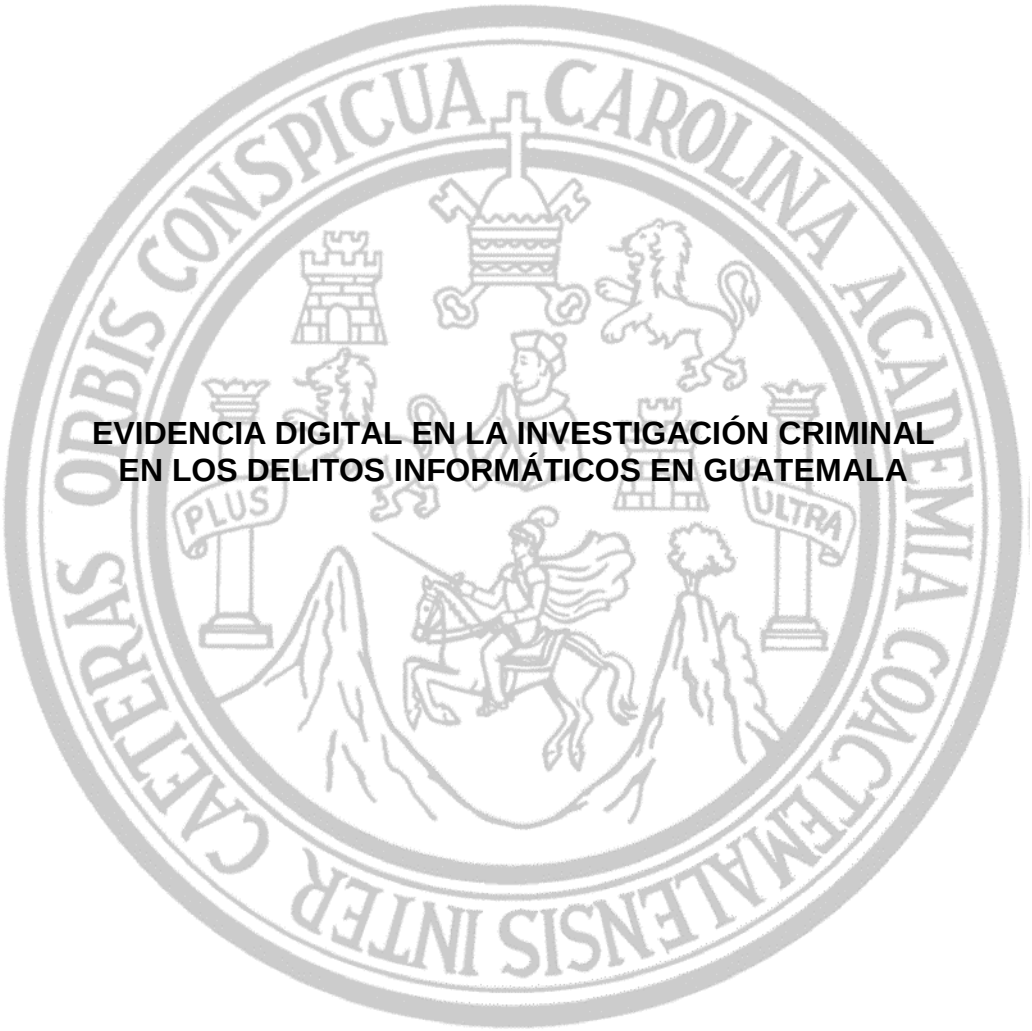
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN DERECHO PENAL



