador: Cuscatlan, 2018), 216–17.

sin que en ningún caso se le pueda obligar a ello. Cabría pensar que, como no es necesario que se infiltre físicamente no corre cierto peligro. No obstante, estará tratando con criminales, por lo tanto, siempre habrá un cierto grado de peligrosidad.[279]

Luego de obtenerse una autorización judicial que permita que el investigador de la policía se infiltre con nombre supuesto en la organización criminal, éste deberá aportar a la mayor brevedad posible toda información que vaya obteniendo para que pueda aportarse a la investigación correspondiente en su integridad. Son muy grandes las posibilidades que esta técnica ofrece para el esclarecimiento de los hechos ilícitos que se cometen a través de la red y para la determinación de sus autores y poder luchar contra la delincuencia a través de internet, en supuestos como podrían ser la captación, e incluso las comunicaciones entre terroristas, las estafas informáticas masivas concertadas por grupo organizado (phishing), la distribución grupal de pornografía infantil, o cualesquiera otros delitos vehiculizados a través de las nuevas tecnologías[280].

4.3.2.8.Identificación de IMEI, IMSI y MAC.

En este apartado hay que resaltar la diferencia que hace QUEVEDO en cuanto a los conceptos anteriores, pues con el término IMSI se hace referencia a un código de identificación único para cada línea de telefonía móvil integrada en la tarjeta SIM (Subscriber Identy Module) que permite la identificación del abonado a través de las redes GSM y UMTS. Por su parte, el término IMEI es un código pregrabado en los teléfonos móviles que identifica al aparato

[279]https://riull.ull.es/xmlui/bitstream/handle/915/16410/El%20agente%20encubierto%20informatico.%20Especial%20atencion%20al%20agente%20encubierto%20informatico..pdf?sequence=1 consultado el 28 de abril de 2021.
[280] Quevedo González. *Investigación y prueba del ciberdelito.* 272-273.

unívocamente a nivel mundial y se trasmite por el móvil a la red de telefonía al conectarse a ésta. Es el equivalente al número mac, cuando nos referimos a móviles, pues identifica ese número de serie al equipo. Finalmente el término MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red, también conocida como dirección física y es única para cada dispositivo. Las direcciones Mac son únicas a nivel mundial y constituyen una huella digital que permite determinar desde qué dispositivo de red se ha emitido un determinado paquete de datos.[281]

Tanto el MAC, el IMEI y el IMSI carecen de capacidad de información sobre la identidad del usuario, teniendo valor únicamente si se asocia a otros datos en poder de las operadoras. La captación de tales números a efecto de investigación penal es posible mediante un escaneado o barrido realizado a través de instrumentos electrónicos que detectan aquellos siempre que se actúe en un determinado radio de acción en el que se encuentra el terminal. Su captación se realiza como consecuencia de un seguimiento dirigido específicamente frente a un individuo o individuos determinados. Con posterioridad a la captación, una vez obtenido el correspondiente código identificativo, es necesaria la obtención del número comercial del teléfono, en posesión de la prestadora del servicio de telecomunicación. Ni el MAC, ni el IMSI, ni el IMEI por sí solos, son datos integrables en el concepto de comunicación.[282]

Este tipo de técnica es utilizada como herramienta electrónica para rastrear el espectro radioeléctrico forzando a los dispositivos cercanos a generar un diálogo automático con la herramienta a través de la que facilitan a ésta las

[281] Ibíd. 176 – 177.
[282] Ibíd. 177.

asignaciones numéricas que se corresponden con los números IMEI o IMSI, para luego solicitar a las operadoras de telefonía los datos personales de sus propietarios.[283]

4.3.2.9. Otros programas que son utilizados para la investigación

Un analista forense digital durante el desarrollo de una investigación puede auxiliarse de una serie de programas que le permitan recabar información y datos indispensables para el esclarecimiento de los autores o el origen de un determinado ciberdelito; según el analista de seguridad informática y forense salvadoreño, Ronald González, pueden utilizarse los siguientes programas:

Tinfoleak: Es una de las aplicaciones más completas creadas para recopilar todo tipo de información sobre usuarios de Twitter, ya que permite:

- Mostrar toda la información relacionada con un usuario, como su nombre, fotografía, localización, seguidores, etc.
- Recopila los dispositivos y el sistema operativo que utiliza dicho usuario.
- Muestra otras aplicaciones y redes sociales utilizadas por el usuario.
- Geolocaliza a un usuario a partir de sus fotos, incluso muestra los tweets en Google Earth
- Descarga todas las fotos de un usuario de Twitter.
- Muestra todos los hashtags utilizados y las menciones.[284]

Trape: Es una herramienta de reconocimiento que permite rastrear a las personas y hacer ataques de phishing en tiempo real, la información que se puedes obtener es muy detallada. Se quiere enseñar al mundo a través de

[283] Ver glosario al final de esta investigación para comprender el significado de las siglas utilizadas.
[284] Ronald González, “Ciber Crimen” (PDF, San Salvador, El Salvador, 2020). 9.

esto, cómo las grandes compañías de Internet pueden monitorear a cada uno, obteniendo información más allá de la dirección IP, como la conexión de las sesiones a sitios web o servicios en Internet.[285] Con esto puede determinarse como tanto los Hackers pueden investigar a cualquier persona alrededor del mundo para seleccionar a sus eventuales víctimas de ciberdelitos; así también es una herramienta que puede ser utilizada por un analista informático durante una investigación.

Maltego: Es un servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc. Por ejemplo, a la hora de buscar establecer contacto con una empresa, esta herramienta puede proporcionar datos muy útiles como direcciones de correo electrónico como puede ser de recursos humanos, departamento de ventas, soporte técnico, número telefónico, lo que nos facilitaría el contacto con esta empresa o persona; también posee la capacidad de encontrar distintos tipos de artículos como son autos, motos, aviones, entre otros[286]

4.4. ACTOS DE INVESTIGACION

La ley regula una serie de diligencias que es imprescindible llevar a cabo para la buena marcha de la investigación y del juicio oral, para aportar al proceso una serie de objetos inanimados que sirvan para atestiguar la realidad de un hecho, todo ello como piezas de convicción.[287]

---

[285] González. 10.
[286] González. 11.
[287] Víctor M. Moreno Catena y Valentín Cortés Domínguez, *Derecho procesal penal*, 3. ed, Manuales (Valencia: Tirant lo Blanch, 2008).

Se realizan los actos de investigación con la finalidad de identificar, obtener o asegurar las fuentes de información que permiten eleborar una explicación sobre la forma en que ocurrió el hecho investigado y cuál es su probable autor, se enmarcan en una serie de actuaciones o diligencias que realiza directamente la Fiscalía General de la Republica o que esta encomienda a la Policía Nacional Civil a través de la respectiva dirección funcional (Art. 74 y 75 CPP)

Cualquier acto procesal practicado que tenga como contenido la recaudación de información, no puede ser considerado como prueba, sino meros actos de investigación, tal cual es la naturaleza jurídica de las diligencias iniciales de investigación y los actos de la instrucción, a los cuales el legislador estableció que carecerían de valor en juicio, salvo que se convirtieran en actos de prueba, tal cual lo establece el Art. 311 inc. 2 CPP.

La Sala de lo Constitucional de la Corte Suprema de Justicia ha definido en diversas resoluciones lo que puede entenderse como diligencias iniciales de investigación, indicando, que éstas son aquellos actos realizados por la Policía con Dirección Funcional de la Fiscalía con el objeto de recolectar elementos de convicción que permitan sustentar una imputación, a efecto de que la Fiscalía pueda promover la acción penal a través del respectivo requerimiento, agregando que por su naturaleza y finalidad, las mismas no requieren para su práctica, la presencia de un defensor ni la notificación al sospechoso (Sentencia número SHC 211-2002 de fecha 5 de marzo de 2003)[288]

[288] Carlos Ernesto Sánchez Escobar, Marco Tulio Díaz Castillo, y Sergio Luis Rivera Márquez, *Reflexiones sobre el nuevo proceso penal*, 1. ed (San Salvador, El Salv: Consejo Nacional de la Judicatura, 2009). 87.

Como lo establece ACURIO DEL PINO hay que seguir ciertos principios de actuación en la investigación de los ciberdelitos, principalmente en los actos iniciales de investigación ya que esto asegurará la evidencia que luego será objeto de pruebas periciales u otras diligencias que se orden en la instrucción, dichos principios son los siguientes :

1. El funcionario de la Fiscalía o de la Policía nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios. Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones.[289]
2. Ninguna acción debe tomarse por parte de la Policía, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.[290]
3. En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos. [291]
4. Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue

[289] Paraf. Acurio del Pino, Manual de manejo de evidencias
[290] Ibid.
[291] Ibid.

recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.[292]

5. El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.[293]

4.4.1. Actos Urgentes de Comprobación

Siguiendo a HENRÍQUEZ GONZALEZ resulta conveniente que el capítulo II del título V, Libro I del Código Procesal Penal Vigente -cuyo epígrafe se denomina "actos urgentes de comprobación"- incorpora una multiplicidad de normas que regulan el procedimiento a seguir durante la práctica de actos cuya naturaleza está esencialmente orientada a construir una hipótesis inicial del hecho ocurrido, por eso se observa que los actos urgentes de comprobación, no aluden a los denominados actos de prueba, sino que , más bien, se refieren específicamente a los actos urgentes de investigación, puesto que con ellos lo que se pretende es recabar todos los elementos necesarios para fundamentar la acusación y, finalmente, preparar el juicio – momento procesal oportuno donde se practicará la "verdadera prueba" [294]

---

[292] Ibid.
[293] Ibid.
[294] Irma Joana Henríquez González, "Los actos Urgentes de investigación y el anticipo de prueba en el nuevo código procesal penal", en *Ensayos doctrinarios sobre el nuevo proceso penal salvadoreño*, 1° Edición (San Salvador, El Salvador: Sección de Publicaciones CSJ, 2011), 215–44.

En este caso en concreto piénsese en una computadora que se encuentra apagada o sujeta a una clave de acceso será necesario solicitar al Juez de Paz competente que autorice un Registro con orden judicial de dicho aparato (Art, 191 CPP) y a la vez en el supuesto de la obtención y resguardo de información electrónica (Art. 201 CPP), salvo el caso contemplado en el Art. 281 CPP que prescribe que con el solo consentimiento de la víctima se puede ordenar por parte del Fiscal Auxiliar la grabación de las comunicaciones electromagnética o de cualquier otro medio, entendiéndose cualquier aparato o dispositivo basado en las TIC`s.

4.4.2. Proceso de cadena de custodia de la evidencia digital

Se puede señalar que la cadena de custodia es la documentación de cada paso de las evidencias, desde su inicio, quién la recolecta, quién la entrega, quién la recibe, quién o quienes realizan los análisis o experticias. La cadena de custodia es el documento escrito en donde quedan reflejadas todas las incidencias de una prueba, en dicho documento se reflejan los movimientos y acciones ejercidas sobre el elemento físico de la prueba[295]

También se puede afirmar, que la cadena de custodia, es el procedimiento destinado a garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias recolectadas de acuerdo a su naturaleza e incorporados en el curso de una investigación de un hecho punible, destinado a garantizar su autenticidad para los efectos del proceso a partir de su identificación, recolección, embalaje, rotulación, transporte y peritación hasta

[295] Rommell Ismael Sandoval Rosales, *Código Procesal Penal Comentado* (San Salvador, El Salvador: Consejo Nacional de la Judicatura, 2018). 993.

su presentación en juicio, con el fin de evitar alteraciones, sustituciones, contaminaciones o destrucciones.[296]

La evidencia digital, es un insumo de especial cuidado, para el proceso de investigación de delitos informáticos, que debe ser tratada por parte de los especialistas, realizando todas las medidas de precaución necesarias para no contaminarla y que sea objeto de desestimación[297] ante un proceso penal, por haberse corrompido o alterado la fuente de prueba que se pretendía resguardar.

Es importante clarificar los conceptos y describir la terminología adecuada que señale el rol que tiene un sistema informático dentro del *iter criminis* o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener un caso[298] que ha sido investigado, por tanto el rol que cumpla el sistema informático determinará donde debe ser ubicada y como debe ser usada la evidencia[299]

Ahora bien para el propósito expuesto en el párrafo anterior se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este

---

[296] Sandoval Rosales. 994.
[297] Oscar Carlos Ernesto Aguirre Linares, “Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en El Salvador” (San Salvador, El Salvador, Universidad Don Bosco de El Salvador, 2020). 9.
[298] Acurio del Pino, Óp. Cit.
[299] Ibid.

contexto 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[300], sobre esto remito al lector a lo dicho en el apartado 2.1 de esta investigación.

El proceso a seguir con la evidencia digital es el siguiente:

Primer paso: Se debe asegurar la integridad de la evidencia original, es decir, que no se deben realizar modificaciones ni alteraciones sobre dicha evidencia.

Segundo paso: Si se comprueba que el sistema está comprometido, es decir, ha sido atacado, se encuentra infectado o no se puede accesar a el, se requiere establecer la prioridad entre las alternativas de:

1) Levantar la operación del sistema. Suele ser restablecer el sistema a su estado normal, pero se debe considerar que esta actitud podría resultar en que se pierdan casi todas las evidencias que aún se encuentren en la “escena del delito” e incluso puede resultar en el impedimento de llevar a cabo las acciones legales pertinentes.

2) Investigación forense detallada. Al seleccionar esta alternativa el profesional debe iniciar con el proceso de recopilar las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

[300] Ibid.

Tercer paso: Hay que asegurarse de llevar un registro de cada uno de los pasos realizados y características o información de los hallazgos encontrados, es recomendable que durante el desarrollo de este proceso, lo asista u acompañe una persona, preferentemente imparcial. Durante esta fase, es recomendable utilizar una técnica o metodología de recolección de evidencias, para ello, el profesional debe hacer uso de prácticas o metodologías que sean reconocidas y que sobre todo puedan ser reproducidas o replicadas, bajo el mismo contexto del escenario presente.

Cuarto paso: De iniciarse un proceso contra los atacantes del sistema, será necesario documentar en forma precisa y clara como se ha preservado la evidencia tras su recopilación a lo largo de todo el proceso de pasos anteriores. Se recomienda la obtención de copias exactas de la evidencia obtenida utilizando mecanismos de comprobación de integridad de cada copia, las cuales deben ser documentadas y agregadas en el etiquetamiento realizado.

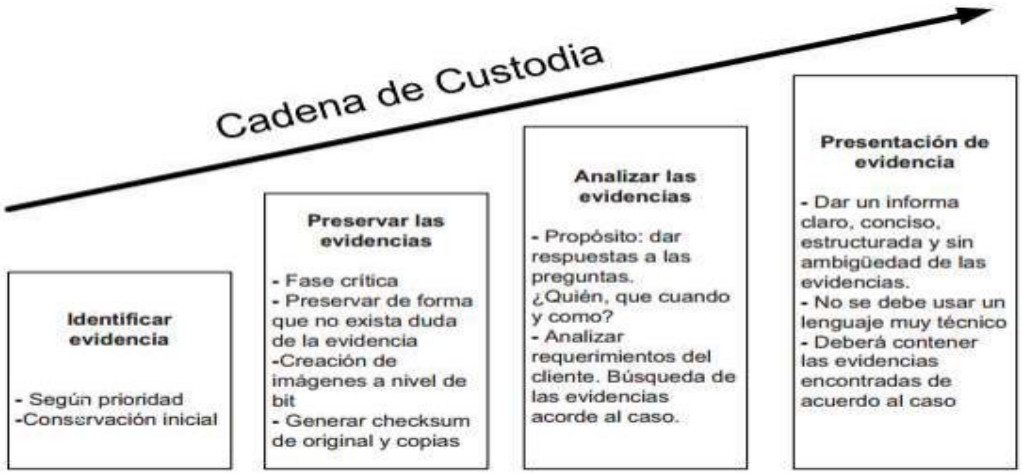

Fig. 2: Proceso de la cadena de custodia[301]

[301] Parraf. Oscar Carlos Ernesto Aguirre Linares. 12.

La cadena de custodia es – como se ha dicho- la garantía del justiciable que los objetos o documentos que se incorporen en la vista pública para probar los hechos que se le acusan, son los mismos que fueron incautados en algún momento procesal y que de haberse modificado o cambiado es por razones legales o técnicas.

Es importante destacar, que en virtud que técnicamente, los equipos informáticos y dispositivos de almacenamiento de información, están en su mayoría diseñados para registrar -en la llamada metadata de los archivos que contienen- la información o datos informáticos, es factible a través de pericias determinar cuándo ocurrió el último acceso o modificación de los mismos; ello conlleva a que un perito puede determinar esa información y con ello permitir el cotejo con el día y hora en que la incautación ocurrió, expresado en las actas correspondientes levantadas por las mismas autoridades policiales o fiscales y con ello evidenciar que estando esos equipos o dispositivos en manos de ellas, sucedió un acceso ilegal a tal información y con ello, cuando menos configurar un cuestionamiento a la legalidad de la prueba[302] Es por ello tener presente lo preceptuado en los Arts. 251 y 252 del CPP a fin de mantener prístina la fuente de prueba y evitar su impugnación.

También deben seguirse las recomendaciones de ACURIO DEL PINO sobre qué hacer al encontrar un dispositivo informático o electrónico, que son los siguientes:

[302] Víctor Manuel Rodríguez Luna, “Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos” (Secretaria de Naciones Unidas y Fiscalía General de la Republica, 2018). 115.

i)No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

ii) Asegure el lugar y los equipos de cualquier tipo de intervención física o electrónica hecha por extraños.

iii) Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección.

iv) Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.

v) Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.

vi) Si está encendido, no lo apague inmediatamente (para evitar la pérdida de información “volátil”)[303]

En caso que no haya un técnico de la unidad técnica y científica de la policía o del laboratorio de la misma deberán seguir estos pasos:

-No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.

-Si está encendido, no lo apague inmediatamente.

[303] Acurio del Pino, Óp. Cit.

-Si tiene un “Mouse”, muévalo cada minuto para no permitir que la pantalla se cierre o se bloqueé.

-Si una Computadora Portátil (Laptop) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberar la batería del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.

-Si el aparato está conectado a una red, anote los números de conexión, (números IP).

-Fotografíe la pantalla, las conexiones y cables.

-Usar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

-Coloque etiquetas en los cables para facilitar reconexión posteriormente.

-Anote la información de los menús y los archivos activos (sin utilizar el teclado) Cualquier movimiento del teclado puede borrar información importante.

-Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel.

-Bloqueé toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.

-Selle cada entrada o puerto de información con cinta de evidencia.

-De igual manera deben selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.

-Desconecte la fuente de poder y quite las baterías y almacénela de forma separada el equipo (si funciona a base de baterías o es una computadora portátil)

-Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético.

-Al llevar aparatos, anote todo número de identificación, mantenga siempre la CADENA DE CUSTODIA.

-Lleve todo cable, accesorio, conexión-

-Lleve, si es posible, manuales, documentación, anotaciones

-Se debe tener en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto

desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).[304]

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos. Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD). No se debe perder de vista que existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.[305]

4.5.Prueba de los ciberdelitos

El Derecho Procesal no ha tenido más remedio que volverse permeable al avance técnico y ceder a su empuje, abriendo a la información sus contenidos.[306] Todo esto hace que en un futuro próximo el nuevo procedimiento probatorio sea mucho más ágil, con un claro objetivo: acortar el tiempo[307] superar las barreras del espacio a la hora de practicar algunas pruebas, con el fin de conseguir estar en otros lugares distintos de la sala de vistas mediante el uso de los sistemas de videoconferencia o del correo electrónico. Las nuevas tecnologías suponen un importante cambio en el

---

[304] Ibid.
[305] Ibid.
[306] Federico Bueno de Mata, *Prueba electrónica y proceso 2.0: especial referencia al proceso civil*, Abogacia practica 63 (Valencia: Tirant lo Blanch, 2014), 89. Citando a *ESTEBAN CASTILLO, E., "La fe pública judicial ante las nuevas tecnologías", Revista jurídica de la Comunidad de Madrid, n° 6, enero-febrero 2000, páq. 4.*
[307] Bueno de Mata, *Prueba electrónica y proceso 2.0*, 2014. 89 *cita a "…idea expresada por ORTEGA Y GASSET, J., en su célebre conferencia pronunciada en1932, en la Universidad Menéndez y Pelayo de Santander, El hombre y la técnica.*

sector judicial con el que se otorga celeridad a una multitud de actos procesales y se produce una supresión de distancias; acotando las dos grandes coordenadas que limitan el actuar humano: el tiempo y el espacio; y todo ello afecta de forma directa a la fase capital de todo proceso: la fase probatoria.[308]

La importancia de la fase probatoria en el proceso se infiere a través de múltiples referentes, la cual revela hasta qué punto sin pruebas no habría proceso, o hasta qué punto el proceso sólo se justifica por qué existe algo que probar. Dentro de las diferentes fases en las que se divide un proceso, hay que destacar la importancia capital que posee el período probatorio, pues es la fase en la que el juez toma un contacto personal con el material fáctico.[309]No se debe de perder de vista que la prueba constituye un elemento capital en la estructura de todo proceso, al no tener normalmente un carácter contingente sino necesario, de ahí que la atención que se le tiene que prestar a la información de la fase probatoria debería ser superlativa por parte de todos los operadores jurídicos y del propio legislador.[310]

La prueba siempre ha sido considerada por la doctrina clásica como el factor decisivo del proceso judicial radica en la ella[311], y es que el material aportado debe adaptarse a los cambios de la sociedad con el fin de seguir desempeñando ese papel insustituible de cara a fundamentar la defensa de

---

[308] Bueno de Mata, 89. Cita a *DE URBANO CASTRILLO, E. y MAGRO SERVET, V., La prueba tecnológica en la Ley de Enjuiciamiento Civil, Madrid, 2003, pág. 21*

[309] Bueno de Mata, 90. Cita a CALVO SANCHEZ, M. C., "La prueba: disposiciones generales. Análisis de los artículos 281 a 298 de la Ley de Enjuiciamiento Civil 1/2000, Responsa lurisperitorum Digesta Vol. III.págs. 129-140.