EVIDENCIA DIGITAL EN LA INVESTIGACIÓN CRIMINAL EN LOS DELITOS INFORMÁTICOS EN GUATEMALA

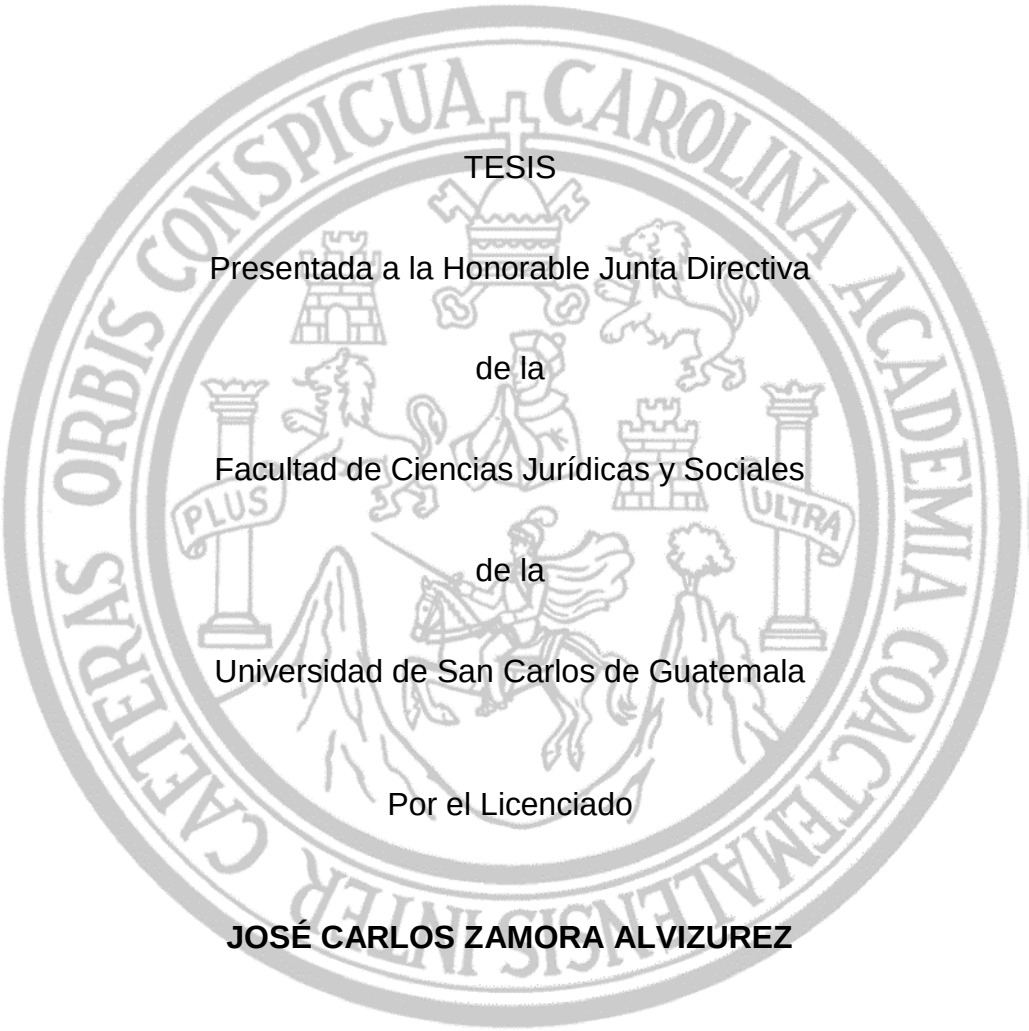
LICENCIADO

JOSÉ CARLOS ZAMORA ALVIZURES

GUATEMALA, ENERO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN DERECHO PENAL

EVIDENCIA DIGITAL EN LA INVESTIGACIÓN CRIMINAL EN LOS DELITOS INFORMÁTICOS EN GUATEMALA



TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por el Licenciado

JOSÉ CARLOS ZAMORA ALVIZUREZ

Previo a conferírsele el Grado Académico de

MAESTRO EN DERECHO PENAL

(Magister Scientiae)

Guatemala, enero de 2021

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

VOCAL I EN SUSTITUCIÓN		
DEL DECANO:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	M. Sc.	Henry Manuel Arriaga Contreras
VOCAL III:	M. Sc.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Denis Ernesto Velásquez González
VOCAL V:	Br.	Abidán Carías Palencia
SECRETARIO:	M. Sc.	Luis Renato Pineda

CONSEJO ACADÉMICO DE ESTUDIOS DE POSTGRADO

VOCAL I EN SUSTITUCIÓN		
DEL DECANO:	Licda.	Astrid Jeannette Lemus Rodríguez
DIRECTOR:	M. Sc.	Luis Ernesto Cáceres Rodríguez
VOCAL:	Dr.	Carlos Estuardo Gálvez Barrios
VOCAL:	Dr.	Nery Roberto Muñoz
VOCAL:	Dr.	William Enrique López Morataya

TRIBUNAL EXAMINADOR

PRESIDENTA:	Dra.	Sonia Doradea Guerra
VOCAL:	M. Sc.	Sandra Marina Ciudad Real
SECRETARIA:	M. Sc.	Ana Patricia Secaida Marroquín

Guatemala, 30 de Noviembre de 2018

Director
Dr. Ovidio David Parra Vela
Escuela de Estudios de Postgrado
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.