[310] Federico Bueno de Mata, *Prueba electrónica y proceso 2.0: especial referencia al proceso civil*, Abogacia practica 63 (Valencia: Tirant lo Blanch, 2014). 90.

[311] Bueno de Mata. 90 *citando a* SIMPSON, J., the problema of trial, Nueva York 1949, pags 141 y ss.

las partes en un determinado de litigio. En razón de lo anterior, y al llegar a este punto, independientemente de la influencia tecnológica, se puede ver como la prueba posee una esencia tradicional y convencional; con unos valores estándar que vienen recogidos ya por la doctrina de siglos pasados, y que permanecerán inalterables con el paso del tiempo autónomamente de los nuevos medios tecnológicos probatorios.[312]

En sentido amplio prueba es lo que confirma o desvirtúa una hipótesis o una afirmación precedente, en virtud de esta definición, es posible considerar que en el proceso penal salvadoreño, todos los documentos que se adjuntan al requerimiento fiscal (art. 294 CPP.) y al dictamen en cualquier sentido (art. 356 CPP.), tienen por objeto sostener las afirmaciones sobre los hechos realizadas en estos documentos por los fiscales[313] con lo que se denota que con la prueba se pretende determinar el binomio procesal de realización del hecho delictivo e imputación del mismo a uno o más sujetos, por eso la prueba se vuelve el medio más confiable para descubrir la verdad real de los hechos sometidos al juicio.

4.5.1. Prueba electrónica

Existen multitud es de autores clásicos que brindan conceptos de prueba, su significado y su finalidad, tales como: Devis Echandía, Sentís Melendo, Bentham, Carnelutti, Calamandrei, Calvo Sánchez, etc. debate sobre este tema, la inclusión de nuevas técnicas y medios de prueba es arduo que bien daría para varias investigaciones documentales. Por todo, ello se ve que la

[312] Bueno de Mata. 91
[313] Víctor Manuel Rodríguez Luna, “Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos”.

doctrina procesal se muestra acorde en que “la prueba” se trata de un concepto multívoco, que designa a diversas significaciones de acuerdo con la finalidad que se le atribuye en el proceso: demostración material de los hechos según ocurrieron o el establecimiento formal de los mismos para la resolución del litigio.[314]

El avance tecnológico cala de tal forma en la fase probatoria que modula el concepto material que tenemos de prueba creando un nuevo concepto, *“la prueba electrónica”* ; un concepto difuso y sin una regulación específica que hace que se esté en presencia con una laguna jurídica que plantea un desafío y un reto investigador de gran importancia y actualidad[315].

Para PICÓ I JUNOY, la prueba electrónica posee una característica adicional en materia probatoria: puede ser objeto y medio de prueba. Esta será objeto de prueba cuando se trate de probar un hecho electrónico, cómo puede ser constatar el envío de un mensaje vía Smartphone; o también puede ser un medio de prueba cuando se deba probar electrónicamente un hecho, como cuando se reconoce haber pagado algo y dar constancia de ello a través de un recibo electrónico. Pero, como bien señala el mismo autor, también puede darse el caso de que sea medio y objeto de prueba a la vez, esa situación se dará cuando se tenga que probar electrónicamente un hecho electrónico, Por ejemplo, comprobar la compra de un dominio web a través de una factura electrónica.[316]

---

[314] Bueno de Mata, *Prueba electrónica y proceso 2.0*, 2014. 92
[315] Bueno de Mata. 94
[316] Bueno de Mata. 94 *citando a ABEL LLUCH, X., "Prueba electrónica", La prueba electrónica, Libro de la Colección de Formación Continua Facultad de Derecho ESADE, Barcelona, 2011, págs. 61-64.*

Al llegar, uno de los primeros problemas que se encuentra es la ambigüedad del concepto de “prueba electrónica”, lo que da pie en la doctrina a la utilización de otras equivalentes, como prueba por medios tecnológicos, por soportes informáticos, por medios audiovisuales, etc. A ello se une otro factor que es el hecho de la carencia de una definición legal de la misma, dado que el litigante enfrenta un concepto abierto y dinámico; igualmente, destaca la parquedad en su regulación legal en las leyes procesales generales, unida a una manifiesta dispersión en su legislación específica.[317]

SANCHIS CRESPO[318] define la prueba en soporte electrónico, o prueba electrónica, como aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, o bien al fijar este hecho como cierto atendiendo a una norma legal[319].

La distinción entre ambos conceptos de fuente y medio de prueba es analizada por MONTERO AROCA[320]", quien señala que la fuente de prueba designa una realidad extrajurídica preexistente e independiente del proceso, que representa lo sustantivo, lo material, y el medio de prueba es un concepto procesal, referido a la actividad necesaria para introducir dicha realidad en el proceso; la regulación procesal no afecta a las fuentes de prueba, pues es la realidad social la que las manifiesta, mientras que a las leyes procesales sólo

---

[317] Ortuño Navalón, *La Prueba Electrónica Ante los Tribunales*. 34.
[318] Ortuño Navalón, *La prueba electrónica ante los tribunales*. *citando a SANCHIS CRESPO, CAROLINA. La Prueba en soporte electrónico. en la obra colectiva las tecnologías de la información y la comunicación en la administración de Justicia. Gamero casado, EDUARDO Y VALERO TORRIJOS, JULIÁN (coord.). Aranzadi, 2012, pág. 713.*
[319] Ortuño Navalón. 34
[320] Ortuño Navalón. *Citando A Montero Aroca, Juan. La prueba en el proceso civil. 52 edic. Ed. Civitas, Madrid, 2007, pág. 150. Y este mismo autor, en Derecho Jurisdiccional, Proceso civil, Tomo II, Valencia 2001, págs. 262-265.*

corresponde regular el modo por el cual tales fuentes de prueba acceden al proceso. Al distinguir entre las fuentes de prueba que - serían las palabras, datos, cifras, operaciones matemáticas, imágenes, sonidos-y los medios de prueba-serían los soportes o instrumentos de archivo, conocimiento o reproducción de datos (CD, DVD, CD-rom, pendrive,...) donde se recogen y almacenan tales fuentes; y la práctica de la prueba consiste en la reproducción ante el Tribunal de tales datos[321].

De otro lado, la prueba electrónica puede constituir tanto el objeto de la prueba (v.gr: acreditar la remisión de un e-mail), como ser un medio de prueba (V.gr: la prueba de una determinada conducta a través de su reconocimiento en un correo electrónico), o simultáneamente un objeto y un medio de prueba (v.gr: la acreditación electrónica de un hecho de esta naturaleza, como puede ser la remisión de un virus)[322].

Todo lo dicho sirve para determinar que luego de realizar diversas operaciones técnicas de parte de la policía técnica y científica, para la obtención de las fuentes de prueba estas deben ser ubicadas dentro de un medio de prueba de los regulados en la legislación adjetiva para ser llevados ante el órgano jurisdiccional y servir para ser valorado para que el juez pueda realizar o no una imputación de la conducta delictiva al o los responsables de haber realizado un ciberdelito, tomando como prueba los resultados y evidencias que valorados sobre las reglas de la sana critica den lugar a formar la conclusión del caso a través de una sentencia.

[321] Ortuño Navalón. 35
[322] Ortuño Navalón. 35

Lo dicho en el párrafo anterior se ve muy fácil, pero en una realidad como la salvadoreña, es necesario retomar experiencias internacionales como las de España, documentadas tanto por Ortuño Navalón como Quevedo González[323] que hacen énfasis en que antes de las reformas de la Ley de enjuiciamiento criminal de dicho país del año 2015 que introdujeron especificas técnicas de investigación tecnológica, debían utilizar la jurisprudencia de los máximos tribunales de justicia y la regulación de la Ley de Enjuiciamiento Civil para llenar los vacíos existentes en esos temas.

En cierta medida se considera que El Salvador se encuentra en la actualidad con una situación muy parecida a la Española de antes del 2015, con la diferencia que de forma abierta el Art. 186 CPP permite la realización de operaciones técnicas y científicas electrónicas y demás disponibles por la ciencia y la técnica policial, con lo cual las técnicas estudiadas en este capítulo pueden ser utilizadas, solo verificando que si las mismas requerirán una invasión o eventual lesión a derechos fundamentales deberá contarse con la respectiva autorización judicial, que determinará los alcances, el contenido y la duración de la misma como un acto urgente de comprobación.

En la LECDIC como norma penal especial solo se regulan las conductas constitutivas de ciberdelitos, pero no se establecen aspectos procesales los cuales deben ser tratados de conformidad con lo prescrito en el CPP, pero siendo este insuficiente en cuanto a la regulación de los Art. 186 y 201 de dicho cuerpo legal, para poder establecer medios de prueba para llevar las fuentes de prueba en las que se haya utilizado técnicas modernas de investigación de

[323] Ver los trabajos de Ortuño Navalón, *La Prueba Electrónica Ante los Tribunales*; Josefina Quevedo González, “Investigación y prueba del ciberdelito”.

parte de la policía, se puede utilizar lo prescrito en el Art. 396 y 397 del Código Procesal Civil y Mercantil como medios de prueba útiles para el proceso penal.

No obstante lo antes dicho, no se debe de olvidar que en la investigación de los ciberdelitos es posible la realización de peritajes y para ello sin lugar a dudas se aplicarán los Arts. 226 y siguientes del CPP a fin de que obteniendo fuentes de prueba con las operaciones técnicas realizadas por la policía las mismas sean analizadas por un experto de la policía técnica y científica para demostrar su autenticidad y puedan ser presentadas para iniciar un proceso o durante el desarrollo del mismo.

Aunque parezca de poca monta, es necesario aclarar que este tipo de técnicas novedosas de investigación de los ciberdelitos pueden realizarse tanto en un caso de investigación administrativa, el cual es precedido por una denuncia, aviso o querella de realización de un ciberdelito como en casos donde pueda encontrarse al o los autores en flagrante delito y por la premura de presentación del respectivo requerimiento se hagan unas diligencias como acto de comprobación y las otras bajo la respectiva vigilancia y control del juez de instrucción.

4.5.2. Prueba Pericial

La cual puede ser definida como aquel medio de prueba por medio del cual personas ajenas a las partes, que poseen conocimientos especiales en alguna ciencia, arte o profesión, y que han sido previamente designadas en un proceso determinado, perciben, verifican hechos, los ponen en conocimiento del juez y dan su opinión fundada sobre la interpretación y apreciación de los mismos, a fin de formar la convicción del magistrado, siempre que para ello se

requieran esos conocimientos.[324] En este caso se trata de una prueba que emplea los conocimientos en abstracto de personas extrañas a las partes y que no tienen ningún interés en las resultas del proceso pero que entran en contacto con éste a raíz de un requerimiento del juez para dictaminar sobre ciertas fuentes de prueba y su relación con los hechos objeto del juicio, siendo su opinión sobre hechos pasados, presentes e incluso su relación con los futuros.

Lo dicho anteriormente encaja perfectamente con lo regulado en el Art. 226 CPP, siendo entendido que existen dos clases de peritos los **permanentes y los accidentales**, estos últimos son los propuestos en específico por los litigantes cuando no existen laborando para ninguna institución del Estado especialistas en una determinada ciencia o arte o existiéndolo se pretende impugnar o ampliar el dictamen hecho por un perito permanente, por lo.cual están sujetos a acreditar su especialidad, deben ser juramentados y sus honorarios son pagados por la parte que lo propuso; contrario sensu el perito permanente está exento de juramentación o protesta previa a realizar la práctica de la pericia y por laborar para el Estado sus honorarios serán los designados en la institución donde labora y contaran con los respectivos permisos para realizar esta actividad.

Para el caso de esta investigación un medio de prueba idóneo, pertinente y útil sería un especialista en sistemas informáticos y de ciberseguridad, es decir, un perito especializado en el área de las tecnologías de la información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis. Así puede influir para su selección la

[324] Jorge L. Kielmanovich, *Teoría de la prueba y medios probatorios*, Cuarta edición, ampliada y actualizada (Buenos Aires: Rubinzal-Culzoni Editores, 2010). 565.

plataforma tecnológica el lenguaje de programación usado, el sistema de base de datos, sistema operacional, entre otros, entonces, el perito informático debe emitir un criterio u opinión, la cual, debe estar fuertemente sustentada tanto en la parte técnica como científica, que logre llegar a conclusiones objetivas e imparciales sobre un hecho, y no solo basarse en impresiones u opiniones.[325]

También el perito debe cumplir una serie de deberes: Asumir el cargo, cuando la designación no es hecha libremente por la parte; de comparecer ante el Juez, cuando existe esa formalidad; de posesionarse y prestar el juramento; de practicar personalmente las operaciones necesarias para su dictamen, bajo el control del Juez y en la forma como la Ley Procesal determine; de obrar y conceptuar con lealtad, imparcialidad y buena fe; de fomentar su dictamen y de rendirlo en forma clara y precisa; de guardar el secreto profesional, cuando el caso lo requiera.[326]

El perito informático debe poseer un perfil definitivamente técnico, siendo de vital importancia que el perito esté familiarizado con las técnicas de análisis y recuperación de datos. Como elemento adicional, el perito debe contar con amplios conocimientos legales que le permitan desarrollar su tarea sin que la misma sea descalificada o impugnada durante su presentación judicial. Las tareas a desarrollar por el perito informático no son distintas de la de otros peritos judiciales. Por lo tanto deberá recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha

[325] Oscar Carlos Ernesto Aguirre Linares, "Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en El Salvador". 27.
[326] Hernando Devis Echandia, *Teoría General de la Prueba Judicial, Tomo II*, Quinta Edición (Buenos Aires, Argentina: Victor P. de Zavalia, 1981). 368.

requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada.[327]

Como se puede apreciar en esta investigación el flagelo de la Ciberdelincuencia es un problema mundial que va en aumento y cada vez los hechos delictivos son más graves, poniendo en peligro incluso la seguridad nacional de los Estados y la buena marcha de las empresas, estando el delincuente en un determinado lugar o país distinto de donde se han producido los resultados de los hechos ilícitos lo que hace necesario que los peritos que se designen para investigar este tipo de casos sepan cómo realizar valoraciones, dictámenes y peritaciones informáticas con el fin de colaborar en la resolución de procesos por medio de la extracción de la evidencia digital y presentarlas ante el Juez. Estos profesionales deben actualizar sus conocimientos para resolver problemas que surgen en su quehacer profesional y tomar decisiones tácticas y estratégicas en sus puestos.

Es vital que ante una pericia o experticia práctica se tengan claro los siguientes aspectos: La ductibilidad y la interpretación.

-La ductibilidad: El perito de cualquier especialidad se apoya en la ductibilidad, a efectos de determinar bajo un criterio lógico, las distintas alternativas posibles que hay para llegar a un mismo resultado es importante mencionar que la ductibilidad no es sinónimo de sentido común o criterio, permite tener una visión global y detallada de los distintos problemas a resolver para llegar a un resultado, a diferencia del criterio común para que haya ductibilidad el perito debe contar con profundos conocimientos en la materia a ser estudiada.

---

[327] Aguirre Linares, op. Cit. 30

-La interpretación: El perito se apoya en la interpretación para explicar el o los distintos métodos que pudieron haber sido utilizados para llegar a un resultado, vale decir que en medida de la profundidad de conocimiento del perito se descartan los distintos métodos posibles.[328]

El perito debe estar al tanto, sobre cuál es su ámbito de acción, y para ello debe conocer las fases de un proceso pericial. La autoridad competente ordenará que se realicen las experticias que correspondan dentro de un proceso, el mismo que puede haber sido solicitado por una de las partes intervinientes, para la investigación de un determinado delito, especificando la necesidad de la experticia, la cual deberá seguir las siguientes fases:

Fase de designación de perito: Esta deviene luego de que una de las partes o ambas han solicitado el Juez de la causa que se realice la pericia, para lo cual se busca un perito permanente en la división de la policía técnica y científica o de la Unidad de delitos informáticos de la PNC para que realice el análisis forense digital se define como un conjunto de técnicas de recopilación y exhaustivo peritaje de datos, la cual sin modificación alguna podría ser utilizada para responder en algún tipo de incidente en un marco legal (Ley Especial de Delitos Informáticos y Conexos).[329] El caso que generará problemas se referirá cuando por lo general del Defensor particular o el querellante trate de nombrar un perito accidental para la investigación de un ciberdelito, ya que uno de los principales retos que tiene El Salvador consiste en determinar la calidad habilitante que se exige al perito para la investigación

[328] Ibíd. 38.
[329] González, op. Cit. 12

de estos casos que prescribe el Art. 227 CPP, pero de esto se hablará en el próximo capitulo.

Fase de Posesión de la calidad de perito: En esta etapa es primordial que el perito no tenga ningún motivo de inhabilidad o excusa, en lo que se refiere al proceso, otro aspecto valioso a considerar, es que el perito designado, debe conocer y saber diferenciar en la diligencia cuando se establecen periodos de tiempo para la entrega de su informe pericial, es decir la contabilizan o no de los días no laborables.

Fase de investigación: En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente, aparentemente de los regulados en la LECDIC.

Sí el aparato con tecnología basado en las TIC´s está encendido se hace lo siguiente:

+Extraer la memoria RAM, se puede analizar programas en ejecución y sus PID, buscar los encabezados y comprobar si son maliciosos; conexiones sospechosas establecidas; usuario y contraseña de usuario logueado.

+Crear imagen forense bit a bit de disco duro.

+Si es laptop desconectar el cargador y extraer la batería sin apagar de forma tradicional

Sí el aparato con tecnología basado en las TIC´s está apagado se hace lo siguiente:

-Se extrae el disco duro o la memoria del dispositivo

-Se crea una imagen forense bit a bit del disco duro o memoria

En esta misma fase el Perito debe realizar su estudio, aplicando las técnicas y herramientas necesarias para determinar lo solicitado por el Fiscal, Defensor, Querellante o Juez de la causa, en la providencia de designación, en cuyo caso, generalmente se aplican técnicas de informática forense, o auditoria informática, entro otras, que el perito considere necesarias. Durante esta fase se recomienda que las técnicas utilizadas deban ser sustentadas de manera técnica y científica, además de la aplicación de guías o metodologías, por parte del profesional designado.[330]

Fase de análisis: Finalmente, una vez obtenida la información y preservada, se pasa a la parte más compleja. Sin duda, es la fase más técnica, donde se utilizan tanto hardware como software específicamente diseñados para el análisis forense.[331]

Fase de presentación de informes y resultados: En este proceso el perito debe remitir dentro del plazo o término estipulado por el juez según el Art. 233 CPP, los hallazgos encontrados durante su investigación, con sus respectivas conclusiones, las cuales se presentarán en un Dictamen el cual puede ser necesario que el experto deba exponer durante el desarrollo de la vista pública.

La Figura siguiente resume la forma de elaboración de un dictamen pericial:

---

[330] Parraf. Aguirre Linares, óp. Cit. 40.
[331] González, óp. Cit. 21.

Fig. 3: Elaboración de un dictamen pericial[332]

[332] Tomada de Aguirre Linares, óp. Cit. 42.

CAPITULO V: LIMITACIONES DEL SISTEMA PENAL SALVADOREÑO PARA INVESTIGAR Y PROBAR LA COMISIÓN DEL CIBERDELITO

SUMARIO: 5.1. Panorama general de la realidad. 5.2. Limitaciones en cuanto a la Legislación. 5.2.1. Falta de suscripción y ratificación del Convenio de Budapest sobre la Ciberdelincuencia. 5.2.2. Falta de suscripción y ratificación de otros acuerdos internacionales para la investigación de ciberdelitos ya sean multilaterales o bilaterales. 5.2.3. Falta de una normativa procesal penal relativa a la evidencia digital, resguardo de información, y prueba electrónica. 5.3. Limitaciones de la PNC. 5.4. Limitaciones de la FGR. 5.5 Limitaciones en la CSJ.

RESUMEN

En el presente capitulo se abordan desde un panorama general las distintas limitaciones que han sido encontradas en el sistema penal salvadoreño, en cada una de las instituciones que se vinculan para la aplicación de la LECDIC, lo cual incide en la investigación y posterior prueba de la realización de los ciberdelitos.

5.1. PANORAMA GENERAL DE LA REALIDAD

El creciente desarrollo de las computadoras y las modernas Tecnologías de la Información y la Comunicación, así como el aumento de las capacidades de almacenamiento y procesamiento de datos, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, ejemplifican el desarrollo actual de lo que se conoce como la “era de la información”.

El uso de las nuevas tecnologías digitales se ha generalizado, pues brindan a los usuarios la libertad para poderse mover y permanecer comunicados (o conectados) con miles de servicios construidos sobre redes. Brinda la posibilidad de participar de los entornos en línea; de enseñar y aprender, de jugar y trabajar. A medida que las sociedades dependen cada vez más de estas tecnologías, es necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados, como los delitos informáticos, ya que las tecnologías de la sociedad de la información pueden utilizarse, -y de hecho se utilizan-, para perpetrar y facilitar diversas actividades delictivas.

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario del mundo, siendo difícil individualizar a los sujetos activos cuando estos hechos ilícitos son realizados de forma transnacional sino se cuenta con los respectivos tratados o convenios internacionales de cooperación. A la vez es necesario tener una reacción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática, por lo cual los Estados Nacionales deben considerar que no se pueden mantener al margen o aislados de esta realidad y deben buscar formas de cooperar en esta aldea global que se está formando en la sociedad del siglo XXI.

El Salvador, no puede ser la excepción a lo antes dicho, pero debe reconocerse que existe una gran brecha digital entre la población salvadoreña en sí y de esta en general con las de otros países incluso dentro de la misma Latinoamérica solo para hacer referencia a una región a la que se pertenece; en el país a penas el Gobierno de la Republica está distribuyendo computadoras a cada niño, niña o adolescente para que puedan realizar sus estudios y disminuir la brecha a la que se ha hecho referencia; pero en las

instituciones encargadas por velar por la aplicación de las Leyes la realidad es distinta, muchas veces las computadoras han venido solo a sustituir la conocida “máquina de escribir” y son un instrumento que facilita el trabajo, pero no han sido vistas como herramientas por las cuales puede cometerse hechos delictivos o que son o pueden ser objeto de ataque.

Debe entenderse por "sistema penal" al control social punitivo institucionalizado, que en la práctica abarca desde que se detecta o supone que se detecta una sospecha de delito hasta que se impone y ejecuta una pena, presuponiendo una actividad normativizadora que genera la ley que institucionaliza el procedimiento, la actuación de los funcionarios y señala los pasos y condiciones para actuar. Esta es la general idea de "sistema penal" en un sentido limitado, se puede decir que abarca la actividad del legislador, del Ministerio Público, de la policía, de los jueces y magistrados.

A continuación se expondrán las limitantes que existen en sistema penal de El Salvador para luchar contra la ciberdelincuencia.

5.2. LIMITACIONES EN CUANTO A LA LEGISLACIÓN

Como se ha dicho a lo largo de esta investigación en El Salvador existen ciertas limitaciones para luchar contra el flagelo de las conductas determinadas como ciberdelitos; dichas limitantes hacen que el país tenga una ley especial contra los ciberdelitos que desde su vigencia ha parecido más un Derecho penal simbólico que un verdadero cuerpo normativo vigente para la lucha contra la ciberdelincuencia, siendo en este caso responsabilidad del Legislador nacional que no ha determinado su necesidad para la buena aplicación de la ley. Las limitaciones que pueden apreciarse, en el sentido antes dicho, son las siguientes:

5.2.1. Falta de suscripción y ratificación del Convenio de Budapest sobre la Ciberdelincuencia

El 23 de noviembre de 2001, en la ciudad de Budapest se crea y se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración, entrando en vigor a partir del 1 de julio de 2004[333]. El objetivo del Convenio es establecer una legislación penal y de procedimientos comunes entre los miembros y demás suscriptores del mismo, para la persecución de delitos cometidos a través de medios electrónicos e informáticos; y a su vez, fortalecer la cooperación internacional, teniendo en cuenta el carácter de la información que se maneja en la red para cometer delitos y de que las pruebas relativas a éstos sean almacenadas y transmitidas por medio de dichas redes. También el establecimiento de medidas procesales o cautelares adaptadas al medio digital, que faciliten la detección, investigación y la obtención de pruebas de infracciones contra o un mediante sistemas informáticos o cuyas fuentes de prueba se hallen en soporte electrónico.[334]

La adhesión al tratado, según establece su artículo 37, se encuentra abierta a la incorporación de países que no sean miembros del Consejo de Europa. A la fecha, el Convenido de Budapest ha sido rarificado por 60 Estados, junto a los Estados miembros de Unión Europea; el Convenio ha sido ratificado por países no europeos, entre ellos Estados Unidos, Canadá, Australia, Japón,

---

[333] Dicho convenio esta abierto para que cualquier Estado solicite adherirse al mismo a través de invitación del Comité de Ministros del Consejo de Europa previa consulta a los Estados contratantes del Convenio, así lo dispone el mismo en su Art. 37 punto 1.

[334] Morón Lerma, Esther, *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, 2°, s/f. 170.

Israel, República Dominicana, Chile, Argentina, Colombia. Otras organizaciones también se han adherido a él, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT).

En cuanto a su estructura, el Convenio de Budapest se divide en cuatro capítulos y un preámbulo, el cual se enfoca en los objetivos del Convenio, y la necesidad de armonizar a nivel internacional la persecución contra el cibercrimen. Los capítulos se encuentran desarrollados de la siguiente manera:

Capítulo I, titulado *"Terminología"*, contiene solo un artículo, el cual introduce algunas definiciones a efectos de comprender los conceptos utilizados en el cuerpo del Convenio.

Capítulo II, titulado *"Medidas que deben adoptarse a nivel nacional"*, compuesto de 3 secciones, referidas a Derecho Penal, Derecho Procesal y Jurisdicción respectivamente, en las cuales se incorporan las medidas que se deberán adoptar por cada Estado, para la entrada en vigencia del Convenio; considerando particularmente la obtención, conservación y presentación de datos informáticos dentro del procedimiento, y sus normas de jurisdicción.

Capítulo III, titulado *"Cooperación internacional"*, el que incluye normas especiales respecto el procedimiento de extradición, la asistencia mutua, la utilización y restricción de uso a la información obtenida; medidas provisionales, asistencia entre órganos de investigación, la creación de una red 24/7, entre otras.

Capítulo IV, titulado *"Cláusulas finales"*, contiene las formalidades para la firma, entrada en vigor, adhesión, reservas, solución de controversias y la denuncia del tratado, entre otros.[335]

En cuanto a la inclusión de tipos penales, el Convenio establece cuatro categorías, así:

- Delitos contra la confidencialidad y la disponibilidad de los datos y sistemas informáticos.
- Delitos propiamente informáticos.
- Delitos relacionados con el contenido del mismo.
- Delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.[336]

En materia procesal, el Convenio regula normas que corresponden tanto a los órganos investigadores como a los tribunales; a partir del artículo catorce se dan las normas relativas al establecimiento de parámetros de obtención y tenencia de pruebas que constan en las redes y sistemas, defendiendo los derechos fundamentales de las personas.

La evidencia digital es susceptible a ser destruida y/o alterada, por tanto, la conservación de los datos es vital para asegurar o demostrar el por qué de una investigación. Por tal motivo el Convenio se ocupa de establecer diferentes métodos para asegurar la autenticidad e integridad de la evidencia digital, de manera que pueda ser sujeto de incorporación para su investigación; esto

---

[335]Repositorio Universidad de Chile http://repositorio.uchile.cl/bitstream/handle/2250/176344/Herramientas-del-convenio-de-Budapest-sobre-ciberdelincuencia-y-su-adecuacion-a-la-legislacion-nacional.pdf?sequence=1&isAllowed=y consultado el :28 de abril de 2021

[336]Estos artículos se encuentran desarrollados entre los art. Dos y diez del convenio.

debe ser verificada, comprobando que los datos no hayan sido alterados mediante la denominada "*cadena de custodia"* [337], es decir, que cada uno de los custodios que vigilan la prueba debe asegurar que no la haya modificado y que al contrario- la protegió ante la posibilidad de una alteración.

Uno de los pilares del Convenio es la coordinación internacional para efectos de conseguir la persecución eficaz de los delitos informáticos que en muchas ocasiones traspasan las fronteras de jurisdicción nacional. Actualmente existe una multiplicidad de Convenios de asistencia mutua en materia penal, tanto de carácter bilateral como multilateral[338], en los que establece el concepto de autoridad central como institución clave en la tramitación efectiva de solicitudes en esta materia. Así, la idea es que el Estado requirente y el Estado requerido de la solicitud se comuniquen a través de una autoridad especializada determinada por cada Estado, que no obedezca a la coyuntura diplomática y permita mayor celeridad que la vía judicial que procedería en términos generales.

Lo dicho en el párrafo anterior es una de las principales limitantes en cuanto a legislación que tiene El Salvador, ya que no basta con tener la LECDIC para combatir las conductas constitutivas de ciberdelitos, sino que es necesario contar con cooperación internacional para lograr esclarecer estos hechos, que es de conocimiento general que pueden iniciar su ejecución en un país y el resultado suceder en otro país, para lo cual el criterio de territorialidad en la aplicación de la ley penal se vuelve insuficiente para proteger a los la población, nacional e internacional, contra este tipo de delincuencia.

---

[337] Art. 250 y siguientes CPP de El Salvador.
[338] Tales como la Convención Europea de Asistencia Mutua en Materia Penal, suscrita en Estrasburgo, el 20 de abril de 1959 y complementada por sus protocolos adicionales.

A pesar de la importancia que reviste este convenio, en los planes del actual gobierno no se encuentra su suscripción y posterior ratificación por el país, lo cual puede apreciarse en el expediente SAI 109-2020(1) de la Oficina de Acceso a la Información Pública del Ministerio de Relaciones Exteriores en la cual se puntualiza que El Salvador no ha sido suscriptor y no se encuentra en planes de formar parte del convenio de Budapest del 23-XI-2001.[339] Con esto El Salvador tiene una limitante para la lucha contra la ciberdelincuencia ya que con la LECDIC solo puede investigar, acreditar y procesar las conductas ilícitas realizadas dentro del territorio nacional y pero no cuenta con la protección y cooperación que cobija a los países que han ratificado este convenio, lo cual se comprueba de la sola lectura del Art. 2 de la LECDIC que desarrolla el principio de ubicuidad, que ya estaba regulado en el Art. 12 del Código Penal.

Entre los deberes que debe realizar el país una vez adherido al convenio, se destacan por un lado, la designación de un punto de contacto para la red 24×7 (según define el artículo 35 del convenio) con el fin de proveer apoyo y cooperación de forma rápida y efectiva, es decir, que si El Salvador suscribiera y luego ratificara este Convenio entraría a un selecto grupo de países que están comprometidos con la lucha contra la ciberdelincuencia lo que permitiría tener información de primera mano para ubicar en que país del mundo se encuentra el sujeto activo de un ciberdelito y donde se encuentra disgregada la prueba del mismo, ya que la evidencia digital puede estar dispersa en diferentes países del mundo.

Otro beneficio es que al formar parte del Convenio se realiza un proceso de adecuación de normativa interna al convenio de Budapest, como lo han hecho

[339] Ver anexo 1.b de esta investigación

diversos estados miembros lo que implica es una unificación de la legislación a nivel mundial que facilitará la adecuación típica de las conductas independientemente de donde se haya cometido el ciberdelito; así también se unificarán normas procesales para el tratamiento de las evidencias y el resguardo de la misma. La evidencia digital es volátil e intangible, es decir, puede desaparecer o ser alterada muy rápido, por lo que las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas. Para esto, se requiere un proceso penal ágil y eficiente, con esfuerzo organizado por parte de los países que tienen vigente el Convenio de Budapest.

Finalmente, aunque no menos importante es el beneficio de la cooperación internacional que permitirán investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o ciberdelitos, pues se podrá realizar localización de sospechosos, recolección o envío de evidencia digital y la posibilidad de la extradición de los eventuales imputados por la realización de ilícitos.

5.2.2. Falta de suscripción y ratificación de otros acuerdos internacionales para la investigación de ciberdelitos ya sean multilaterales o bilaterales.

Como se indicó en el apartado anterior en el expediente SAI 109-2020(1) de la Oficina de Acceso a la Información Pública del Ministerio de Relaciones Exteriores también fue informado que el país no tiene suscritos ni ratificados convenios, tratados o acuerdos internacionales sobre ciberdelincuencia o delitos informáticos, ya sea multilaterales o bilaterales. Lo que determina a que El Salvador, con relación a otros países del mundo, se encuentra aislado de la cooperación internacional procesal para poder intercambiar información

que ayude a dar con los autores de una determinada conducta calificada como ciberdelito que haya producido sus efectos en el país o que haya sido iniciada en él pero sus resultados hayan sido sufridos en otro país.

Como parte de estas dos limitantes en cuanto a la legislación, se debe poner acento en que la criminología sostiene que tanto el factor espacio como el tiempo constituyen elementos de riesgo que el delincuente tendrá en cuenta al momento de cometer la acción ilícita; pero en los delitos informáticos estos dos factores se ven altamente disminuidos.[340] Así como la denominada "aldea global" ha eliminado la frontera que divide a las distintas naciones, la cibercriminalidad se ha adaptado a este fenómeno, pero esto no ha pasado con las normas penales internas de cada país ni en lo que se ha dado en llamar derecho penal internacional, por ello es importante que el Estado relaje un poco su principio de soberanía y participe de esta comunidad internacional, siendo importante que suscriba y luego ratifique el Convenido de Budapest como un primer paso y que realice acuerdos bilaterales o multilaterales con otras naciones para intercambiar información y cooperar en las investigaciones de estos ilícitos.

5.2.3. Falta de una normativa procesal penal relativa a la evidencia digital, resguardo de información, y prueba electrónica.

Como ha sido puesto de manifiesto por FEUSIER la vigente ley que castiga al cibercriminalidad encuentra como sus principales obstáculos aquellos de carácter procedimental u operativo, en la ejecución y cumplimiento de la investigación de estos delitos, dificultades que ya habían sido detectadas por

[340] Palazzi, *Delitos informáticos*, 71.

organizaciones internacionales desde hace varios años.[341] Estas dificultades señaladas van orientadas al poco presupuesto destinado para combatir la ciberdelicuencia y la falta de soporte de los servicios de Internet prestados por los proveedores de los mismos, quienes no tienen en la LECDIC ninguna responsabilidad de resguardar información de usuarios sospechosos de haber cometido algún hecho ilícito en la red; así también el Gobierno de la Republica no mantiene relaciones de cooperación con compañías establecidas fuera del país que proveen servicios de Internet relevantes, tales como el e - mail, redes sociales o dominios de sitios web.[342]

Lo dicho en el párrafo anterior es muy importante ya que de la simple lectura de la LECDIC se puede apreciar que la misma no obliga a las empresas servidoras de Internet a nivel nacional resguardar la información o datos de las IP´s de todas las personas que se van conectando en el servicio web de los servidores lo cual dificulta el trabajo investigativo de la PNC y de la FGR para poder obtener evidencia digital de la realización de hechos delictivos a través de la web o que tengan por objetivo utilizarla como medio para afectar un sistema informático.

Sin la evidencia digital o con poca posibilidad de obtenerla, es muy difícil que un perito de la Unidad de delitos informáticos de la PNC pueda tener los insumos necesarios para realizar una pericia sobre datos que se encuentren en un servidor de una empresa proveedora de servicios de internet a nivel nacional esto es importante, ya que se debe recordar, como lo hace FEUSIER

[341]Oswaldo Ernesto Feusier Ayala. Aplicación y contenido de la Ley Especial contra la delincuencia informática y conexos. (San Salvador, El Salvador: Consejo Nacional de la Judicatura, 2018). 6

[342] Paraf. OEA. Tendencias de seguridad cibernética en América Latina y El Caribe. (Washington: OEA, 2014)

citando a Flores Prada que una de las principales dificultades de la cibercriminalidad, es la dificultad para identificar al autor del hecho, que fácilmente se esconde en el anonimato y opacidad que ofrecen las redes informáticas, complejas, e intervenidas por múltiples operadores privados.[343]

Como puede analizarse sin esta cooperación establecida como obligatoria en la ley no hubiera podido ser esclarecido y recuperado parte del rescate del caso “DarkSide” de este año al que se hizo referencia en el capítulo IV de esta investigación, ya que los proveedores de servicios de Internet pueden colaborar con las autoridades para la obtención de elementos tales como: a) La dirección IP asignada al sospechoso por el proveedor y sus datos contractuales, b) La localización de la conexión a través del proveedor, c) El teléfono origen y destino de las comunicaciones del sospechoso, d) La copia de ficheros que disponga el sospechoso en su espacio web, e) El tipo de servicio telefónico empleado por el sospechoso, entre otros elementos que permitirán coadyuvar en la investigación delictiva de los ciberdelitos, pero si no se realiza una reforma en la legislación el perito de la PNC solo podrá trabajar, para obtener evidencia digital, sobre las memorias de los aparatos que se fundamenten en las TIC´s que sean incautados o secuestrados en operativos realizados de forma física.

Así mismo hay una falta de regulación de lo relativo a la evidencia digital y la prueba electrónica, ya que el CPP solo se refiere a ella dentro de los actos urgentes de comprobación, en las operaciones técnicas por parte de la PNC (Art. 186) la obtención y resguardo[344] de información electrónica (Art. 201); en

[343] Feusier. Óp. Cit. 68.
[344] En este caso se refiere al resguardo en un espacio físico para los aparatos basados en las TIC´S que poseen la información o su grabación o imagen informática en un disco duro externo

las diligencias iniciales de investigación, el Fiscal puede ordenar con el consentimiento de la víctima la grabación por cualquier medio electrónico de las comunicaciones telefónicas, radiotelefónicas o que utilicen el espectro electromagnético (Art. 281) y fuera de dichos artículos el legislador guardo silencio en cuanto a técnicas o medios de prueba que pudieran facilitar la labor de investigación, tanto en la etapa administrativa como en la instrucción.

Lo dicho en el párrafo anterior toma mayor realce si se piensa que dentro de la historia de los proyectos de ley, antes de la vigencia de la LECDIC, se contó con una opinión del Fiscal General en Funciones Licenciado José Ovidio Portillo Campos hecha en el año 2012 en la que existía un apartado titulado ***"Consideraciones acerca de la problemática probatoria"*** dentro de la cual se destacaba la necesidad que la investigación de los ciberdelitos lleve aparejado un desarrollo en las habilidades tecnológicas investigativas de las agencias de investigación, la cual textualmente decía:

"…Concretando la opinión al respecto, finalmente todo se traduce a la necesidad de dotar a la División Técnica Científica de la Policía Nacional Civil, del suficiente y capacitado recurso humano técnico que pueda identificar mediante la informática, los elementos necesarios para el sustento técnico de los casos, puesto que la tipificación por sí sola, carecería de eficacia jurídica…"[345]

Por dicha opinión la comisión que estudiaba la necesidad de una ley especial contra los ciberdelitos, en el mes de octubre del 2012, decidió realizar una consultoría de un experto, y dado el caso que no existía nadie a nivel nacional

---

como parte de la cadena de custodia, no debe ser tomado como el resguardo que se ha críticado que no tienen las proveedoras de servicios de internet.

[345] Feusier. Óp. Cit. 11-12.

en julio de 2013 se decidió la búsqueda de un consultor internacional, resultando elegido el Dr. Emilio Viano, de la Universidad de Nueva York, EE. UU. Que presentó un resultado final que se titulaba “Proyecto de Ley Especial de Protección contra los Delitos Informáticos y de Datos” que incluía aspectos preventivos en materia de esta criminalidad, pasando por aspectos relacionados con la investigación de los delitos[346] los cuales sin ninguna explicación fueron suprimidos de la actual LECDIC pero se hacen necesarios para realizar una investigación y posterior obtención de prueba para demostrar la realización de un ciberdelito y la imputación de esa conducta a una persona o personas determinadas.