Dr. Parra Vela:

Según Acta del Consejo Académico de la reunión Ordinaria celebrada el 31 de mayo del 2017, en el Acta No. 02-2017, Punto CUARTO, Inciso 4.4 y de la Acta No. 13-2017, contenida en el Punto CATORCE, Inciso 14.10, se hace de su conocimiento que se ha elaborado, asesorado y revisado el informe final de tesis intitulado EVIDENCIA DIGITAL EN LA INVESTIGACION CRIMINAL EN LOS DELITOS INFORMATICOS EN GUATEMALA del estudiante Lic. JOSE CARLOS ZAMORA ALVIZURES, el cual se enmarca dentro de los contenidos teóricos, metodológicos de la Maestría en Derecho Penal, cuyo proceso se realizó durante los meses de julio a noviembre del 2018.

El informe final de tesis del Lic. JOSE CARLOS ZAMORA ALVIZURES, cumple con los requisitos establecidos en el Normativo de Tesis de Maestría y Doctorado de la Escuela de Estudios de Postgrado de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, por lo tanto extendemos el dictamen de aprobación para que el sustentante pueda continuar con el proceso de tesis.

Así mismo, se deja constancia que la originalidad de los criterios vertidos en la tesis EVIDENCIA DIGITAL EN LA INVESTIGACION CRIMINAL EN LOS DELITOS INFORMATICOS EN GUATEMALA, son responsabilidad exclusiva del autor, como se estipula en el Artículo 5 Derecho de Autor.

Atentamente,

Magíster ALBA PLÁCIDA MÉNDEZ
Docente Escuela de Estudios de Postgrado
Facultad de Ciencias Jurídicas y Sociales
USAC.

Magíster MARÍA LESBIA LEAL CHÁVEZ
Docente Escuela de Estudios de Postgrado
Facultad de Ciencias Jurídicas y Sociales
USAC

Guatemala, 8 de junio de 2020

Doctor Luis Ernesto Cáceres Rodríguez
Director de la Escuela de Estudios de Postgrado
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Señor director:

Por la presente, hago constar que he realizado la revisión de los aspectos de redacción, ortografía, sistema de referencias y estilo, de la tesis denominada:

Evidencia digital en la investigación criminal en los delitos informáticos en Guatemala

Esta tesis fue presentada por el **licenciado José Carlos Zamora Alvizures**, de la Maestría en Derecho Penal, de la Escuela de Postgrado, de la Facultad de Ciencias Jurídicas y Sociales, de la Universidad de San Carlos de Guatemala.

En tal sentido, considero que, después de realizadas las correcciones indicadas, el texto puede imprimirse.

Atentamente,

Dra. Gladys Tobar Aguilar
Revisora
Colegio Profesional de Humanidades
Colegiada 1450

Dra. Gladys Tobar Aguilar
Doctorado en Educación y Licenciatura en Letras.
Colegio Profesional de Humanidades
Colegiada. 1450

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

D.E.E.P. ORDEN DE IMPRESIÓN

LA ESCUELA DE ESTUDIOS DE POSTGRADO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, Guatemala, 23 de octubre del dos mil veinte.----------

En vista de que el Licenciado José Carlos Zamora Alvizures aprobó examen privado de tesis en la **Maestría en Derecho Penal,** lo cual consta en el acta número 105-2019 suscrita por el Tribunal Examinador y habiéndose cumplido con la revisión gramatical, se autoriza la impresión de la tesis titulada **"EVIDENCIA DIGITAL EN LA INVESTIGACIÓN CRIMINAL EN LOS DELITOS INFORMÁTICOS EN GUATEMALA"**. Previo a realizar el acto de investidura de conformidad con lo establecido en el Artículo 21 del Normativo de Tesis de Maestría y Doctorado.----------

"ID Y ENSEÑAD A TODOS"

ESCUELA DE ESTUDIOS DE POSTGRADO FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES USAC DIRECCIÓN

Dr. Luis Ernesto Cáceres Rodríguez
DIRECTOR DE LA ESCUELA DE ESTUDIOS DE POSTGRADO

Índice

Pág.