Se debe de hacer notar que la Constitución de la República establece los derechos y garantías que le asisten a todos los habitantes del país por igual, pues en ella, se encuentran las bases fundamentales que permiten que las leyes secundarias se desarrollen y sean cumplidas por la población, es decir, que sean de imperativo cumplimiento. En atención a lo dicho se debe hacer una lectura del Art. 11 inciso 1º que literalmente dice:

“…*Ninguna persona puede ser privada del derecho a la vida, a la libertad, a la propiedad y posesión, ni de cualquier otro de sus derechos sin ser previamente oída y vencida en juicio con arreglo a las leyes, ni puede ser enjuiciada dos veces por la misma causa…*”

[346] Feusier, Op. Cit. 12. Debe hacerse mención que incluso el anteproyecto dicho incluía un apartado que ordenaba la producción, preservación o divulgación de datos (hasta por 21 días en el caso de la preservación) a una empresa, proveedor de servicios o persona natural ante el requerimiento del Ministerio Público Fiscal, y que podía ser ampliado en el caso de la preservación de datos por un tiempo similar con la ayuda de un juez de paz.

De la lectura del artículo antes citado se puede deducir que se consagra la garantía de audiencia llamada también “Garantía del Debido Proceso Legal” y para el caso de los tribunales también conocida como “Garantía a la Tutela Judicial Efectiva”. Dicha garantía lo que implica es el derecho que tiene toda persona nacional o extranjera de obtener la protección de los tribunales contra las arbitrariedades del poder público y cuyo objetivo es tutelar la seguridad y certeza jurídica, por tal motivo que la LECDIC no regule aspectos procesales respecto del tratamiento probatorio y que la misma falencia exista en el Código Procesal Penal no puede mantenerse pues implicaría la posible impunidad de los Ciberdelitos o la lesión a la garantía de inocencia del imputado en un caso de ciberdelincuencia al lesionársele derechos por no tener claras las reglas del juego en cuanto a los aspectos probatorios.

Dicha falta de regulación sobre aspectos investigativos y relativos al proceso penal ha generado en la actualidad la existencia de un vacío legal o *laguna del derecho* que la jurisprudencia de la Sala de lo Constitucional ha venido a llenar o por lo menos se ha tomado criterio al respecto, así en resolución de fecha 08-VII-2010 en la referencia 54-2010 estableció:

“…*es menester indicar que el artículo 20 del Código Procesal Civil y Mercantil establece una regla general para la integración del Derecho en el ordenamiento jurídico procesal, pues prevé que:* ***“En defecto de disposición específica en las leyes que regulan los procesos distintos del civil y mercantil, las normas de este código se aplicarán supletoriamente***…”[347]

[347]Chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.jurisprudencia.gob.sv%2FDocumentosBoveda%2FD%2F1%2F2010-2019%2F2011%2F07%2F930B6.PDF&clen=106907&chunk=true consultada el 30 de noviembre de 2021.

"…*En ese sentido, esta disposición constituye* ***una norma básica para integrar lagunas normativas de las leyes que regulan la actividad jurisdiccional en otras ramas del Derecho****. Tal habilitación legal permite al Código Procesal Civil y Mercantil adquirir el papel de norma general en todas las cuestiones que por su naturaleza y estructura sean comunes a todo proceso, es decir, aquellas que –por su conexión con la estructura básica y esencial de cualquier proceso– puedan ser utilizadas para suplir un vacío en un orden jurisdiccional distinto al civil…*"[348]

Finalmente por lo dicho anteriormente mientras exista este vacío en la LECDIC y el código procesal penal se debe de recurrir a la regulación del Código Procesal Civil y Mercantil, específicamente a los Arts. 396 y siguientes, sobre de los medios de reproducción de sonido, voz e imagen y almacenamiento de información para que supletoriamente junto con las reglas de la cadena de custodia y la prueba pericial reguladas en el CPP puedan servir para el resguardo de la evidencia digital y la obtención de prueba electrónica para el proceso penal, garantizando la tutela legal efectiva en el caso de los ciberdelitos.

5.3. LIMITACIONES DE LA PNC

Debe de resaltarse que una institución que se ha visto reforzada de equipo y personal capacitado desde la vigencia de la LECDIC ha sido la PNC, ya que de pasar del año 2016 sin una unidad especializada para investigar los ciberdelitos en la actualidad cuentan con una unidad elite que trabaja este tipo

[348] Ibid.

de investigaciones, que puede realizar los siguientes análisis forenses relativos a los ciberdelitos:

-Análisis Forense Digital en discos duros por especialistas en Informática Forense.

-Análisis Forense Digital en Dispositivos móviles por especialista en informática Forense Móvil.

-Análisis Forense de Malware y Ransomware.

-Análisis Forense de Sitios Web, aplicaciones y sistemas operativos.

-Intervención por un especialista en la escena para la recolección de evidencia digital.

-Resguardar la evidencia electrónica de forma segura bajo medias de Seguridad Informática.[349]

Dicha unidad tiene acreditado internacionalmente su laboratorio científico, lo cual permite reducir tiempos de casos para obtener mejores evidencias. No obstante una fuente que solicitó el anonimato manifestó que cuenta con poco personal y que no todos están capacitados en los distintos tipos de análisis forenses antes indicados, siendo el principal obstáculo que las capacitaciones se reciben fuera de El Salvador y la gran mayoría requieren conocimientos avanzados del idioma inglés, debido a que el apoyo que tiene la unidad especializada es parte del Gobierno de los Estados Unidos de América. Así

[349] González. Óp. Cit. 27.

mismo manifestó que tienen equipo de avanzada, pero existen limitantes como que aún no se ha definido un protocolo de investigación a seguir y que la FGR no tiene una Unidad Especial para estos casos.[350]

5.4. LIMITACIONES DE LA FGR

En frecuentes supuestos, la investigación del ciberdelito se agrava por la circunstancia de que las alteraciones del programa y de los datos no dejan rastros comparables con los de los ilícitos tradicionales, por lo que es evidente que solo una pequeña parte de los ilícitos informáticos se descubren y cuando ello acontece, suele suceder fortuitamente. Por ese motivo, la ***cifra negra*** de estos comportamientos es excepcionalmente alta.[351]

Sobre este punto puede verse en la solicitud de acceso a la información referencia 207-UAIP-FGR-2020 emitida por la Unidad de Acceso a la información Pública de la FGR[352] se puede apreciar que el ente acusador en el proceso penal al ser requerido sobre que técnicas de investigación se utilizan para la investigación de los delitos informáticos manifestó:

Qué técnicas de investigación se utilizan para la investigación de los delitos informáticos, la FGR en su respuesta manifestó que en atención al Principio Procesal de Libertad Probatoria, regulado en el artículo 176 del Código Procesal Penal, los hechos que surjan de la investigación de cualquier delito pueden probarse por cualquier medio legal de prueba, tal como lo dispone el

---

[350] Se ha puesto en evidencia que la policía aún no ha definido un protocolo de investigación criminal para realizar las indagaciones necesarias para determinar los autores de un hecho delictivo y el tratamiento que se le dará a la prueba informática. En https://archivos.juridicas.unam.mx/www/bjv/libros/5/2379/5.pdf consultada el 30 de diciembre de 2021.
[351] Balmaceda Hoyos, *El delito de estafa informática*, 67–68.
[352] Ver anexo 2.

artículo antes señalado que establece: *"Los hechos y circunstancias relacionados con el delito podrán ser probados por cualquier medio de prueba establecido en este Código y en su defecto, de la manera que esté prevista la incorporación de* pruebas *similares, siempre que se respeten las garantías fundamentales de los personas consagrados en la Constitución y demás leyes.* Razón por la cual, este requerimiento de información solicitado por el peticionario no es factible de proporcionarlo, ya que requieren de una explicación en relación a temas concretos sobre el desarrollo de las investigaciones, en virtud que cada caso tiene sus particularidades en el desarrollo de la investigación, lo que puede conllevar a que en algunos casos se utilicen diversas técnicas y en otros no.

Como puede apreciarse al brindar la información ha existido silencio en cuanto a las técnicas de investigación circunstancia que denota que hay falta de capacitación de los Agentes Auxiliares de cómo realizar este tipo de investigaciones, pues debe recordarse que en el sistema penal salvadoreño son los Agentes del Fiscal General quienes libran la dirección funcional a la PNC para que realice las diligencias iniciales de investigación y son también estos quienes dan las instrucciones a la policía sobre los actos urgentes de comprobación que habría que realizar, entonces cómo es que no existen técnicas generales de investigación de los Ciberdelitos, se considera que esto se debe a lo dicho en el apartado anterior relativo a que no existe un protocolo de investigación definido para los Ciberdelitos.

También puede determinarse que aún la LECDIC no cuenta con suficientes casos ingresados para investigación en dicha institución que hayan permitido definir un plan de acción pues como puede verse en la siguiente tabla, que se basa en información contenida en el Anexo 2, se detallan los casos ingresados

desde la vigencia de la ley especial hasta mediados del año 2020 a nivel nacional:

Tabla 3. Ingreso de denuncias o casos regulados por la LECDIC desde su vigencia hasta mediados del año 2020

Casos Ingresados a la FGR regulados en la LECDIC	AÑO 2016	AÑO 2017	AÑO 2018	AÑO 2019	AÑO 2020
TOTAL	144	359	566	814	420

De la universalidad de casos antes indicados se puede ver que muy pocos han sido judicializados, así como hasta que etapa del proceso penal se mantuvieron en proceso los mismos y cuál fue el resultado del mismo

Tabla 4. Casos Judicializados sobre ilícitos regulados por la LECDIC desde su vigencia hasta mediados del año 2020

Casos judicializados por la FGR regulados en la LECDIC	**AÑO 2016**	**AÑO 2017**	**AÑO 2018**	**AÑO 2019**	**AÑO 2020**
Audiencia Inicial/Imposición de medidas	8	27	32	20	10
Audiencia Preliminar	1	12	30	22	3
Vista Publica		4	19	21	4
TOTAL	**9**	**43**	**81**	**63**	**17**
Resultado Absolutorio		*3*	*7*	*6*	*3*
Resultado Condenatorio		*5*	*23*	*26*	*6*

Los datos no son muy alentadores, pudiendo determinarse que no existe capacidad investigativa, ni se cuenta con personal capacitado en estos temas aunado a que según el informe de acceso a la información no existe una unidad especializada para la investigación de los ciberdelitos, ya que en la misma solicitud de información se dijo: *"La Institución no cuenta con una Unidad Organizativa ni fiscales auxiliares nombrados exclusivamente para conocer de la investigación y procesamiento de los delitos contenidos en la Ley Especial de Delitos Informáticos y Conexos. Por to que cada Oficina Fiscal, dependiendo de la naturaleza de cada denuncia, decide que Unidad conocerá la investigación, de conformidad al Art. 193 de la Constitución de la República."*

Al cierre de la presentación de esta investigación se ha conocido que el Fiscal General de la Republica se hizo presente a la Asamblea Legislativa el pasado 10 de noviembre de 2021 a proponer una serie de reformas a la LECDIC pues manifestó que la fiscalía *"no cuenta con las herramientas adecuadas para realizar las investigaciones"*[353] lo cual concuerda con lo dicho por la Jefe del Programa Global de Ciberdelito de la ONU para quien se hace necesario crear un departamento enfocado en el tema del ciberdelito o evidencia para que se enfoque en atender con urgencia este tipo de delitos.[354]

Finalmente en la solicitud de acceso a la información referencia 207-UAIP-FGR-2020 emitida por la Unidad de Acceso a la información Pública de la FGR se informa las capacitaciones que la institución ha brindado a su personal sobre estos temas, pero la misma es cuestionable ya que de no existir una unidad centralizada que se dedique a la investigación y posterior presentación de estos casos a los tribunales hace que no se pueda tener claridad si las

---

353 https://www.elsalvador.com/noticias/nacional/fiscal-impuesto-rodolfo-delgado-reformas-delitos-informaticos-diputados/899117/2021/ consultada el día 30 de noviembre de 2021.
354 Ver https://www.asamblea.gob.sv/node/11686

mismas inciden o no en el trabajo fiscal, así como no se informó sobre la cantidad de fiscales capacitados sobre estos temas. Así mismo la Fiscalía establece que no tienen acuerdos con proveedores de servicios de internet, tanto nacionales como internacionales, para resguardar información que sea necesaria para determinar la existencia de un ciberdelito e imputar su responsabilidad, lo cual conlleva a considerar que la LECDIC desde su vigencia en el año 2016 ha sido más una ley simbólica que una ley aplicada, lo cual ha propiciado la impunidad en temas relacionados con la ciberdelincuencia.

5.5. LIMITACIONES DE LA CSJ

Con la CSJ las limitaciones para la aplicación de la LECDIC en cuanto a la investigación y prueba de los ciberdelitos se denota por hecho que se demuestra en el anexo 3, que en resumen consiste en que la misma Corte Plena no tiene acuerdos de cooperación ni con proveedores nacionales de Internet y servicios de telefonía, ni con proveedores internacionales, lo cual es un obstáculo para cuando un juez requiera o se le facilite la cooperación en materia de actos de prueba para contar en el proceso con medios de prueba que proporcionen información o datos que sean necesarios dentro del desarrollo de un caso o se solicite su resguardo para que un perito especializado realice un examen indispensable sobre la evidencia digital que podría estar incluida en esos datos. Si bien es cierto que el Estado salvadoreño debería de propiciar estos acuerdos o convenios a través del Ministerio de Relaciones Exteriores, quedo establecido en el apartado 5.2.2, que según datos que constan en el anexo 1 el país no tiene proyectado realizar ningún acuerdo o convenio internacional de cooperación con proveedores de servicios de internet, por ello es que sería conveniente que la CSJ los tuviera.

Para la Jefa del programa global de ciberdelito de la ONU, considera que El Salvador debe contemplar la cooperación internacional en la investigación, ya que los delitos cometidos por medio del ciberespacio dejan evidencia que es volátil y si las autoridades no actúan de manera oportuna puede ser eliminada por los delincuentes. En algunos casos, estos delitos también pueden ser cometidos en varios territorios, lo que los convierte en transnacionales[355] siendo necesario que los países relativicen sus parámetros de jurisdicción y competencia buscanto más la colaboración Estatal a través del Ministerio publico y las distintas policías para atacar frontalmente el problema de la cibercriminalidad.

Por otra parte, parafraseando lo dicho por el presidente de la Asociación Salvadoreña de Abogados Digitales y Nuevas Tecnologías han propuesto a la Comisión de Seguridad y Combate a la Narcoactividad de la Asamblea Legislativa que se debe analizar la creación de juzgados especializados en materia de ciberdelincuencia y que los mismos tengan peritos adscritos a dichos juzgados[356]. La necesidad de jueces especializados se debe a la diversidad de temas de índole particular sobre las TIC´S y sus relaciones con el Derecho, como se verá más adelante, la CSJ ni el CNJ están desarrollando muy pocas capacitaciones sobre estos tópicos en los aplicadores de la ley lo que propicia la impunidad en este tipo de delitos pues su tratamiento no es conocido

Asimismo siempre existe por parte de los abogados que ejercen la defensa técnica de los imputados algún tipo de celo o desconfianza de los peritos permanentes de la PNC a los cuales se les cuestiona su falta de objetividad e

[355] https://www.asamblea.gob.sv/node/11686 consultado el día 30 de noviembre de 2021.
[356] Ibid.

imparcialidad; es por ello que resultaría conveniente que el órgano jurisdiccional tenga sus propios peritos[357] permanentes para garantizar la objetividad de peritaje, máxime en un país como El Salvador donde en ninguna universidad se preparan analistas informáticos forenses que puedan ser utilizados para realizar peritajes de parte, si se tienen dudas sobre lo realizado por el experto de la PNC. En el anexo 3 de esta investigación se revela que la CSJ no tiene ningún especialista en análisis de delitos informáticos adscrito a la misma en ninguna de sus dependencias.

Finalmente los jueces han tenido una capacitación mínima en temas relativos a la cibercriminalidad como se pone en evidencia en el anexo 4 de esta investigación, pues desde el 2016 al 2020 solo han recibido el curso titulado ***"Análisis de Estados financieros para la indagación de delitos de corrupción y conexos***" y el curso ***"Los delitos cometidos a través de nuevas tecnologías en la Ley Especial contra los Delitos Informáticos y Conexos"*** lo cual demuestra lo ínfimamente capacitados que están los jueces sobre este tema y el gran desconocimiento que tienen sobre la evidencia digital y la prueba informática, lo que puede ocasionar que no tengan la claridad necesaria a la hora que deban valorar la prueba sobre estos temas en un proceso determinado.

[357] Lo que se trata de establecer es un símil a lo que ocurre con los peritos médicos forenses, que por estar adscritos al Órgano Judicial dan más garantía de imparcialidad que los peritos que laboran para la FGR. Así también se busca que aquellos imputados que carezcan de recursos económicos suficientes para pagar un perito de parte, puedan solicitar al juez el nombramiento de un perito judicial que haga exámenes o dictámenes sobre evidencia electrónica.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

1) Los ciberdelitos son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos sin el consentimiento o con abuso del mismo. La finalidad usual de estos comportamientos es lesionar o poner en peligro de manera ilícita la seguridad de las funciones informáticas y la información; sin perjuicio de que esto implique la lesión o la puesta en peligro de otros bienes jurídicos tutelado

2) Se puede apreciar que las técnicas de investigación policial estudiadas en esta investigación y que se han desarrollado por la doctrina son bastante novedosas y que con base en el Art. 186 CPP pueden ser aplicadas en El Salvador para la lucha contra la ciberdelincuencia al establecer la norma citada que la policía podrá realizar las operaciones técnicas y científicas de tipo electrónicas disponibles por la ciencia y la técnica, esto es lo que permite utilizarlas con cierta discreción tratando de no lesionar derechos fundamentales.

3) Uno de los principales problemas para la investigación de los ciberdelitos es que la mayoría de los proveedores de internet a nivel mundial tienen su sede en el extranjero, principalmente en EEUU, por lo que en caso de requerir su colaboración para la investigación de ciberdelitos es que los datos que poseen se encuentran ubicados en servidores informáticos fuera del territorio salvadoreño, para cuya consecución es prácticamente obligado solicitarlos

mediante la oportuna comisión rogatoria internacional, lo que generalmente ralentiza, si no inutiliza, la investigación.

4) Se considera que El Salvador se encuentra en la actualidad con una situación, en la cual existe una falta de regulación de técnicas de investigación policial, evidencia digital y prueba informática, por lo que ante este vacío para investigar los Ciberdelitos, puede a la fecha llenarse de forma abierta que el Art. 186 CPP permite la realización de operaciones técnicas y científicas electrónicas y demás disponibles por la ciencia y la técnica policial, con lo cual las técnicas estudiadas en esta investigación pueden ser utilizadas, solo verificando que si las mismas requerirán una invasión o eventual lesión a derechos fundamentales, pues si es el caso deberá contarse con la respectiva autorización judicial, que determinará los alcances, el contenido y la duración de la misma como un acto urgente de comprobación.

5) En la LECDIC como norma penal especial solo se regulan las conductas constitutivas de ciberdelitos, pero no se establecen aspectos procesales los cuales deben ser tratados de conformidad con lo prescrito en el CPP, pero siendo este insuficiente en cuanto a la regulación de los Art. 186 y 201 de dicho cuerpo legal, para poder establecer medios de prueba para llevar las fuentes de prueba en las que se haya utilizado técnicas modernas de investigación de parte de la policía, se puede utilizar lo prescrito en el Art. 396 y 397 del Código Procesal Civil y Mercantil como medios de prueba útiles para el proceso penal, al igual que pueden realizarse peritajes sobre dichas fuentes.

6) El Salvador no tiene proyectado a la fecha ni suscribir y por ende tampoco ratificar el Convenio contra la Ciberdelincuencia de Budapest del 23-XI-2001 lo cual coloca al país en una posición de desventaja a fin de luchar contra la ciberdelincuencia y no le permite gozar del apoyo y cooperación internacional

que tienen los países para los cuales dicho convenio está vigente. Así mismo no forma parte de otros convenios multilaterales o ha realizado acuerdos bilaterales con otros países o entidades para la lucha contra el ciberdelito.

6.2. RECOMENDACIONES

1) El Salvador debe considerar formar parte de los países que tienen vigente en sus legislaciones nacionales el convenio de la cibercriminalidad a fin de poderse beneficiar con la cooperación internacional principalmente en los delitos que son cometidos fuera de las fronteras patrias pero que afectan a los ciudadanos salvadoreños, para lo cual también sería conveniente que realizara acuerdos bilaterales o multilaterales con organismos de la Región centroamericana o en Latinoamérica.

2) Los legisladores deben realizar reformas a la LECDIC o al CPP a fin de incluir el tratamiento de la evidencia digital, el resguardo de la información por parte de los proveedores de servicios de internet y el tratamiento de la prueba electrónica.

3) Se hace necesario que la PNC cuente con más personal capacitado para realizar análisis forenses informáticos que sirvan para obtener información y luego la prueba electrónica muy necesaria para judicializar los casos para que la LECDIC deje de parecer un mero Derecho penal simbólico y se determine su aplicación para juzgar a los implicados en dichos hechos ilícitos.

4) Se hace indispensable que la FGR tenga, al igual que la PNC, una unidad especializada para la investigación y promoción de procesos penales sobre ilícitos sancionados en la LECDIC a fin de que sean capacitados y entrenados debidamente para aplicar dicha normativa.

5) La CSJ en coordinación con el CNJ debe promover la capacitación de los jueces sobre los temas relativos a la ciberdelincuencia y a los mecanismos que sean necesarios para la producción de prueba y valoración de la misma.

GLOSARIO

En este apartado se presentan los conceptos o abreviaturas, así como sus respectivas definiciones de los términos más importantes que tendrá el desarrollo de la tesis, tal cual se presentan a continuación:

ADMINISTRADOR: Aquel que tiene el poder absoluto sobre la máquina, el control sobre el funcionamiento del sistema informático.[358]

ADJUNTO – ATTACHMENT: Fichero que se incluye en un mensaje de correo electrónico, puede contener texto, imágenes, sonido, secuencias[359], etc

ANCHO DE BANDA: Tamaño de la conducción de datos

ARCHIVO: Forma de estructurar la información. También es sinónimo de fichero. Todos los archivos que son sólo de texto, son archivos binarios. Hay que distinguir entre archivo de datos y archivo ejecutable. Archivo de datos, es la fórmula simple, una especie de contenedor de información. Archivo ejecutable, sería en realidad un programa, puesto que siguiendo los parámetros que da, realiza unas acciones determinadas.[360]

BIT: Unidad básica de datos. Nombre que se da a los dos dígitos, 0 y 1, que utiliza la numeración binaria, también llamada lenguaje binario, lenguaje de máquina o código de máquina[361]

---

[358] Juan José González Rus, et al. *Cuadernos penales José María Lindón.* (Bilbao: Universidad de Deusto, 2007) 392.
[359] Ibid.
[360] Ibid 393.
[361] Ibid 393.

BOT: Diminutivo de robot. Es un programa informático que realiza en línea funciones normalmente realizadas por humanos. En un sitio de conversación, un *bot* puede simular ser una persona. Se les considera una de las herramientas favoritas de los *hackers.*[362]

BYTES: Son las unidades que usan los ordenadores (computadoras) para representar una letra, un número o un símbolo. Unidad de medida informática. Un byte suele ser equivalente a ocho bits, un *megabyte,* mil Kilobytes. El orden de medida sería el siguiente: *Byte, kilobyte (*KB*), megabyte* (MB*), gigabyte* (GB), *terabyte* (TB)[363]

CABALLO DE TROYA o TROYANOS: Programas que se ocultan dentro de otros, para no ser descubiertos, y se instalan en el sistema de un usuario, de forma que al actuar producen un auténtico sabotaje contra el sistema informático. Los Troyanos no se replican a sí mismos lo que les diferencia de los virus puros, aunque algunos si son capaces de enviarse como adjuntos.[364]

CARPETA: Espacio que podemos crear en la computadora para almacenar datos, equivale a un directorio.

CIBERCRIMEN: Es el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o

---

[362] Ibid 394..
[363] Ibid. 385
[364] Ibid. 395.

autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual[365]

CIBERESPACIO: Concepto que procede de la literatura de ficción, concretamente utilizado por Willian Gilbson, para referirse al mundo entre los ordenadores conectados, redes de información y medios digitales[366]

CIBERDELITO: Este concepto se utiliza para referirse a una gama de actividades ilícitas cuyo denominador común es el papel central que desempeñan las redes de información y la comunicación (TIC) en su comisión.[367] No obstante, existen autores para los cuales este concepto es sinónimo de cibercrimen[368], por lo que en la investigación se utilizarán como sinónimos.

CIBERPUNK: Se ha utilizado en ocasiones para los *hackers* por lo que significa movimiento social de desconfianza o ataque a las máquinas.[369]

CRACKER: De forma simple, pirata informático malo. Persona que accede ilegalmente a un sistema informático ajeno con fines vandálicos o dañinos, para cierta parte de la doctrina este aspecto queda igualmente incluido en el

---

[365] Carlos María Romeo Casabona. *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminales*, en El Cibercrimen. (Granada: Comares, 2006) 1-43

[366] González Rus. 396

[367] Quevedo González. *Investigación y prueba del ciberdelito.* 58.

[368] En este caso puede confrontarse la definición de Carlos Maria Romedo Casabona con la utilizada por Josefina Quevedo en la cual puede apreciarse que es la misma de aquel autor pero enmarcada bajo la idea del ciberdelito.

[369] González Rus. 396.

Hacking por lo que desde este concepto restringido su objetivo sería producir daño, frente al *hacker* que busca obtener información.[370]

DERECHO INFORMATICO: Es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad[371]

DELINCUENCIA INFORMATICA o CRIMINALIDAD INFORMATICA: Son los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera y todos aquellos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva[372]

FTP: Es la abreviatura del grupo de palabras de origen inglés que se leen *"File Transer Protocolo"* que traducido al español significa Protocolo de transferencia de archivos que es una forma de mover información de un punto a otro u otros en la red.

GSM: Corresponde a una sigla en inglés de "Global Sistem Movile" que significa "Sistema Global de Comunicaciones Móviles. Se trata de un estándar muy utilizado desde principios de siglo y también se conoce como 2G y fue denominado así porque antes de esto todas las comunicaciones eran analógicas.

HACKER: Pirata informático. El concepto original, *Hacking,* abarcaba cualesquiera accesos no autorizados, con o sin intención dañosa, con o sin

---

[370] Ver González Rus Óp cit 397 y confrontar con Azola Calderón que manejan la misma opinión en cuanto a este concepto.
[371] Leyre Hernández Díaz. *Aproximación a un concepto de derecho penal informático.* en Derecho penal informático, (Bilbao: Instituto Vasco de Criminología)
[372] Ibid.

intención de lucro. Según algunas opiniones, el concepto no incluye a quien entra en el ordenador con intención criminal o vandálica, para el cual sería apropiado el término **"*Cracker".*** Según algunas fuentes, el concepto viene de "*hack"* que era el sonido que se empleaba en las empresas de telefonía al golpear el aparato telefónico para que funcionara.[373]

HTTP: Es la abreviatura de un hipter texto que remite a un protocolo de internet, en ingles significa *"Hyper Text Transfer Protocol"* que se usa para dirigirse a una zona de internet determinada.

IP: Es la abreviatura de las palabras *"Internet Protocol"* que es un protocolo de internet para identificar la fuente y origen de una conexión o alojamiento de cierta información, así mismo son un conjunto de normas técnicas de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional, es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

IMEI: Es la abreviatura en idioma Ingles de "International Mobile Equipment Identity", que significa identidad internacional de equipo móvil, que es un código pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

IMSI: Es el acrónimo de "International Mobile Subscriber Identity" que se traduce en "Identidad Internacional del Abonado Móvil". Es un código de

---

[373] González Rus, Óp cit. 400

identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

INTERNET: Red de redes de ordenadores a escala mundial con un sistema de comunicación común

ISP: Es la abreviatura con la que se designa a un proveedor de servicios de internet, que por su origen en Ingles significa: "*Internet Service Provider"*

LAN: Que abrevia las palabras "*Local Area Network"* que hace referencia a la red local donde una o varias personas pueden conectarse para accesar al internet.

MAC: Significa "Media Access Control" que se traduce en "Control de acceso a medios"; es un identificador único para las interfaces de red. Se utiliza como dirección de red para la mayoría de las tecnologías de la información y la comunicación.

RANSOMWARE: Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo que es infectado por el programa y los ejecutores de este programa piden un rescate a cambio de quitar la restricción que tiene secuestrados los datos.

SERVIDOR: Ordenador que permite a un usuario autorizado utilizar recursos y servicios de un ordenador remoto. El término obedece a que ese ordenador presta servicios a las otras máquinas o clientes. Los servicios pueden ser de todo tipo, almacenar o acceder a archivos, aplicaciones, correo electrónico,

etc. Se les denomina también *host* y el hecho de publicar algo en ellos se denomina *"hosting"* que se podría traducir como alojar lo escrito.[374]

SISTEMA INFORMÁTICO: Es un conjunto de elementos que hace posible el tratamiento automático de la información. Las partes de un sistema informático son: • Componente físico: está formado por todos los aparatos electrónicos y mecánicos que realizan los cálculos y el manejo de la información. • Componente lógico: se trata de las aplicaciones y los datos con los que trabajan los componentes físicos del sistema. • Componente humano: está compuesto tanto por los usuarios que trabajan con los equipos como por aquellos que elaboran las aplicaciones.

SKINNING: Clonado de tarjetas de crédito.

SOFTWARE: Conjunto de programas y aplicaciones informáticas que hacen funcionar a una computadora o que se ejecutan en ella.

SPYWARE: Programa espía o aplicación maliciosa que se instala sin que el usuario lo advierta, normalmente al descargar otro programa[375].

TCP/IP: En este caso en concreto se fusionan dos abreviaturas que literalmente se leen: *"Transmission Control Protocol/Internet Protocol"* que significa Protocolo de Control de Transmisión al protocolo de internet que indica la forma de control de toda transmisión realizada entre distintos protocolos de internet".

---

[374] Ibid 406.
[375] Ibid. 408.

UMTS; Son las siglas en ingles de "Universal Mobile Telecommunications System" traducido al español como Sistema Universal de Telecomunicaciones Móviles que es una tecnología móvil de la llamada tercera generación (3G), sucesora de la tecnología GSM (Global System for Mogile) o 2G

WEBMASTER: Persona encargada de la gestión y el mantenimiento técnico de un servidor de páginas web o de una web determinada[376].

WEBSITE: Sitio web. Conjunto de páginas web que comparten una misma dirección[377].

www: Abreviatura que hace alusión al conjunto de todas las páginas web de internet, lo que se conoce como la red mundial world wide web.

[376] Ibid. 410.
[377] Ibid. 410.

BIBLIOGRAFIA

1) Aboso, Gustavo Eduardo. Derecho penal cibernético: la cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la información. Buenos Aires: B de F, 2017.

2) Acurio del Pino, Santiago. Manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0 en https://www.oas.org/juridico/english/cyb_pan_manual.pdf

3) Azaola Calderón, Luis y Instituto de Formación Profesional (México). Delitos informáticos y derecho penal. México: Editorial UBIJUS, 2010.

4) Bacigalupo, Enrique. Lineamientos de la teoría del delito. 2a ed., corregida y Actualizada. Colección Escuela Libre de Derecho. San José, Costa Rica: Editorial Juricentro, 1985.

5) Balmaceda Hoyos, Gustavo. El concepto de perjuicio en el delito de estafa análisis dogmático. Bogotá, Colombia: Leyer, 2009.

6) Balmaceda Hoyos, Gustavo. El delito de estafa informática. Bogotá, D.C., Colombia: Leyer, 2009.

7) Bielli, Gastón Enrique, y Carlos Jonathan Ordoñez. La prueba electrónica: teoría y práctica. Ciudad Autónoma de Buenos Aires: Thomson Reuters La Ley, 2019.

8) Bueno de Mata, Federico. Prueba electrónica y proceso 2.0: especial referencia al proceso civil. Abogacía practica 63. Valencia: Tirant lo Blanch, 2014.

9) Calderón Cerezo, Ángel, y José Antonio Choclán Montalvo. Derecho Penal. Tomo I. Parte General. Barcelona: Bosch, 1999.

10) Cardoso Pereira, Flavio. El agente encubierto. Desde el punto de vista del garantismo procesal penal. San Salvador, El Salvador: Cuscatlán, 2018.

11) Carrancá, Raúl. Derecho Penal Mexicano, Parte General. Ciudad de México: Porrúa, 2016.

12) Castillo González, Francisco. La estafa informática. San José, Costa Rica: Editorial Jurídica Continental, 2016.

13) Choclan Montalvo, José Antonio. El delito de estafa. 2. ed. Barcelona: Bosch, 2009.

14) Cremades, Javier, Miguel A. Fernández Ordóñez, y Rafael Illescas Ortiz, eds. Régimen jurídico de Internet. Colección Derecho de las telecomunicaciones. Las Rozas (Madrid): La Ley, 2002.

15) Devis Echandia, Hernando. Teoría General de la Prueba Judicial, Tomo II. Quinta Edición. Buenos Aires, Argentina: Victor P. de Zavalia, 1981.

16) Donna, Edgardo Alberto. Teoría del delito y de la pena. 2: Imputación delictiva. Buenos Aires: Depalma/Astrea, 1995.

17) Fernández Carrasquilla, Juan. Derecho penal fundamental. 2. reimpresión de la 2. ed. Santa Fe de Bogotá, Colombia: Editorial Temis, 1989.

18) Flores Prada, Ignacio. Criminalidad Informática. Aspectos Sustantivos y Procesales". Valencia, España: Tirant lo Blanch, 2012.

19) Feusier Ayala, Oswaldo Ernesto. Aplicación y contenido de la Ley Especial contra la delincuencia informática y conexos. San Salvador, El Salvador: Consejo Nacional de la Judicatura, 2018.

20) Garrido Montt, Mario. Derecho penal. Segunda edición actualizada. Santiago, Chile: Editorial Jurídica de Chile, 2016.

21) Gómez, Leopoldo Sebastián. “Evidencia digital en la investigación penal”. En Cibercrimen, 619–37. Buenos Aires: B de F, 2017.

22) González Benitez, Lenin y Hector Tulio Baires. "Legislación penal", San Salvador: Editorial Cuscatleca, 2021.

23) González Hurtado, Jorge Alexandre. “Delincuencia informática: Daños informáticos del Artículo 264 del Código Penal y propuesta de reforma”. Tesis Doctoral, Universidad Complutense de Madrid, 2013.

24) González, Ronald. “Ciber Crimen”. PDF, San Salvador, El Salvador, 2020.

25) González Rus, Juan José. Cuadernos Penales José María Lidón. 4. Bilbao: Universidad de Deusto, 2007.

26) Gutiérrez Francés, María Luz. Fraude informático y estafa: aptitud del tipo de estafa en el derecho español ante les defraudaciones por medios informáticos. Madrid: Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, 1991.

27) Henríquez González, Irma Joana. “Los actos Urgentes de investigación y el anticipo de prueba en el nuevo código procesal penal”. En Ensayos doctrinarios sobre el nuevo proceso penal salvadoreño, 1° Edición., 215–44. San Salvador, El Salvador: Sección de Publicaciones CSJ, 2011.

28) Jiménez Huerta, Mariano. La tipicidad. México D.F.: Porrúa, 1955.

29) Kielmanovich, Jorge L. Teoría de la prueba y medios probatorios. Cuarta edición, Ampliada y Actualizada. Buenos Aires: Rubinzal-Culzoni Editores, 2010.

30) Ligia Maribel García Juárez. “La investigación de delitos emergentes en internet, su detección y control”. Universidad Rafael Landivar, 2014.

31) López Betancourt, Eduardo. Teoría del delito. México: Porrúa, 2015.

32) Luzón Peña, Diego-Manuel. Derecho penal: parte general. Montevideo; Buenos Aires: Editorial B de F, 2018.

33) Mayer Lux, Laura “El bien jurídico protegido en los delitos informáticos” en Revista Chilena de Derecho, volumen 44, número uno, año 2017. pp. 235 – 260.

34) Moreno Catena, Víctor M., y Valentín Cortés Domínguez. Derecho procesal penal. 3. ed. Manuales. Valencia: Tirant lo Blanch, 2008.

35) Morón Lerma, Esther. Internet y derecho penal: Hacking y otras conductas ilícitas en la red. Barcelona: Aranzadi, 1999.

36) Muñoz Conde, Francisco. Derecho Penal. Parte General. 4 Edición. Valencia: Tirant lo Blanch, 2000.

37) Muñoz Conde, Francisco. Teoría general del delito. Bogotá, Colombia: Temis, 2018.

38) Nava Garcés, Alberto Enrique. Delitos informáticos. México: Editorial Porrúa, 2007.

39) Nava Garcés, Alberto Enrique. Delitos informáticos. México: Porrúa, 2016.

40) Novoa Monreal, Eduardo. Curso de Derecho Penal Chileno. Parte General. Santiago: Jurídica de Chile, 2010.

41) OEA. Tendencias de seguridad cibernética en América Latina y El Caribe. Washington: OEA, 2014.

42) Ortuño Navalón, Maria del Carmen. La prueba electrónica ante los tribunales. Valencia: Tirant lo Blanch, 2014.

43) Oscar Carlos Ernesto Aguirre Linares. “Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en El Salvador”. Universidad Don Bosco de El Salvador, 2020.

44) Otto, Harro, y José R Béguelin. Manual de derecho penal: Teoría general del derecho. Barcelona: Atelier Libros, 2017.

45) Palazzi, Pablo Andrés. Delitos informáticos. 1. ed. Buenos Aires: Ad-Hoc, 2000.

46) Pérez del Valle, Carlos. Lecciones de derecho penal: parte general. Madrid: Dykinson, 2016.

47) Posada Maya, Ricardo. Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del título VII bis del Código penal colombiano. Colección Ciencias penales. Bogotá, D.C., Colombia: Universidad de los Andes : Grupo Editorial Ibáñez, 2017.

48) Quevedo González, Josefina. "Investigación y prueba del ciberdelito". Tesis Doctoral, Universidad de Barcelona, 2017.

49) Reyes Echandía, Alfonso. Antijuridicidad. Cuarta edición. Santa Fe de Bogotá: Temis, 1999.

50) Reyes Echandia, Alfonso. Tipicidad. 2.reimpr. de la 6. ed. Santa Fe de Bogotá: Temis, 1999.

51) Reza Reyes, Sandra. "Uso ilícito de la red: 'El caso de la DEEP WEB'". En Ciberdelitos, 181–96. México: Tirant lo Blanch - INACIPE, 2019.

52) Rodríguez Luna, Víctor Manuel. "Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos". Secretaria de Naciones Unidas y Fiscalía General de la Republica, 2018.

53) Romo Medina, Miguel. Criminología y derecho. 2. ed. Serie J--Enseñanza de derecho y material didáctico, num. 10. México: Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, 1989.

54) Roxin, Claus. Derecho penal. Parte general. Madrid, España: Editorial Civitas, 1997.

55) Roxin, Claus. Derecho penal parte general, tomo I, fundamentos, la estructura de la teoría del delito. Madrid: Civitas, 2007.

56) Sánchez Escobar, Carlos Ernesto, Marco Tulio Díaz Castillo, y Sergio Luis Rivera Márquez. Reflexiones sobre el nuevo proceso penal. 1. ed. San Salvador, El Salv: Consejo Nacional de la Judicatura, 2009.

57) Sandoval Rosales, Rommell Ismael. Código Procesal Penal Comentado. San Salvador, El Salvador: Consejo Nacional de la Judicatura, 2018.

58) Sanjurjo Rebollo, Beatriz. Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, proteccion de datos, negocios audiovisuales, ecommerce, consumidores, marketing online y publicidad digital. Madrid: Dykinson, 2015.

59) Serrano, Armando Antonio, Delmer Edmundo Rodríguez Cruz, José David Campos Ventura, y Miguel Alberto Trejo, eds. Manual de derecho procesal penal. San Salvador: Centro de Información Jurídica, Ministerio de Justicia, 1998.

60) Silvestroni, Mariano H. Teoría constitucional del delito. 2. ed., Actual. Buenos Aires: Eds. Del Puerto, 2007.

61) Téllez Valdés, Julio. Derecho informático. 2. ed. Serie jurídica. México: McGraw Hill, 1996.

62) Trejo, Miguel Alberto, Armando Antonio Serrano, Ana Lucila Fuentes de Paz, y Delmer Edmundo Rodríguez Cruz, eds. Manual de derecho penal. Parte Especial. 2º Edición. San Salvador: Centro de Información Jurídica, Ministerio de Justicia, 1999.

63) Urbano Castrillo, Eduardo de. La valoración de la prueba electrónica. Valencia: Tirant lo Blanch, 2009.

64) Zapata Marcó, Juan Carlos. “El delito de estafa en la modalidad ‘phishing’ a través de internet y sus medios probatorios en Venezuela,”. Universidad de Carabobo, 2009.