Capítulo III

Capítulo IV

Introducción

En la época actual el uso de la internet y de las Tecnologías de la Información ha ayudado al desarrollo de la humanidad, derivado de que estas herramientas son utilizadas en casi todas las actividades que realiza el ser humano, desde lo más cotidiano como realizar un llamada telefónica, leer un libro electrónico o digital, realizar compras a través de la internet, estudiar un idioma, revisar las últimas noticias a nivel nacional e internacional, hasta situaciones más complejas como utilizar la banca virtual, realizar transferencias monetarias nacional e internacionalmente, realizar actividades comerciales a gran escala, utilizar la tecnología de punta para construir robots más sofisticados que incluso han sido enviados en misiones especiales, los avances en la medicina, hasta los inicios de lo que se conoce como inteligencia artificial, entre otras.

El desarrollo tan acelerado de los últimos veinte años de la humanidad, ha aumentado exponencialmente derivado del desarrollo de la internet y de las tecnologías de la información, que han traído muchos beneficios, como el hecho de que actividades que antes eran realizadas por las personas ahora son realizadas por máquinas programadas para hacer estas tareas, la manufactura industrial ahora se realiza en su mayor parte por estas máquinas, existen programas de computadora (software) que realizan tareas de organización y administración en las diferentes empresas y entidades de gobierno y académicas, lo que ayuda a maximizar el tiempo en otras actividades como la toma de decisiones o evaluar nuevos procedimientos, también con la creación de las denominadas *apps* o aplicaciones que pueden utilizarse desde un teléfono móvil, hacen que toda la actividad social, laboral, académica e incluso familiar, a través de las denominadas redes sociales, puedan ser desarrolladas por medio de la tecnología y el acceso a la internet, de manera más rápida y en tiempo real.

Sin embargo, así como existen innumerables aspectos positivos en la existencia de las tecnologías de la información y la internet para las personas, también existen muchos aspectos negativos que en su momento no fueron pensados, como el hecho de la

utilización de las tecnologías de la información y la internet para realizar conductas que chocan con las leyes de cada uno de los países teniendo cada que legislar tipos penales que describan estas conductas y asignarles una pena con el objeto de evitar la comisión de estas y retribuir el daño causado en los casos que estas conductas sean consumadas, a estas conductas se les conoce como delitos informáticos

Esto ha sido un reto a nivel mundial, debido a que muchas de las conductas que se realizan por medio de cualquier tecnología de la información o la internet no han podido ser descritas con precisión para evitar la analogía y que se genere seguridad jurídica para que cada persona entienda y comprenda que actividades pueden ser catalogadas como delitos. En el caso de Guatemala, el Código Penal vigente describe varias conductas denominadas como delitos informáticos; sin embargo, deja sin regular un grupo más grande de conductas esto derivado que los ilícitos que pueden llegar a cometerse van en aumento al mismo tiempo que las tecnologías se van desarrollando, lo que hace que siempre se esté uno, dos o más pasos atrás de las tecnologías.

Pero, no solo en aspectos sustantivos existen dificultades para proteger a la ciudadanía de ser víctima de los delitos informáticos, también la forma en que se persigue y se investiga estas conductas se han convertido en un desafío legal, aún y cuando el proceso penal ha ido evolucionando desde su etapa inquisitiva hasta la actual acusatoria tratando de hacerlo más eficiente y con ello alcanzar la finalidad que se proyecta con el objeto de la averiguación, específicamente de un hecho criminal, la aparición de la denominada evidencia y sus características tan particulares ha creado la necesidad de especializar a los diferentes actores que intervienen en el proceso investigativo, básicamente para reforzar la persecución de los delitos informáticos, con el objeto de buscar la forma de recolectar y preservar la evidencia digital, ser analizada y poder ser presentada en un juicio oral y público, pero de igual manera es necesario capacitar a los jueces para el diligenciamiento de la evidencia y la valoración respectiva así como a los abogados defensores, quienes tienen la función de fiscalizar la legalidad y sobre todo idoneidad de la evidencia digital dentro del proceso penal del país.

Es de esta manera como, en el proceso investigativo, se abordó con detenimiento el tema de la evidencia digital y sobre todo la necesidad de que exista y se regulen procedimientos y protocolos encaminados a reducir los riesgos de pérdida o modificación de la evidencia digital en la persecución penal no solo de los denominados delitos informáticos, sino, además, en todos las conductas ilícitas en donde se utilicen las tecnologías de la información y la internet como instrumento u objeto del delito, la proliferación de la realización de estas conductas y los grandes beneficios económicos al atacar principalmente bienes jurídicos como el patrimonio y la información, ha derivado en la existencia de grupos delictivos que encontrado en las lagunas legales en cuanto a la regulación y persecución penal una forma de vivir, a través de lo que se conoce como Ciberdelincuencia o Delincuencia Organizada Informática.