Páginas Web Consultadas

1) https://histinf.blogs.upv.es/2011/12/05/proyecto-eniac/#:~:text=El%20proyecto%20ENIAC%20(%20Electronic%20Numerical,la%20maquina%20hasta%20el%201946. Consultado el 30 de diciembre de 2020.

2) http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc, consultada el 31/12/20.

3) http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc Consultada el 31/12/20.

4) https://www.youtube.com/watch?v=1pB2kan_AFk, y https://www.youtube.com/watch?v=KbHlWaeniHE, consultados ambos el 31/12/20,

5) http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc, consultado el 31/12/20.

6) http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc Consultada el 31/12/20.

7) https://www.google.com.sv/?gws_rd=cr,ssl&ei=l1_9WOGdNcPemAH6lpCwDw#q=ram+que+signific sin autor, consultada en 23/04/2017.

8) https://hipertextual.com/2016/05/softram-historia-duplicadores-ram, sin autor, consultada el 23/03/17.

9) http://www.sopitas.com/378293-los-estafas-realizadas-eninternet-mas-grandes-de-la-historia/ , sin autor, consultada el 23/04/17

10) https://www.youtube.com/watch?v=7qaoSIeySzI consultada el 23/04/2017.

11) http://www.asamblea.gob.sv/noticias/legislatura-2012-2015/noticias/analizan-penalizar-delitos-cometidos-a-traves-de-la-tecnologia-informatica.

12) https://www.uv.es/~bellochc/pdf/pwtic1.pdf

13) http://www.politicacriminal.gov.co/Portals/0/documento/queespoliticacriminal-ilovepdf-compressed.pdf?ver=2017-03-09-180813-317

14) http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/capitulo1.pdf (consultado el 05 de diciembre de 2018)

15) https://concepto.de/dato-en-informatica/#ixzz6sRh034Zv

16) http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF

17) www.ladeepweb.blogspot.mx

18) http://conventions.coe.int/Treaty/EN/projets/cybercrime27.html).

19) https://grupo4nri.wordpress.com/2-normativa-internacional/

20) http://www.uncjin.org/documents/irpc4344.pdf

21) http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF

22) http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

23) https://www.unifr.ch/ddp1/derechopenal/articulos/a_20100831_02.pdf

24) José Maria Molina Mateos https://www.abogacia.es/publicaciones/blogs/blog-nuevas-tecnologias/la-ciberseguridad-como-bien-juridico-protegido/

25) https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/ManualUnicoInvestigacion.pdf

26) http://www.slideshare.net/mariaelenasotojara/las-redes-sociales-son-estructuras-sociales-compuestas-de-grupos-de-personas

27) https://histinf.blogs.upv.es/2011/12/05/proyecto-eniac/#:~:text=El%20proyecto%20ENIAC%20(%20Electronic%20Numerical,la%20maquina%20hasta%20el%201946.

28) http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc

29) https://www.google.com.sv/?gws_rd=cr,ssl&ei=l1_9WOGdNcPemAH6lpCwDw#q=ram+que+signific

30) http://www.asamblea.gob.sv/noticias/legislatura-2012-2015/noticias/analizan-penalizar-delitos-cometidos-a-traves-de-la-tecnologia-informatica.

31) http://www.internautas.org/html/8833.html

32) https://riull.ull.es/xmlui/bitstream/handle/915/16410/El%20agente%20encubierto%20informatico.%20Especial%20atencion%20al%20agente%20encubierto%20informatico..pdf?sequence=1

33) http://repositorio.uchile.cl/bitstream/handle/2250/176344/Herramientas-del-convenio-de-Budapest-sobre-ciberdelincuencia-y-su-adecuacion-a-la-legislacion-nacional.pdf?sequence=1&isAllowed=y

34) https://www.laprensagrafica.com/economia/El-Salvador-advierten-de-fraudes-bancarios-por-correos-electronicos-20210822-0026.html,

35) https://www.laprensagrafica.com/economia/Banco-Agricola-alerta-a-clientes-ante-alza-de-denuncias-por-fraude-20210906-0078.html

36) https://www.elsalvador.com/noticias/negocios/estafas-bitcoin-bancos/871906/2021/

37) https://www.elsalvadortimes.com/articulo/sucesos/clientes-denuncian-que-algunas-cuentas/20210823153256081461.html

38) https://www.elsalvadortimes.com/articulo/sucesos/maestra-pierde-salario/20210830122530081561.html

39) https://www.elsalvadortimes.com/articulo/sucesos/capturan-acusan-especialista-em-sistemas-informacion/20210901105915081592.html

40) https://www.bbc.com/mundo/noticias-america-latina-58482830

41) https://diario.elmundo.sv/chivo-wallet-sigue-con-fallas-y-sin-disponibilidad-para-varios-modelos-a-una-semana-de-lanzamiento/

42) https://youtu.be/6E__nE3eSBI

43) https://youtu.be/8ThpWu_li6U

44) file:///Users/lucioarias/Downloads/elementos_descriptivos,_normativos_y_subjetivos_del_tipo_penal.pdf

45) https://archivos.juridicas.unam.mx/www/bjv/libros/5/2379/5.pdf

46) https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

47) https://iurisnow.com/es/articulos/delito-intrusismo-informatico/

48) https://www.camjol.info/index.php/DERECHO/article/download/12223/14276/44901

49) https://www.larazon.es/tecnologia/los-ciberataques-con-motivacion-politica-se-disparan-LG15028672/

50) https://www.latimes.com/espanol/eeuu/articulo/2021-05-09/eeuu-ciberataque-a-oleoducto-esta-ligado-a-grupo-criminal, Por Mae Anderson y Frank Bajak Associated Press. 9 de mayo de 2021,

51) https://www.milenio.com/negocios/financial-times/hackers-lamentan-dano-a-sociedad-por-oleoducto

52) https://youtu.be/sEEmY7SFvtg

53) https://www.elmundo.es/elmundo/2010/03/25/navegante/1269554529.html

54) https://youtu.be/GwVhSMqVcl0

55) https://diarioelsalvador.com/policia-nacional-civil-y-fiscalia-investigaran-casos-de-suplantacion-de-identidad-en-la-chivo-wallet/143668/ consultado el 30 de noviembre de 2021.

56) https://www.elsalvador.com/noticias/nacional/fiscal-impuesto-rodolfo-delgado-reformas-delitos-informaticos-diputados/899117/2021/ consultado el 30 de noviembre de 2021.

57) chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.jurisprudencia.gob.sv%2FDocumentosBov

eda%2FD%2F1%2F20102019%2F2011%2F07%2F930B6.PDF&clen=106907&chunk=true consultado el 30 de noviembre de 2021.

58) https://www.asamblea.gob.sv/node/11686 consultado el 30 de noviembre de 2021.

59) https://www.elsalvador.com/noticias/nacional/fiscal-impuesto-rodolfo-delgado-reformas-delitos-informaticos-diputados/899117/2021/ consultado el 30 de noviembre de 2021.

ANEXO 1: INFORMACION DE RELACIONES EXTERIORES

La infrascrita Oficial de Información del Ministerio de Relaciones Exteriores, CERTIFICA: que en el procedimiento de tramitación de la solicitud de acceso a la información iniciado por el señor Lucio Albino Arias López, se encuentra la resolución de las trece horas y cinco minutos del día treinta y uno de julio de dos mil veinte, que literalmente DICE: """""""""""

SAI 109-2020(1)

OFICINA DE ACCESO A LA INFORMACIÓN PÚBLICA DEL MINISTERIO DE RELACIONES EXTERIORES. Antiguo Cuscatlán, a las trece horas y cinco minutos del día treinta y uno de julio de dos mil veinte.

Por recibida la solicitud de acceso a la información, procedente de la dirección de correo electrónico lucio.arias@ues.edu.sv, presentada a las trece horas y treinta y ocho minutos del día veintidós de julio de dos mil veinte, por **Lucio Albino Arias López**, por medio de la cual requiere, en síntesis, información referente a la suscripción y ratificación de determinados instrumentos internacionales.

ADMISIBILIDAD Y TRÁMITE DE LA SOLICITUD DE ACCESO A LA INFORMACIÓN

I. La suscrita Oficial de Información, habiendo examinado que la solicitud de acceso a la información cumple con los requisitos señalados en el artículo 66 de la Ley de Acceso a la Información Pública (LAIP), y los artículos 50, 52 y 54 del Reglamento de la Ley de Acceso a la Información Pública (RLAIP), determinó su admisibilidad, y en consecuencia procedió a darle el trámite correspondiente.

II. A continuación, la suscrita Oficial de Información trasladó la solicitud en cuestión a la unidad organizativa que pudiera poseer dicha información, a fin de que se verificara su existencia y clasificación, y de ser procedente, se trasladara a esta Oficina, de conformidad con lo establecido en el artículo 70 LAIP.

FUNDAMENTACIÓN DE LA RESPUESTA

III. El derecho de acceso a la información surge como manifestación del derecho a la libertad de expresión, contemplado en el artículo 6 de la Constitución, que comprende la libertad de buscar, recibir y difundir información de toda índole, y específicamente, aquella que se derive de la gestión gubernamental. Asimismo, la Ley de Acceso a la Información Pública reconoce el principio de máxima publicidad, y establece que la información en poder de los entes obligados es pública y su difusión irrestricta, salvo las excepciones expresamente establecidas por la ley –Art. 4 letra a) LAIP–.

En relación con el deber de motivación de las resoluciones administrativas, los artículos 65 y 72 LAIP, y los artículos 55 y 56 RLAIP, establecen que las decisiones de los entes obligados respecto a las solicitudes de acceso a la información deben entregarse por escrito, haciendo mención en la resolución de los fundamentos que la motivan, y ser notificada al solicitante en el plazo establecido.

IV. En síntesis, la solicitud de acceso a la información incoada por el peticionario va encaminada a obtener determinada información respecto de la suscripción y ratificación de ciertos instrumentos internacionales. En atención a ello, la Dirección General de Asuntos Jurídicos trasladó la documentación que da respuesta a lo requerido en la solicitud.

V. Consecuentemente, habiéndose comprobado por dicha Dirección General que la respuesta trasladada en atención a la solicitud de acceso a la información no está sujeta a alguna de las limitaciones de divulgación de información contemplada en la Ley de Acceso

a la Información Pública y su Reglamento, debe procederse a la entrega de la misma al peticionario por medio de documento anexo a este proveído.

PARTE RESOLUTIVA

VI. En virtud de lo anterior, y con base en las disposiciones legales citadas, la suscrita Oficial de Información **RESUELVE**:

1. *Declárase* admisible la solicitud de acceso a la información presentada a las trece horas y treinta y ocho minutos del día veintidós de julio de dos mil veinte, por el señor Lucio Albino Arias López.

2. *Entréguese* al peticionario la información requerida en la solicitud de acceso a la información.

3. *Notifíquese* la presente resolución al interesado en el medio y forma señalados para tales efectos.

Ana Lucía de los Ángeles Orantes Hernández
Oficial de Información a.i.
Ministerio de Relaciones Exteriores

ES CONFORME CON SU ORIGINAL, con la cual se confrontó y para ser entregada al señor Lucio Albino Arias López, se extiende, firma y sella la presente CERTIFICACIÓN, constando de un folio útil, a las trece horas y treinta y cinco minutos del día treinta y uno de julio de dos mil veinte.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS

1. El Salvador ha ratificado Convenio sobre la Ciberdelincuencia, de Budapest, 23-XI-2001. El Salvador no ha ratificado dicho Convenio.

2. El Salvador es suscriptor del Convenio sobre la Ciberdelincuencia, de Budapest, 23-XI-2001. El Salvador no es suscriptor del Convenio.

3. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos internacionales sobre Ciberdelincuencia o delitos informáticos. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de suscripciones o ratificaciones de Convenios, Tratados o Acuerdos internacionales sobre Ciberdelincuencia o delitos informáticos.

4. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos Bilaterales sobre Ciberdelincuencia o delitos informáticos. Si la respuesta es afirmativa cuales, con que Estados los hay y emita el texto del mismo (en español) y manifieste si ya entro en vigencia. No hay registro de suscripciones o ratificaciones de Convenios, Tratados o Acuerdos bilaterales sobre Ciberdelincuencia o delitos informáticos.

5. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos internacionales sobre cooperación en caso de delitos transnacionales. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. Tratado sobre el Comercio de Armas.
SUSCRITO EL 5 DE JUNIO DE 2013
D. L. No. 537, DE FECHA 14 DE NOVIEMBRE DE 2013
D. O. No. 224, TOMO 401, DE FECHA 29 DE NOVIEMBRE DE 2013

6. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos bilaterales sobre cooperación en caso de delitos transnacionales. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de suscripciones o ratificaciones de Convenios, Tratados o Acuerdos bilaterales sobre cooperación en caso de delitos transnacionales.

7. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos internacional sobre cooperación en investigación de delitos transnacionales o delitos informáticos. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de suscripciones o ratificaciones de Convenios, Tratados o Acuerdos internacionales sobre cooperación en investigación de delitos transnacionales o delitos informáticos.

8. El Salvador ha suscrito o ratificado Convenios, tratado o acuerdos bilaterales sobre cooperación en investigación de delitos transnacionales o delitos informáticos. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de

suscripciones o ratificaciones de Convenios, Tratados o Acuerdos bilaterales sobre sobre cooperación en investigación de delitos transnacionales o delitos informáticos.

9. Que convenios, tratados o acuerdos internacionales o bilaterales tiene El Salvador suscrito o ratificado sobre extradición. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. Tratado de Extradición entre la República de El Salvador y la República del Perú.
FIRMADO EN LIMA EL 7 DE JULIO DE 2005.
D.L. n.º 713, DE FECHA 12 DE JUNIO DE 2014
D.O. No. 125, TOMO No.404 DEL 8 DE JULIO DE 2014
EN VIGENCIA A PARTIR DEL 4 DE JUNIO DE 2015

10. Existe algún acuerdo de cooperación entre El Salvador y proveedores de internet o telefonía celular internacional para el combate de los delitos informáticos. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de Acuerdos bilaterales sobre sobre cooperación en caso de algún Acuerdo de cooperación entre proveedores de internet o telefonía celular internacional para el combate de los delitos informáticos.

11. Existe algún acuerdo de cooperación entre INTERPOL y el Gobierno de El Salvador para compartir información e investigar ciberdelitos o delitos informáticos. Si la respuesta es afirmativa cuales son y emita el texto del mismo (en español) y manifieste si ya entro en vigencia a nivel internacional. No hay registro de algún Acuerdo de Cooperación con INTERPOL para compartir información e investigar ciberdelitos o delitos informáticos.

ANEXO 2: INFORMACION DE FISCALIA GENERAL DE LA REPUBLICA

Fiscalía General de la República
Unidad de Acceso a la Información Pública

Solicitud Nº 207-UAIP-FGR-2020

FISCALÍA GENERAL DE LA REPÚBLICA, UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA. San Salvador, a las catorce horas con diez minutos del día veintidós de julio del año dos mil veinte.

Se recibió con fecha uno de julio del presente año, solicitud de información escrita en esta Unidad, conforme a la Ley de Acceso a la Información Pública (en adelante LAIP), presentada por el ciudadano **LUCIO ALBINO ARIAS LÓPEZ**, con Documento Único de Identidad número cero cero trescientos cuarenta mil cuatrocientos seis guion siete, de la que se hacen las siguientes **CONSIDERACIONES:**

I. De la solicitud presentada, se tiene que el interesado literalmente pide se le proporcione la siguiente información: *"1. Datos estadísticos de denuncias por delitos informáticos (todos los de la Ley Especial de Delitos Informáticos con toda forma de ingresos)*
2. Cantidad de casos judicializados por los delitos la Ley Especial de Delitos Informáticos y las diferentes etapas en que se encuentran (inicial, preliminar o vista pública).
3. Datos estadísticos respecto al número de sentencias absolutorias y condenatorias respecto de casos conforme a la Ley Especial de Delitos Informático.
4. Nombres de las Unidades que conocen de los delitos contemplados en la Ley Especial de Delitos Informáticos y si la misma está centralizada en la Oficina Central o está centralizada en cada Oficina Fiscal a nivel nacional.
5. Qué técnicas de investigación se utilizan para la investigación de delitos informáticos y que unidades Fiscales y Policiales intervienen en la investigación.
6. Que capacitaciones tiene el personal de la institución que conoce de los delitos regulados en la ley especial de delitos informáticos.
7. Que convenios internacionales o interinstitucionales o entes privados (nacionales o internacionales) existen para investigar los delitos contemplados en la ley de delitos informáticos.
Toda la información desagregada por delito a nivel nacional."
Período Solicitado: Desde enero de 2016 hasta junio de 2020.

II. Conforme a los artículos 66 LAIP, 72 y 163 inciso 1° de la Ley de Procedimientos Administrativos (en adelante LPA), se han analizado los requisitos de fondo y forma que debe cumplir la solicitud, verificando que ésta cumple con los requisitos legales, de claridad y precisión; y habiendo el interesado presentado copia de su Documento Único de Identidad, conforme a lo establecido en el artículo 52 del Reglamento LAIP, se continuó con el trámite de su solicitud.

III. Con el objeto de localizar, verificar la clasificación y, en su caso, comunicar la manera en que se encuentra disponible la información, se transmitió la solicitud al Departamento de Estadística, Departamento de Proyectos, a la Escuela de Capacitación Fiscal y a la Unidad Asuntos Legales Internacionales, conforme al artículo 70 LAIP.

IV. Con relación al plazo, se observa que según el detalle de la información solicitada por el peticionario, comprende desde el mes de enero del año 2016 hasta el mes de junio del año 2020, y por el desglose con el que es requerida la información, ha implicado un mayor esfuerzo para la búsqueda, procesamiento y construcción en detalle de los datos requeridos, utilizando para ello mayor cantidad de tiempo y el empleo de más recurso humano; por dichas circunstancias excepcionales se volvió necesario extender el plazo de respuesta de la solicitud a cinco días adicionales, de conformidad a lo dispuesto en el inciso 2º del Art. 71 LAIP.

V. De los requerimientos de información solicitados por el peticionario, se hace necesario realizar un análisis ordenando de los mismos a fin de darle respuesta a su petición y para efecto de fundamentar la decisión de este ente obligado, se procede de la siguiente forma:

1. En relación, a los requerimientos de información consistentes en: "*-Datos estadísticos de denuncias por delitos informáticos (todas los de la Ley Especial de Delitos Informáticos con toda forma de ingresos). -Cantidad de casos judicializados por los delitos la Ley Especial de Delitos Informáticos y las diferentes etapas en que se encuentran (inicial, preliminar o vista pública). -Datos estadísticos respecto al número de sentencias absolutorias y condenatorias respecto de casos conforme a la Ley Especial de Delitos Informático. -Nombres de las Unidades que conocen de los delitos contemplados en la Ley Especial de Delitos Informáticos y si la misma está centralizada en la Oficina Central o está centralizada en cada Oficina Fiscal a nivel nacional. -Que capacitaciones tiene el personal de la institución que conoce de los delitos regulados en la ley especial de delitos informáticos. -Que unidades Fiscales intervienen en la investigación,* es información que esta Institución genera, por lo que es información pública y no se encuentra dentro de ninguna de las causales de reserva previstas en el artículo 19 LAIP, y tampoco es información considerada confidencial de acuerdo con lo establecido en el Art. 24 LAIP, siendo factible su entrega.

2. Sobre los Requerimientos de información en los cuales solicita: ***-Qué técnicas de investigación se utilizan para la investigación de delitos informáticos. -Que unidades Policiales intervienen en la investigación y -Que convenios internacionales existen para investigar los delitos contemplados en la ley de delitos informáticos,*** se hacen las siguientes consideraciones:

   a. El Art. 1 LAIP, define el objeto de la Ley, el cual consiste en garantizar el derecho de acceso de toda persona a la información pública, de lo cual se extrae que la LAIP regula el ejercicio pleno de acceso a la información pública; lo anterior se complementa con lo dispuesto en el Art. 2 LAIP, que dispone que toda persona tiene derecho a solicitar y recibir información generada, administrada o en poder de las instituciones públicas y demás entes obligados; en virtud de lo cual, la Fiscalía General de la República debe garantizarle a los ciudadanos el acceso a la información que genera, administra o tenga en su poder; esto se confirma con lo dispuesto en el Art. 6 Inc. 1º letra "c" LAIP, que expresa que se entiende como información pública aquella en poder de los entes obligados contenida en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio, ya sea impreso, óptico o electrónico, independientemente de su fuente, fecha de elaboración, y que no sea confidencial; además, que dicha información podrá haber sido generada, obtenida, transformada o conservada por éstos a cualquier título.

   b. El literal c) del artículo 50 LAIP, establece como una de las funciones del Oficial de Información el de: "*Auxiliar a los particulares en la elaboración de solicitudes y, en su caso, orientarlos sobre las dependencias o entidades que pudieran tener la información que*

solicitan.", siendo esto aplicable, para aquella información que no es generada o no esta en poder de esta Institución.

c. En ese orden de ideas, sobre el requerimiento consistente en ***Qué técnicas de investigación se utilizan para la investigación de delitos informáticos,*** al realizar un análisis del mismo se puede colegir que el solicitante requiere se le brinden explicaciones sobre las diversas técnicas utilizadas, tomando en cuenta que dicho término es muy amplio, ya que existen infinidad de técnicas que puedan utilizarse en las investigaciones criminales, esto conforme al Principio Procesal de Libertad Probatoria, establecido en el artículo 176 del Código Procesal Penal, en ese sentido, los hechos que surjan de la investigación de cualquier delito pueden probarse por cualquier medio legal de prueba, tal como lo dispone el artículo antes señalado que establece: "*Los hechos y circunstancias relacionados con el delito podrán ser probados por cualquier medio de prueba establecido en este Código y en su defecto, de la manera que esté prevista la incorporación de pruebas similares, siempre que se respeten las garantías fundamentales de las personas consagradas en la Constitución y demás leyes.*"

Razón por la cual, este requerimiento de información solicitado por el peticionario no es factible de proporcionarlo, ya que requieren de una explicación en relación a temas concretos sobre el desarrollo de las investigaciones, en virtud que cada caso tiene sus particularidades en el desarrollo de la investigación, lo que puede conllevar a que en algunos casos se utilicen diversas técnicas y en otros no. En ese sentido, lo peticionado está fuera del alcance de la LAIP, ya que la generación de dichas explicaciones implica la creación de información que existirá al momento de elaborar el documento, ya que dichas explicaciones pueden variar en casos concretos, razón por la que la petición de información del solicitante está fuera del alcance de aplicación de la LAIP. Sobre este punto, el Instituto de Acceso a la Información Pública mediante resolución de referencia NUE 113-A-2016, de fecha veintitrés de mayo de dos mil dieciséis, ha señalado lo siguiente: "*...este Instituto aclara, que los procedimientos de acceso a la información pública sustanciados por las Unidades de Acceso a la Información Pública son para acceder a información generada, administrada o en poder de los entes obligados (Art. 2 de la LAIP), no así para generar información.*"

En razón de lo anterior, se hace de conocimiento al solicitante, que la Fiscalía General de la República cuenta con un servicio de entrevista, por medio del cual el tipo de información requerida puede ser accedida por una vía diferente a la LAIP, ya que se cuenta con un enlace institucional por el que las personas pueden acceder a información aún no generada por este ente obligado; en tal sentido, el interesado puede comunicarse al Departamento de Comunicación Interna de la Fiscalía General de la República, ubicado en Bulevard y Colonia La Sultana, Edificio G-12, Antiguo Cuscatlán, llamando a los teléfonos números 2593-7091, 2593-7000 y 2593-7001, y se le informen los pasos que debe seguir a fin de dirigir su petición a dicho Departamento y gestionar una entrevista con un servidor público conocedor del tema y de esa forma acceder a la información.

d. En cuanto al requerimiento de información consistente en ***Que unidades Policiales intervienen en la investigación,*** la información requerida es generada por una institución diferente a la Fiscalía General de la República, ya que dicha información está directamente vinculada con la Policía Nacional Civil y en vista que dicha Institución conforme su organigrama institucional, posee una Sub Dirección de Investigaciones, la cual esta conformada por varias Divisiones de Investigación, la información requerida, debe ser consultada directamente a la Policía Nacional Civil, por ser esta la que genera la misma. En ese sentido, se concluye que no es la Unidad de Acceso a la Información

Pública de la Fiscalía General de la República, la competente para proporcionar la información que el solicitante requiere, por lo que en virtud de ello es procedente orientar al usuario para que dirija su requerimiento a la Unidad de Acceso a la Información Pública de la Policía Nacional Civil, siendo la dirección de web de dicha Unidad la siguiente: https://transparencia.pnc.gob.sv/ y el correo electrónico oir@pnc.gob.sv.

e. En relación a la petición consistente en ***Que convenios internacionales existen para investigar los delitos contemplados en la ley de delitos informáticos***, se comunica al peticionario que dicha información no es generada ni custodiada por la Fiscalía General de la República, sino más bien, la celebración de los Instrumentos Internacionales corresponde al Órgano Ejecutivo y a la Asamblea Legislativa su ratificación, tal como lo regula la Constitución, ya que en el artículo 168 se regulan las atribuciones y obligaciones del Presidente de la República, estableciendo en el ordinal 4º la de *Celebrar tratados y convenciones internacionales, someterlos a la ratificación de la Asamblea Legislativa, y vigilar su cumplimiento*; asimismo el articulo 131 ordinal 7º de la Carta Magna establece que le corresponde a la Asamblea Legislativa *Ratificar los tratados o pactos que celebre el Ejecutivo con otros Estados u organismos internacionales, o denegar su ratificación;* en ese sentido, el registro sobre la existencia o no de Convenios Internacionales, deberá de obrar en los archivos de dichos Órganos de Estado.

Al respecto, se comunica al peticionario que puede consultar a la Unidad de Acceso a la Información Pública del Ministerio de Relaciones Exteriores, si poseen en sus registros lo solicitado, ya que dicha Institución en la sección Servicios de su Portal de Transparencia señala que posee el servicio de Sistema de Tratados el cual es una herramienta digital que registra los instrumentos jurídicos internacionales, considerados como información pública, que han sido suscritos por el Estado salvadoreño, de forma bilateral y/o multilateral. Dicha plataforma permite consultar los textos de Tratados, Acuerdos, Convenios, Canje de Notas, Convenciones, Memorándum de Entendimiento que se encuentran registrados en el archivo de la Dirección General de Asuntos Jurídicos, dependencia encargada de la conservación y custodia de tales Instrumentos. La dirección web del Portal de Transparencia de dicho Ministerio es https://www.transparencia.gob.sv/institutions/rree y el correo electrónico el siguiente oaip@rree.gob.sv. Asimismo, puede consultar en la Unidad de Acceso a la Información Pública de la Asamblea Legislativa, si poseen registros de lo requerido. La dirección web del Portal de Transparencia de dicha Institución es https://transparencia.asamblea.gob.sv/ y el correo electrónico el siguiente oficial.informacion@asamblea.gob.sv.

3. En cuanto al requerimiento de información consistente en ***"Que convenios interinstitucionales o entes privados (nacionales o internacionales) existen para investigar los delitos contemplados en la ley de delitos informáticos"***, se comunica al peticionario, que de conformidad con el trámite que establece la LAIP y con el objeto de localizar, verificar la clasificación y, en su caso, comunicar la manera en que se encuentra disponible la información, se transmitió la solicitud al área correspondiente, conforme al artículo 70 LAIP, obteniendo como respuesta que dentro de los archivos institucionales, no se encuentra documento alguno en el que conste un Convenio interinstitucional *o entes privados (nacionales o internacionales)* para investigar los delitos contemplados en la ley de delitos informáticos. En ese sentido, de conformidad con lo dispuesto en el Art. 2, en relación con el Art. 6 letra "c" y 73 todos LAIP, en el presente caso, la información requerida es inexistente.

Sobre este punto, el Instituto de Acceso a la Información Pública mediante resolución de referencia NUE 113-A-2016 de fecha veintitrés de mayo de dos mil dieciséis, ha señalado lo siguiente: *"este Instituto aclara, que los procedimientos de acceso a la información pública sustanciados por las Unidades de Acceso a la Información Pública, son para acceder a información generada, administrada o en poder de los entes obligados (Art. 2 de la LAIP), no así para generar información."* En ese sentido, la LAIP no faculta a los entes obligados a entregar información que no haya sido generada, administrada o no esté en poder de las instituciones públicas.

POR TANTO, en razón de lo anterior, con base en los artículos 131 ordinal 7ª y 168 ordinal 4ª de la Constitución, 1, 2, 6, 50, 62, 65, 66, 68, 70, 71, 72 y 73 todos de la LAIP, 72 y 163 inciso 1° LPA, 176 del Código Procesal Penal se **RESUELVE:**

A) **REORIENTAR**, al peticionario para que pueda acceder a la información sobre ***-Qué técnicas de investigación se utilizan para la investigación de delitos informáticos. -Que unidades Policiales intervienen en la investigación y -Que convenios internacionales existen para investigar los delitos contemplados en la ley de delitos informáticos,*** de la manera en que le ha sido expresado en el Romano V, numeral 2 de la presente resolución.

B) **ES INEXISTENTE,** la información referente a ***"Que convenios interinstitucionales o entes privados (nacionales o internacionales) existen para investigar los delitos contemplados en la ley de delitos informáticos"***.

C) **CONCEDER EL ACCESO A LA INFORMACIÓN,** respecto a los requerimientos consistentes en *Datos estadísticos de denuncias por delitos informáticos (todos los de la Ley Especial de Delitos Informáticos con toda forma de ingresos). -Cantidad de casos judicializados por los delitos la Ley Especial de Delitos Informáticos y las diferentes etapas en que se encuentran (inicial, preliminar o vista pública). -Datos estadísticos respecto al número de sentencias absolutorias y condenatorias respecto de casos conforme a la Ley Especial de Delitos Informático. -Nombres de las Unidades que conocen de los delitos contemplados en la Ley Especial de Delitos Informáticos y si la misma está centralizada en la Oficina Central o está centralizada en cada Oficina Fiscal a nivel nacional. -Que capacitaciones tiene el personal de la institución que conoce de los delitos regulados en la ley especial de delitos informáticos. -Que unidades Fiscales intervienen en la investigación,* por medio de las siguientes respuestas:

1. **DATOS ESTADÍSTICOS DE DENUNCIAS POR DELITOS INFORMÁTICOS (TODOS LOS DE LA LEY ESPECIAL DE DELITOS INFORMÁTICOS CON TODA FORMA DE INGRESOS)**

   R/ La información que se brinda corresponde a la cantidad de casos ingresados por todas las formas de ingreso, por los delitos y periodo requerido

CANTIDAD DE CASOS POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO Y AÑO.						
DELITOS		Año 2016	Año 2017	Año 2018	Año 2019	Año 2020
Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Acceso indebido a sistemas informáticos (4 L.D. Informáticos)	1	6	7	19	5
	Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	3	8	5	7	6
	Interferencia del sistema informático (6 L.D. Informáticos)	0	3	1	2	1
	Daños a sistemas informáticos (7 L.D. Informáticos)	1	2	3	1	3
	Posesión de equipos o prestación de servicios para la vulneración de la seguridad (8 L.D. Informáticos)	1	0	0	2	0
	Violación de la seguridad de sistemas (9 L.D. Informáticos)	0	2	4	6	1
	Estafa informática (10 L.D. Informáticos)	0	6	7	24	17
	Estafa informática (10 Lit. a. L.D. Informáticos)	1	1	0	0	1
	Estafa informática (10 Lit. c. L.D. Informáticos)	1	0	0	0	0
	Fraude informático (11 L.D. Informáticos)	2	6	7	9	6
	Espionaje informático (12 L.D. Informáticos)	2	0	2	6	0
	Hurto por medios informáticos (13 L.D. Informáticos)	7	8	17	46	24
	Manipulación de registros (15 L.D. Informáticos)	0	0	0	3	1
	Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	4	7	17	16	13
	Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	3	3	10	11	6
	Alteración, daño a la integridad o disponibilidad de los datos (19 L.D. Informáticos)	2	3	2	5	5
	Intercepción de transmisiones entre sistemas de las TIC (21 L.D. Informáticos)	2	0	0	1	0
	Hurto de identidad (22 L.D. Informáticos)	19	44	81	124	73
	Divulgación no autorizada (23 L.D. Informáticos)	1	5	17	51	10
	Utilización de datos personales (24 L.D. Informáticos)	19	32	50	59	25
	Obtención y transferencia de información de carácter confidencial (25 L.D. Informáticos)	1	2	1	0	0

1. **DATOS ESTADÍSTICOS DE DENUNCIAS POR DELITOS INFORMÁTICOS (TODOS LOS DE LA LEY ESPECIAL DE DELITOS INFORMÁTICOS CON TODA FORMA DE INGRESOS)**

R/ La información que se brinda corresponde a la cantidad de casos ingresados por todas las formas de ingreso, por los delitos y periodo requerido

CANTIDAD DE CASOS POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO Y AÑO.						
DELITOS		Año 2016	Año 2017	Año 2018	Año 2019	Año 2020
Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Acceso indebido a sistemas informáticos (4 L.D. Informáticos)	1	6	7	19	5
	Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	3	8	5	7	6
	Interferencia del sistema informático (6 L.D. Informáticos)	0	3	1	2	1
	Daños a sistemas informáticos (7 L.D. Informáticos)	1	2	3	1	3
	Posesión de equipos o prestación de servicios para la vulneración de la seguridad (8 L.D. Informáticos)	1	0	0	2	0
	Violación de la seguridad de sistemas (9 L.D. Informáticos)	0	2	4	6	1
	Estafa informática (10 L.D. Informáticos)	0	6	7	24	17
	Estafa informática (10 Lit. a. L.D. Informáticos)	1	1	0	0	1
	Estafa informática (10 Lit. c. L.D. Informáticos)	1	0	0	0	0
	Fraude informático (11 L.D. Informáticos)	2	6	7	9	6
	Espionaje informático (12 L.D. Informáticos)	2	0	2	6	0
	Hurto por medios informáticos (13 L.D. Informáticos)	7	8	17	46	24
	Manipulación de registros (15 L.D. Informáticos)	0	0	0	3	1
	Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	4	7	17	16	13
	Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	3	3	10	11	8
	Alteración, daño a la integridad o disponibilidad de los datos (19 L.D. Informáticos)	2	3	2	5	5
	Intercepción de transmisiones entre sistemas de las TIC (21 L.D. Informáticos)	2	0	0	1	0
	Hurto de identidad (22 L.D. Informáticos)	19	44	81	124	73
	Divulgación no autorizada (23 L.D. Informáticos)	1	5	17	51	10
	Utilización de datos personales (24 L.D. Informáticos)	19	32	50	59	25
	Obtención y transferencia de información de carácter confidencial (25 L.D. Informáticos)	1	2	1	0	0

2. CANTIDAD DE CASOS JUDICIALIZADOS POR LOS DELITOS LA LEY ESPECIAL DE DELITOS INFORMÁTICOS Y LAS DIFERENTES ETAPAS EN QUE SE ENCUENTRAN (INICIAL, PRELIMINAR O VISTA PÚBLICA).

CANTIDAD DE CASOS POR ETAPA DEL PROCESO PENAL (AUDIENCIA INICIAL, AUDIENCIA PRELIMINAR Y VISTA PÚBLICA), POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, ETAPA Y AÑO.

AÑO	DELITOS		Audiencia Inicial/Imposición de Medidas	Audiencia Preliminar/Audiencia Preparatoria	Vista Pública/Vista de la Causa	Total
Año 2016	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Estafa informática (10 Lit. a. L.D. Informáticos)	1	0	0	1
		Hurto por medios informáticos (13 L.D. Informáticos)	2	0	0	2
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	2	0	0	2
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	1	0	0	1
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D. Informáticos)	0	1	0	1
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	2	0	0	2
		Total	8	1	0	9
Año 2017	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	1	0	0	1
		Estafa informática (10 Lit. a. L.D. Informáticos)	0	1	0	1
		Estafa informática (10 Lit. c. L.D. Informáticos)	1	0	0	1
		Hurto por medios informáticos (13 L.D. Informáticos)	3	2	0	5
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	2	2	0	4
		Utilización de datos personales (24 L.D. Informáticos)	1	0	0	1
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	3	0	1	4
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	5	1	0	6
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D. Informáticos)	4	1	2	7
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	4	2	1	7

CANTIDAD DE CASOS POR ETAPA DEL PROCESO PENAL (AUDIENCIA INICIAL, AUDIENCIA PRELIMINAR Y VISTA PÚBLICA), POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, ETAPA Y AÑO.						
AÑO	DELITOS		Audiencia Inicial/Imposición de Medidas	Audiencia Preliminar/Audiencia Preparatoria	Vista Pública/Vista de la Causa	Total
		Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	3	1	0	4
		Pornografía a través de las TIC agravada (28 y 33 L.D. Informáticos)	0	1	0	1
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC agravada (30 y 33. L.D. Informáticos)	0	1	0	1
		Total	27	12	4	43
Año 2018	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Daños a sistemas informáticos (7 L.D. Informáticos)	0	1	0	1
		Posesión de equipos o prestación de servicios para la vulneración de la seguridad (8 L.D. Informáticos)	0	1	0	1
		Estafa informática (10 L.D. Informáticos)	1	0	0	1
		Hurto por medios informáticos (13 L.D. Informáticos)	4	1	1	6
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	5	2	1	8
		Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	1	0	0	1
		Hurto de identidad (22 L.D. Informáticos)	2	0	0	2
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	2	2	1	5
		Acoso a través de TIC (27 L.D. Informáticos)	3	1	1	5
		Pornografía a través de TIC (28 L.D. Informáticos)	1	0	0	1
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	2	5	5	12
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D. Informáticos)	7	6	5	18
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	2	8	3	13
		Acoso a NNA o personas con discapacidad a través del	1	2	2	5

CANTIDAD DE CASOS POR ETAPA DEL PROCESO PENAL (AUDIENCIA INICIAL, AUDIENCIA PRELIMINAR Y VISTA PÚBLICA), POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, ETAPA Y AÑO.

AÑO	DELITOS		Audiencia Inicial/Imposición de Medidas	Audiencia Preliminar/Audiencia Preparatoria	Vista Pública/Vista de la Causa	Total
		uso de las TIC (32 L.D. Informáticos)				
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC agravada (31 y 33 L.D. Informáticos)	0	1	0	1
		Acoso a NNA o personas con discapacidad a través del uso de las TIC agravada (32 y 33 L.D. Informáticos)	1	0	0	1
		Total	32	30	19	81
Año 2019	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Acceso indebido a sistemas informáticos (4 L.D. Informáticos)	1	0	0	1
		Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	0	1	0	1
		Posesión de equipos o prestación de servicios para la vulneración de la seguridad (8 L.D. Informáticos)	1	0	0	1
		Estafa informática (10 L.D. Informáticos)	1	0	0	1
		Estafa informática (10 Lit. c. L.D. Informáticos)	0	1	0	1
		Hurto por medios informáticos (13 L.D. Informáticos)	0	2	0	2
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	0	3	0	3
		Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	0	1	0	1
		Hurto de identidad (22 L.D. Informáticos)	0	1	1	2
		Utilización de datos personales (24 L.D. Informáticos)	0	1	0	1
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	10	1	3	14
		Acoso a través de TIC (27 L.D. Informáticos)	2	1	2	5
		Pornografía a través de TIC (28 L.D. Informáticos)	0	2	1	3
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	1	3	4
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30	2	2	6	10

CANTIDAD DE CASOS POR ETAPA DEL PROCESO PENAL (AUDIENCIA INICIAL, AUDIENCIA PRELIMINAR Y VISTA PÚBLICA), POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, ETAPA Y AÑO.

AÑO	DELITOS		Audiencia Inicial/Imposición de Medidas	Audiencia Preliminar/Audiencia Preparatoria	Vista Pública/Vista de la Causa	Total
		L.D. Informáticos)				
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	0	2	3	5
		Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	2	1	1	4
		Pornografía a través de las TIC agravada (28 y 33 L.D. Informáticos)	0	1	0	1
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC agravada (31 y 33 L.D. Informáticos)	1	0	1	2
		Acoso a NNA o personas con discapacidad a través del uso de las TIC agravada (32 y 33 L.D. Informáticos)	0	1	0	1
		Total	20	22	21	63
Año 2020	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Hurto por medios informáticos (13 L.D. Informáticos)	1	0	0	1
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	2	1	1	4
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	2	1	1	4
		Acoso a través de TIC (27 L.D. Informáticos)	2	0	1	3
		Pornografía a través de TIC (28 L.D. Informáticos)	0	0	1	1
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	1	0	1
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D. Informáticos)	1	0	0	1
		Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	2	0	0	2
		Total	10	3	4	17
TOTAL GENERAL			97	68	48	213

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 05072020
Nota: Los datos entregados son independientes a la fecha de inicio del caso.

3. DATOS ESTADÍSTICOS RESPECTO AL NÚMERO DE SENTENCIAS ABSOLUTORIAS Y CONDENATORIAS RESPECTO DE CASOS CONFORME A LA LEY ESPECIAL DE DELITOS INFORMÁTICOS.

R// La información que se entrega corresponde a la cantidad de casos con resultados absolutorios y condenatorios, por los delitos regulados en la Ley Especial contra Delitos Informáticos y Conexos; la cual es independiente a la fecha de inicio del caso. Aclarándose que las condenas y las absoluciones comprenden las Sentencias y los Procedimientos Abreviados.