En el capítulo I, se abordará el tema del proceso penal, su evolución y desarrollo a través de la historia, así como los principios procesales y garantías constitucionales que reconoce el derecho procesal penal en busca de la verdad histórica de los hechos, además, una rama cuyo surgimiento se ha dado con el surgimiento del internet y, sobre todo, de las tecnologías de la información hasta arribar al derecho informático.

En el capítulo II, se desarrolla con detenimiento el tema de los delitos informáticos, desde el origen de estos, su definición y características, así como los instrumentos internacionales que buscan crear un catálogo estándar de delitos informáticos y la necesidad de la cooperación internacional para su persecución.

En el capítulo III, se desarrolla el tema de la evidencia digital, desde el punto de vista del derecho probatorio, así como las características particulares de esta clase de evidencia que como cualquier medio probatorio requiere de un estudio especializado para establecer su importancia y papel dentro del proceso penal en la persecución de los delitos informáticos en Guatemala.

Por último, en el capítulo IV, se analiza la importancia de la evidencia digital, lo que actualmente puede hacerse con esta en una investigación penal, así como la propuesta

de procedimientos mínimos para la recolección, embalaje en la escena del crimen y posterior traslado al laboratorio de análisis forense, con el objeto de preservar y proteger la evidencia.

Capítulo I

2. El proceso penal y el derecho informático

Dentro de los aspectos iniciales que se requieren abordar de la investigación se encuentra todo lo relativo al proceso penal y su relación con el derecho informático, en consecuencia, es preciso describir los antecedentes, definición, importancia, principios generales y específicos del proceso penal, completando este apartado con un breve detalle del derecho informático y esencialmente de la informática jurídica.

1.1. Antecedentes

El desarrollo histórico del proceso penal pone de manifiesto, tres sistemas: el acusatorio, inquisitivo y mixto, pudiéndose agregar, el sistema consuetudinario indígena, que, si bien no se encuentra plenamente reconocido, transcurre paralelamente a los otros, tomando en cuenta que constitucionalmente se reconoce este y que debe supeditarse el marco de sus actuaciones a lo normado dentro del marco jurídico del país.

> Un panorama integral de desarrollo histórico del proceso penal que comience por el derecho griego continúe por el romano y se manifiesta también en el español, sin olvidar las legislaciones que más han influido en su formación, son el mejor aporte a la política procesal y permitir valorar los diversos sistemas vigentes (Berducido Mendoza, 2004, p. 32).

Esto permite tener una aproximación al desarrollo general del proceso penal, entonces, para disponer de un criterio más amplio y comprender el desarrollo de este proceso se efectúa una segunda valoración en torno a los vestigios históricos del tema de la siguiente manera:

> Históricamente la forma inquisitoria surge cuando, por los cambios políticos, desaparecieron las circunstancias que mantenían la forma acusatoria, que cae su

> desuso en el siglo XVI, en este sistema los escritores de la época enseñaban que el juez debía de proveer todo, incluso a la defensa. Los llamados regímenes procesales, reflejan una concepción ideológica imperante en cada etapa en que suele presentarse una reforma a cada sistema. (Velez Mariconde, 2006: p. 19).

En función de los aspectos vertidos con anterioridad, se considera que el desarrollo del proceso en materia penal nunca ha estado exento de aspectos que son susceptibles de señalar como negativos; en ese sentido, el procedimiento acusatorio germánico, que sucedió al romano una vez invadida Roma, se sustentó principalmente en aspectos mágicos místicos como las ordalías o las pruebas de Dios, que sirvieron de sustento a lo que en la actualidad es el proceso penal, tal y como se aplica al menos en las legislaciones a nivel latinoamericano.

> Las reformas procesales penales se han diseminado rápidamente en América Latina. En los últimos 15 años, 14 países latinoamericanos y un número sustancial de provincias y Estados Latinoamericanos han introducido nuevos códigos procesales penales. Estos códigos son, posiblemente, la transformación más profunda que los procesos penales latinoamericanos han experimentado en sus casi dos siglos de existencia. Si bien estas reformas no han sido exactamente iguales en todas estas jurisdicciones, los reformadores han descrito a estas reformas en términos similares, como una movida de un sistema inquisitivo a uno acusatorio o adversarial (Langer, 2011, p. 4).