CANTIDAD DE CASOS CON RESULTADOS ABSOLUTORIOS Y CONDENATORIOS, POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, RESULTADO Y AÑO.

RESULTADO	DELITOS		Año 2017	Año 2018	Año 2019	Año 2020
Absoluciones	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	0	0	0	1
		Hurto de identidad (22 L.D. Informáticos)	0	0	1	0
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	0	1	1	0
		Acoso a través de TIC (27 L.D. Informáticos)	0	0	1	0
		Pornografía a través de TIC (28 L.D. Informáticos)	0	0	0	1
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	3	0	0
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D Informáticos	1	1	1	0
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	2	1	1	0
		Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	0	1	0	0
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC agravada (31 y 33 L.D. Informáticos)	0	0	1	0
		Total	**3**	**7**	**6**	**2**
Condenas	Ley Especial de Contra Delitos informáticos y Conexos (LEDIC)	Hurto por medios informáticos (13 L.D. Informáticos)	0	1	0	0
		Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	0	1	0	1
		Hurto de identidad (22 L.D. Informáticos)	0	0	1	0
		Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	1	1	2	2
		Acoso a través de TIC (27 L.D. Informáticos)	0	1	1	1

CANTIDAD DE CASOS CON RESULTADOS ABSOLUTORIOS Y CONDENATORIOS, POR TODOS LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS (LEDIC), A NIVEL NACIONAL, DEL AÑO 2016 HASTA JUNIO 2020; DETALLADO POR DELITO, RESULTADO Y AÑO.						
RESULTADO	DELITOS		Año 2017	Año 2018	Año 2019	Año 2020
		Pornografía a través de TIC (28 L.D. Informáticos)	0	0	1	0
		Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	3	3	0
		Adquisición o posesión de material pornográfico de NNA o personas con discapacidad a través del uso de las TIC (30 L.D Informáticos	1	5	6	0
		Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	0	3	2	0
		Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	0	1	2	0
		Pornografía a través de las TIC agravada (28 y 33 L.D. Informáticos)	0	0	1	0
		Acoso a NNA o personas con discapacidad a través del uso de las TIC agravada (32 y 33 L.D. Informáticos)	0	0	1	0
		Total	**2**	**16**	**20**	**4**
TOTAL GENERAL			**5**	**23**	**26**	**6**

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 05072020
Nota: Los datos entregados son independientes a la fecha de inicio del caso.

4. NOMBRES DE LAS UNIDADES QUE CONOCEN DE LOS DELITOS CONTEMPLADOS EN LA LEY ESPECIAL DE DELITOS INFORMÁTICOS Y SI LA MISMA ESTÁ CENTRALIZADA EN LA OFICINA CENTRAL O ESTÁ CENTRALIZADA EN CADA OFICINA FISCAL A NIVEL NACIONAL.

5. QUE UNIDADES FISCALES INTERVIENEN EN LA INVESTIGACIÓN

R//La Institución no cuenta con una Unidad Organizativa ni fiscales auxiliares nombrados exclusivamente para conocer de la investigación y procesamiento de los delitos contenidos en la Ley Especial de Delitos Informáticos y Conexos. Por lo que cada Oficina Fiscal, dependiendo de la naturaleza de cada denuncia, decide que Unidad conocerá la investigación, de conformidad al Art. 193 de la Constitución de la República.

6. QUE CAPACITACIONES TIENE EL PERSONAL DE LA INSTITUCIÓN QUE CONOCE DE LOS DELITOS REGULADOS EN LA LEY ESPECIAL DE DELITOS INFORMÁTICOS.

R// Conforme a la respuesta brindada en los numerales 4 y 5, en el cual se comunicó que no existe personal asignado exclusivamente para la investigación de delitos informáticos, la información que se proporciona a continuación, corresponde a las actividades formativas que ha recibido el personal de la Fiscalía General de la República en general, en relación a los delitos regulados en la Ley Especial de Delitos Informáticos y Conexos.

CAPACITACIONES AL PERSONAL DE LA FISCALÍA GENERAL DE LA REPÚBLICA EN RELACIÓN A DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMATIVOS Y CONEXOS ENERO DEL AÑO 2016 - JUNIO DEL AÑO 2020			
Año	**Actividad**	**Inicio**	**Fin**
2016	CURSO CIBER CRIMEN Y EVIDENCIA DIGITAL	05/04/2016	07/04/2016
2016	CURSO CIBER CRIMEN Y EVIDENCIA DIGITAL	20/04/2016	22/04/2016
2016	CURSO CIBER CRIMEN Y EVIDENCIA DIGITAL	27/04/2016	29/04/2016
2016	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	22/06/2016	24/06/2016
2016	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	05/07/2016	07/07/2016
2016	TALLER DE FORMACION METODOLOGICA EN LA IMPLEMENTACION DEL MODULO CIBER CRIMEN EN LA NIÑEZ Y LA ADOLESCENCIA	18/07/2016	18/07/2016
2016	CURSO SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION	27/07/2016	28/07/2016
2016	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	19/09/2016	23/09/2016
2016	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	10/10/2016	14/10/2016
2016	CURSO CIBER CRIMEN EN CONTRA DE SISTEMAS, DATOS INFORMATICOS Y OTROS BIENES JURIDICOS	17/10/2016	21/10/2016
2016	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	24/10/2016	28/10/2016
2016	CURSO CIBER CRIMEN EN CONTRA DE SISTEMAS, DATOS INFORMATICOS Y OTROS BIENES JURIDICOS	07/11/2016	11/11/2016
2017	TALLER ANALISIS JURIDICO DE LOS DELITOS INFORMATICOS CONTRA NIÑA, NIÑO, ADOLESCENTE O PERSONAS CON DISCAPACIDAD	28/03/2017	28/03/2017
2017	CURSO CIBER CRIMEN EN LA NIÑEZ Y ADOLESCENCIA	03/04/2017	07/04/2017
2017	CURSO CIBER CRIMEN EN CONTRA DE SISTEMAS, DATOS INFORMATICOS Y OTROS BIENES JURIDICOS	24/04/2017	28/04/2017

ANEXO 3: INFORMACION DE LA CORTE SUPREMA DE JUSTICIA

Órgano Judicial
Corte Suprema de Justicia
Unidad de Asesoría Técnica Internacional

UATI No. 219 / 2020

MEMORANDO

Para: **Licenciada María Soledad Rivas de Avendaño**
Secretaria General

Licenciado Giovanni Alberto Rosales Rosagni
Oficial de Información Interino-Unidad de Acceso a la Información Pública

C.C: **Doctor José Oscar Armando Pineda Navas**
Presidente

De: **Licenciado Mario Gustavo Torres Aguirre**
Jefe interino de la Unidad de Asesoría Técnica Internacional

Asunto: Informe convenios, acuerdos o colaboración recibida sobre delitos informáticos

Fecha: 10 de agosto de 2020

Me refiero a la solicitud de información de parte de Secretaria General, marginada al suscrito por el Despacho de la Presidencia de esta Corte, así como a memorando UAIP/496ac497/823/2020(4), procedente de la Unidad de Acceso a la Información Pública, ambos relacionados entre sí por tratarse de requerimiento de información sobre acuerdos, convenios o colaboración recibida de un organismo relacionada con delitos informáticos, dentro del periodo que abarca desde el año 2016 a la fecha.

Sobre el particular debo informar, que en los registros y base de datos que lleva esta Unidad -desde el año 1991 a la fecha- no existe convenio o acuerdo de cooperación para el intercambio de información en casos de delitos informáticos que haya sido suscrito por este Órgano de Estado con proveedores de internet o telefonía celular de nuestro país, ni tampoco existe en los registros, ningún acuerdo o convenio suscrito con otro órgano judicial.

De igual manera, no se registra ningún convenio o acuerdo mediante el cual se haya recibido colaboración sobre delitos informáticos, de parte de la Oficina de las Naciones Unidas para las Drogas y el Delito, relacionado a donación de equipo informático, capacitación, material bibliográfico o software para facilitar peritajes y demostrar objetivamente la realización de delitos informáticos.

Hago propicia la ocasión para reiterar a Usted las muestras de mi consideración.

Atentamente,

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
CORTE SUPREMA DE JUSTICIA
Nombre:
Fecha: 11-08-2020 Hora: 11:17
RECIBIDO

Corte Suprema de Justicia

Secretaría General

Memorándum

Para: ***Lic. Giovanni Alberto Rosales Rosagni***
Oficial de Información del Órgano Judicial

De: ***Licda. María Soledad Rivas de Avendaño***
Secretaria General

Asunto: ***Informe sobre requerimiento de información***

Fecha: ***31 de julio de 2020***

No. SG-GR-294-20

Cordialmente, me refiero al memorándum UAIP/496ac497/844/2020(4), de fecha 28 de los corrientes, con el cual esa Unidad trasladó requerimiento de información sobre la existencia de algún acuerdo de cooperación entre esta Corte y proveedores de internet o telefonía celular de nuestro país, para el combate de delitos informáticos, o un acuerdo de cooperación internacional entre esta Corte y otros órganos judiciales de otros países, para cooperar en el intercambio de información en casos de dicha clase de delitos.

Al respecto, informar que esta Secretaría no cuenta con la información requerida. Sin embargo, tratándose de una solicitud de supuestos acuerdos de cooperación, sugiero realizar consulta en la Presidencia de esta Corte.

Sin más que informar sobre el particular, me suscribo.

Atentamente.

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
CORTE SUPREMA DE JUSTICIA
Nombre: N
Fecha: 31-7-2020 Hora: 14:35
RECIBIDO

MEMORÁNDUM

CORTE SUPREMA DE JUSTICIA

DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMACIÓN - GGAF

Para: Lcdo. Giovanni Alberto Rosales Rosagni
Oficial de Información Interino del Órgano Judicial

De: Ing. Aníbal Miguel Berdugo Vidaurre
Director
Dirección de Desarrollo Tecnológico e Información GGAF

Asunto: Respuesta a requerimiento UAIP/496ac497/874/2020(4)

Fecha: 13/08/2020 **Ref. ext DDTI-1272-2020 lmg**

De acuerdo a la información solicitada en requerimiento UAIP/496ac497/874/2020(4), con respecto a lo siguiente:

a) Si la Corte Suprema de Justicia tiene una Unidad o un área especializada para pericias informáticas ordenadas por los tribunales nacionales que cuente con peritos permanentes que brinden o realicen pericias objetivas con relación a esclarecer si se han cometido delitos informáticos y si la hay cual es el número de plazas de peritos existentes en la misma; b) en caso de existir peritos permanentes informáticos requiero el perfil técnico de los mismos, es decir, que formación básica han tenido, que cursos de capacitación han recibido en el área o maestrías para ejercer su labor…".

Le hago del conocimiento que dentro de los registros de la Dirección de Desarrollo Tecnológico e Información -DDTI- no se cuenta con personal que tengan la función de peritos, ni existen plazas dentro de la DDTI con ese perfil. Desconocemos si dentro de la Institución exista un área especializada para pericias informáticas que cuente con peritos permanentes o plazas de peritos.

Por lo anterior, sería recomendable se consulte al área responsable de la contratación del personal de la Institución, Dirección de Talento Humano Institucional, para verificar la existencia o no de plazas con el perfil mencionado. Así como a la Dirección de Planificación Institucional para que corrobore la existencia o no de alguna unidad organizativa especializada para pericias informáticas ordenadas por los tribunales nacionales que cuente con peritos permanentes.

Atentamente,

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
CORTE SUPREMA DE JUSTICIA
Nombre:
Fecha: 13 AGO 2020 Hora: 2:43 hrs
RECIBIDO

CORTE SUPREMA DE JUSTICIA
DIRECCIÓN DE TALENTO HUMANO INSTITUCIONAL
MEMORANDUM

PARA:	**Lic. Giovanni Alberto Rosales Rosagni** Oficial de Información del órgano Judicial Interino
CC.:	**Lic.: José Adalberto Chávez** Gerente General de Administración y Finanzas
DE:	**Licda. Carlina de Jovel** Directora Interina
ASUNTO:	Respuesta
FECHA:	11 de agosto de 2020

Ref. DTHI-UATA(RAIP)-1189ª-08-2020

Atentamente, conforme a solicitud efectuada en nota con referencia MEMO UAIP/496ac497/845-2020(4) en la que solicita información relativa a lo siguiente:

"Información de la Institución en el período comprendido entre enero 2016 a junio 2020".
[...] 6. Existe en el Órgano Judicial alguna Unidad que tenga peritos especializados que colaboren con su saber en los procesos por delitos informáticos. Si los hay Cuál es su especialidad y donde han sido formados en ellas" [sic].
En ese sentido, para dar cumplimiento al artículo 70 de la Ley de Acceso a la Información Pública, conforme a los registros con los que cuenta esta Dirección por medio de la Unidad de Recursos Humanos y la Unidad Técnica Central, en nuestra estructura organizativa no existe Unidad a Área especializada en materia de delitos informáticos.

Sin otro particular,

Atentamente.

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
CORTE SUPREMA DE JUSTICIA
Nombre:
11-08-2020
Fecha: Hora: 11:50
RECIBIDO

INSTITUTO DE MEDICINA LEGAL
"DR. ROBERTO MASFERRER"
SAN SALVADOR, EL SALVADOR
Tels. 2529-8602, 2529-8604

CORTE SUPREMA DE JUSTICIA
SAN SALVADOR, EL SALVADOR

MEMORANDUM

Ref.DGIE-IML-139-2020

Para:	**Lic. Giovanni Alberto Rosales Rosagni** Oficial de la Información Interina – Órgano Judicial.
De:	**Dr. Pedro Hernán Martínez Vásquez** Director del Instituto de Medicina Legal "Dr. Roberto Masferrer".
Asunto:	**Respuesta a Ref. UAIP-496ac497-824-2020(4)**
Fecha:	**30 de Julio de 2020.**

En relación a oficio Ref. UAIP-496ac497-824-2020(4), de fecha 28 de julio de 2020 en la que requiere información en el periodo comprendido de enero 2016 junio 2020, según siguiente detalle:

"Existe en el Órgano Judicial alguna unidad que tenga peritos especializados que colaboren con su saber en los procesos por delitos de informáticos. Si los hay, cuál es su especialidad y donde han sido formados en ella."

Informo a usted que a la fecha el Instituto de Medicina Legal no cuenta dentro de su organización interna con un departamento con peritos especializados en el área de experticias para esclarecer delitos informáticos; ya que esa especialidad no es un área que le competa al Instituto dentro de sus funciones efectuar.

Me suscribo atentamente.

Atte.

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
CORTE SUPREMA DE JUSTICIA
Nombre:
Fecha: 30 JUL 2020 Hora: 14:42
RECIBIDO

CC. Archivo.
JPV/2020

ANEXO 4: INFORMACIÓN DEL CNJ

CONSEJO NACIONAL DE LA JUDICATURA

UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA

Ref. UAIP / No 09 / 2020

En cumplimiento de lo que ordena el Art. 66 de la Ley de Acceso a la Información Pública en su inciso último y lo que complementa el Art.53 del Reglamento de citada normativa, SE HACE CONSTAR QUE: en esta fecha, veintidós de julio de dos mil veinte, se da por recibida la solicitud de información interpuesta en esta Unidad por el Licenciado Lucio Albino Arias López, quien se identifica con su Documento Único de Identidad número cero cero tres cuatro cero cuatro cero seis – siete y en la que solicita la siguiente información:

"Que con motivo de estar realizando una investigación Documental para ser presentada como trabajo de TESIS de Maestría, me es indispensable información de vuestra institución del periodo comprendido de enero 2016 Junio 2020, según el siguiente detalle:

1) Cantidad de capacitaciones a nivel NIVEL NACIONAL han recibido los jueces de Sentencia, Instrucción y de Paz sobre Delitos informáticos y sobre la ley Delitos contemplados en la Ley Especial contra los delitos informáticos y conexos.

2) Cantidad de Jueces A NIVEL NACIONAL capacitados sobre investigación de Delitos contemplados en la Ley Especial contra los delitos informáticos y conexos.

3) Nombres y contendidos temáticas de las capacitaciones sobre delitos informáticos, ciberdelincuencia e investigación de la misma ha brindado el CNJ a los jueces.

4) Nombres y contendidos temáticas de las capacitaciones sobre delitos informáticos, ciberdelincuencia e investigación de la misma ha brindado el CNJ a los Procuradores y/o abogados en libre ejercicio, así como cantidad de asistentes a las mismas.

5) Existe algún material escrito o publicación por parte del CNJ que contenga las nociones básicas de los delitos informáticos y su forma de investigación.

6) La Oficina de Naciones Unidas para las drogas y el Delito ha colaborado con la CNJ en la temática de los delitos informáticos y su investigación. Si la respuesta es afirmativa en que ha consistido dicha colaboración."

El plazo para dar respuesta a esta solicitud, de conformidad con el Art. 71 de la Ley de Acceso a la Información no será mayor de diez días, hábiles contados a partir de la fecha de recibida, a menos que por la complejidad de la documentación que contenga la información solicitada se requiera del plazo adicional prescrito en el mismo artículo.

Queda registrada con la Ref. UAIP / No 09 / 2020 la solicitud cuya interposición se hace constar.

Lic. José Manuel Archila
Oficial de Información

Escuela de Capacitación Judicial
Dr. "Arturo Zeledón Castrillo"

Memorándum

ECJ- D-M-152/2020

Para: **Lic. José Manuel Archila**
Oficial de Información UAIP

De: **Dania Elena Tolentino Membreño, LLM, Msc.**
Directora de la Escuela de Capacitación Judicial

Asunto: Remisión de información requerida

Fecha: 13 de agosto 2020

En atención a su Memorándum Ref. UAIP/ECJ/52/2020 de fecha 23/7/2020, remito la información requerida:

1) Cantidad de capacitaciones a nivel nacional, que han recibido los jueces de Sentencia, Instrucción y de Paz, sobre Delitos informáticos y sobre la ley de Delitos contemplados en la Ley Especial contra los delitos informáticos y conexos: **R/ 3**

2) Cantidad de Jueces a Nivel Nacional capacitados sobre investigación de Delitos contemplados en la Ley Especial contra los delitos informáticos y conexos: **R/ 63**

   Nombres y contenidos temáticos de las capacitaciones sobre delitos informáticos, ciberdelincuencia e investigación que la misma ha brindado a los jueces: **R/ 11438 – "Análisis de Estados Financieros para Indagación en Delitos de Corrupción y Conexos"; 1197 – "Los Delitos Cometidos a través de Nuevas Tecnologías en la Ley Especial contra los Delitos Informáticos y Conexos"**; cuyo contenido es el siguiente:

   a) Estructura de la ley
   b) La Competencia y la Jurisdicción
   c) Protección y Seguridad Informática
   d) Fraudes informáticos
   e) Delitos informáticos contra Niños, Niñas y Adolescentes y personas con Capacidades Alternas
   f) Problemas de Persecución Penal
   g) La Computación Forense en la Investigación de los Tipos Penales insertos en la Ley
   h) La Evidencia Digital
   i) La Prueba Informática
   j) Autenticación de la Prueba Informática
   k) La Cadena de Custodia.

Escuela de Capacitación Judicial
Dr. "Arturo Zeledón Castrillo"

Memorándum

3) Nombres y contenidos temáticos de las capacitaciones sobre delitos informáticos, ciberdelincuencia e investigación de la misma, que ha brindado el CNJ a los Procuradores y/o Abogados en Libre Ejercicio, así como la cantidad de asistentes a las mismas. **R/ No se ha brindado capacitaciones en este tema a Procuradores ni a Abogados en el libre ejercicio.**

4) Existe algún material escrito o publicación por parte del CNJ que contenga las nociones básicas de los delitos informáticos y su forma de investigación. **R/ Todos los funcionarios judiciales, secretarios/as, colaboradores/as judiciales y otros operadores del sector de justicia, que han recibido las diferentes capacitaciones con los temas relacionados a la Ley Especial contra los delitos informáticos y conexos, cuentan con el material de apoyo sobre los contenidos de la actividad formativa. Publicación a esta fecha aún no existe.**

5) La oficina de Naciones Unidas para la Droga y el Delito ha colaborado con el CNJ en la temática de los delitos informáticos y su investigación. Si la respuesta es afirmativa, ¿En qué ha consistido dicha colaboración? **R/ La Oficina de las Naciones Unidas contra la Droga y el Delito desde el año 2019, ha brindado acompañamiento técnico a la ECJ asignando a dos especialistas para la actividad formativa presencial denominada "Ciberdelito y Evidencia Digital"; asimismo para el webinario denominado "Cibercrimen en tiempos de Pandemia", de fecha 21/07/2020.**

Cordialmente,