En el proceso penal es el juzgador, quien decide, básicamente donde se requiere el respeto a los derechos de ambas partes. En contraparte, en las controversias donde el juez, juega un papel más bien de acusador, carecería de igualdad entre las partes que en el intervinieran y quiérase o no, se tendría todo el tiempo en un carácter de culpable al procesado sobre todo tratándose de una persona que no tuviera acceso a una buena defensa.

Los modelos procesales penales, independientemente del país donde se implementen, pueden ser tachados de benignos o malignos, es necesario considerar la importancia que tiene para los Estados, la implementación de ese modelo penal en particular, fundamentalmente, porque a través de este, se pretende legitimar el poder del Estado, a la vez que se justifica la regulación del comportamiento de la colectividad, teniendo presente que es esta misma, quien apruebe o no la instauración y vigencia del modelo que se pretenda implementar.

> Con la transformación de los sistemas de justicia en América Latina, el proceso penal en Guatemala pasó del sistema inquisitivo al sistema acusatorio, respetuoso de las garantías constitucionales y procesales y en el proceso, otros actores ingresan en el escenario de justicia. Se logra la inclusión de la Defensa Pública, como parte del Organismo Judicial y se avanza implementando el juicio oral. Como consecuencia, se concluye con la prioridad de crear una institución que en forma autónoma asumiera la defensa de las personas de escasos recursos, garantizando no solo el derecho de defensa, sino también las garantías del debido proceso.
>
> El 5 de diciembre de 1997, el Congreso de la República de Guatemala aprueba el Acuerdo Legislativo 129-97, que corresponde a la Ley del Servicio Público Penal, el cual entra en vigor el 13 de julio de 1998. Con ello se abandona la dependencia institucional del Organismo Judicial. La autonomía funcional e independencia técnica le ha permitido extender su cobertura a los 22 departamentos de Guatemala y a los municipios en donde se instaure Juzgado de Primera Instancia Penal y conquistar un posicionamiento y reconocimiento tanto a nivel nacional como internacional. (IDPP, 2019).
>
> La historia del proceso penal indica que en el momento en que el Estado absorbe toda la autoridad en una sola persona, tal el caso del Emperador, Rey o Cacique, los procesos penales adquieren una manifestación de inquisición y en los periodos en que la sociedad se acerca a la democracia, o se humaniza la justicia, el proceso penal se vuelve acusatorio. Los llamados regímenes procesales reflejan

> una concepción ideológica en cada etapa en que suele presentarse una reforma a cada sistema. (Binder, 1993, p. 19).

Derivado del planteamiento anterior, es razonable señalar que el proceso penal de forma general, se integra gradualmente de varias etapas sucesivas, mismas que corresponden con inicialmente al procedimiento preparatorio o de investigación como también se le conoce; seguidamente se tiene la etapa intermedia; agotada la anterior, se suscita la etapa del juicio; completándose con la etapa de impugnaciones y finalmente la etapa de ejecución; importante resaltar que cada una de estas se estima como fundamental, particularmente del juicio o debate, en virtud que en dicha fase se produce el contradictorio de manera oral bajo la garantía de la igualdad en el proceso, de modo que las partes puedan contribuir con sus actos, a la decisión judicial que obviamente es lo que les interesa a las partes en litigio.

De esta manera se resulta consistente manifestar que dentro de los aspectos valorativos sobre este apartado, el proceso penal, ha ido manifestando y evolucionando paulatinamente, a la par del grado evolutivo de la sociedad en general, es por ello que dicho proceso ha tratado de estar a la par de las exigencias de sus tiempos, pero aparecen etapas regularmente que se han presentado con algunas inconsistencias y regularmente tiene una evidente incidencia en la historia de la humanidad, para el ejemplo basta con ejemplificar algunos pasajes centrales de los períodos del oscurantismo y sobre todo en torno a lo referente de la inquisición.

1.2. Definición

En este apartado resulta de especial trascendencia efectuar las principales concepciones doctrinarias que giran en torno al concepto del proceso penal, en virtud que para los propósitos investigativos se requiere puntualizar en la forma en que convencionalmente se presenta en la mayoría de las legislaciones, requiriéndose en tal sentido, la descripción minuciosa de las principales acepciones.

> Secuencia o serie de actos que se desenvuelven progresivamente con el objeto de resolver, mediante un juicio de la autoridad, el conflicto sometido a su decisión. Serie ordenada de actos preestablecidos por la ley y cumplidos por el órgano jurisdiccional, que se inician luego de producirse un hecho delictuoso y terminan con una resolución final. Acorde con ello, luego de la comisión de un delito, deben reñirse todos los mecanismos legales pertinentes para que el órgano jurisdiccional resuelva la controversia en la que se ve inmerso el procesado, archivando, absolviendo o condenándolo (Marín Vásquez R. A., 2004, p. 18).

En relación con esta consideración, es evidente que, en el entorno del proceso penal, debe existir un litigio, lo que implica un conflicto de intereses calificado por la pretensión de uno de los interesados y la resistencia de la otra parte.

> El conflicto de intereses solo se convierte en litigio cuando una persona formula contra otra una pretensión, es decir, exige la subordinación del interés ajeno al interés propio; frente a esa pretensión la otra parte expresa su resistencia, o sea, se opone a esta, negando subordinar su interés propio al interés hecho valer mediante la pretensión, ahora bien, la pretensión y la resistencia reciben el nombre de partes. (Ovalle, 2016, p. 336)

Marín (2004) al respecto del proceso penal expone lo siguiente: “es un conjunto de actos que se realizan bajo la dirección de un tribunal” (p. 44).

Dentro de un proceso en general y particularmente del ámbito penal, pueden existir diversidad de procedimientos, todos ellos siempre bajo la estricta regulación o conducción de un órgano jurisdiccional correspondiente, todo esto genera todavía cierto grado de incertidumbre, requiriéndose por consiguiente evaluar una segunda definición al respecto, la cual se expone a continuación:

En la opinión que oportunamente expone Vélez (2006) “es una construcción esencial predispuesta para administrar justicia en cuanto surja la sospecha de que se ha infringido la ley penal” (p. 113).

Generalmente, el proceso se activa con la infracción a la ley penal, es decir, en el momento de suscitarse un evento delictivo, se generan los mecanismos para efectuar la persecución penal, circunstancia que conlleva la implementación de una serie de acciones procedimentales, que solo tienen cabida dentro del proceso penal; es importante, por ello, exponer una tercera definición, la cual se describe seguidamente:

> Conjunto de actos concretos, regulados en abstracto por el Derecho Procesal Penal para obtener del órgano jurisdiccional, la confirmación de la pretensión punitiva, deducida por el órgano ejecutivo y eventualmente para realizarla en forma coactiva, lo que constituye la actividad judicial compleja y progresiva denominada proceso penal (Manzini, 1954, p. 20).

Existe alguna relación entre las definiciones anteriores, toda vez que estas convergen en que es un conjunto de actividades o de pasos concretos que deben desarrollarse dentro del proceso en mención, básicamente, para llevar a buen término el desenlace de este o mejor dicho para llegar a la verdad de los hechos.

En la opinión de De Pina (1983), el proceso penal se define así: “conjunto de actos regulados por la ley y realizados con la finalidad de alcanzar la aplicación judicial del derecho objetivo y la satisfacción consiguiente del interés legalmente tutelado en el caso concreto mediante la decisión del juez competente (p. 403).

Nuevamente se manifiesta lo expuesto con anterioridad, se vuelve a mencionar el término, actos, los cuales se encuentran ordenados dentro de un procedimiento, con el firme propósito de cumplir a cabalidad con una expectativa dentro de un ordenamiento jurídico en particular.

El proceso penal en general es el instrumento indispensable o esencial para la aplicación del derecho penal a casos concretos, radica su importancia en que es la expresión de la facultad punitiva del Estado que se constituye en defensa de la sociedad, tratando de restituir el daño moral o material causado, en busca de la convivencia pacífica entre todos los habitantes de la nación.

La intervención del órgano jurisdiccional se desarrolla mediante un proceso, establecido por un orden constitucional. Este lo determina como medio para lograr la sanción penal o *ius puniendi* del Estado. Dentro de esa relación dialéctica, el proceso penal conjuga cuatro elementos básicos para lograr la realización del valor justicia: la jurisdicción, la competencia, la acción penal y la defensa del imputado.

El proceso penal como tal, constituye un conjunto de actos realizados por determinados sujetos (jueces, fiscales, defensores, imputados, entre otros) con el fin de comprobar la existencia de los supuestos que habilitan la imposición de una pena y, en el caso de que tal existencia se establezca, la cantidad, calidad y modalidad de la sanción, así como determinar las medidas de seguridad respectivas y las responsabilidades civiles si fueron reclamadas. (Melini, 2006, p. 45).

En relación con este planteamiento, nuevamente se resalta el hecho de que el proceso en si es una serie de etapas o pasos que deben realizarse para alcanzar una finalidad, en este caso, desde el ámbito eminentemente jurídico y que es una disposición regulada en el Código Procesal Penal, instrumento adjetivo para la aplicación efectiva de la ley.

Se debe hacer énfasis en los elementos doctrinarios, de esa cuenta, Ossorio (2001) se refiere en lo relativo al proceso penal, con la siguiente acepción: Tiene por objeto promover la persecución penal cuando un hecho reviste las características de delito, por lo que persigue la averiguación de este, a efecto de establecer el actor

que lo ha cometido, la imposición de la pena que corresponda o la absolución del inculpado. (p. 403).

Se hace referencia a los fines del proceso, al establecer la existencia de un delito, la forma en que este pudo haber sido cometido, la posibilidad que a través del proceso se establezca quién o quiénes participaron en la comisión de este, deducir la responsabilidad y la pena.

Se plantea una definición de la siguiente manera:

Es el conjunto de disposiciones legales sistemáticamente estructuradas que establecen coactivamente la organización, formas y medios de actuación del poder jurisdiccional del Estado para la aplicación o realización del derecho penal sustantivo, fijando procedimientos que regulen, garantizando los derechos individuales, la investigación judicial y los debates entre las partes, con miras a la declaración de certeza en torno a la comisión de hechos delictivos generadores de pretensión punitiva y eventualmente resarcitoria y las posteriores ejecuciones. (Vásquez Rossi, 2001, p. 76).

En ese contexto, resulta importante señalar lo vertido en registros históricos, en cuanto a que, en su trayecto, los pueblos han adquirido y configurado determinadas formas del proceso penal, las cuales se han adecuado a las circunstancias económicas, sociales y políticas de estos, de donde han surgido tres sistemas procesales básicos, siendo ellos el inquisitivo, el acusatorio y el mixto. En cada uno de ellos la función de acusación, de defensa y de decisión reviste diversas formas, por la naturaleza misma de cada sistema procesal.

1.3. Importancia

La importancia del proceso, radica en que contiene los procedimientos, protocolos y aspectos secuenciales, independientemente de cómo se le quiera denominar, son

elementos esenciales que deben observarse para demostrar los hechos sometidos a controversia, en tal caso por ejemplo, si a un ciudadano común, le roban sin violencia su aparato telefónico y el derecho penal estipula que es un hurto, pero al carecer del derecho procesal no se podría iniciar una disputa en contra del sujeto activo, quien hurtó dicho aparato, de esta manera el tipo penal que describe el hurto, sería obsoleto en virtud que no podría iniciarse el juicio correspondiente, puesto que corresponde al derecho procesal penal, el facilitar el enjuiciamiento de las personas que incurren en una conducta delictiva.

Este aspecto se concentra en detallar la totalidad de los aspectos que convergen en el proceso penal y sobre todo en los procedimientos que deben realizarse para garantizar la efectividad del proceso y brindarle certeza jurídica al sistema de justicia en general, fundamentalmente en el ámbito jurídico guatemalteco.

Cobra especial importancia, el papel que tiene la víctima en todo este proceso, sobre todo cuando debe comparecer a declarar en el proceso penal, en aquellos supuestos en los que su declaración se erige como prueba de cargo fundamental para la condena del acusado.

1.4. Principios generales

En el presente apartado, se puntualiza una serie de elementos que caracterizan al proceso penal y donde los principios generales forman un papel determinante dentro de este. Estos principios son:

a) Principio de equilibrio

Este permite distribuir recursos para la efectiva persecución penal de la delincuencia y con ello enfrentar con relativo éxito, las causas del delito, así también el de proteger garantías individuales y sociales dentro del derecho más contemporáneo, paralelamente a la agilización, persecución y sanción de la delincuencia y con igual

importancia, se mejora y asegura el respeto de los principales derechos humanos y la dignidad del procesado, equilibrando el interés social con los aspectos individuales.

b) Principio de desjudicialización

En torno a este principio, este hace énfasis en que el Estado debe perseguir ampliamente que los hechos delictivos que generan un notable impacto social, en tal sentido, resulta imperativo que los delitos menos graves, de poca o ninguna incidencia social deben tratarse de una forma diferente.

> El Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal establece cuatro presupuestos en los que es posible aplicar este principio, los cuales se refieren específicamente al criterio de oportunidad, la conversión, la suspensión condicional de la persecución penal y el procedimiento abreviado.

c) Principio de concordia

> Dentro de este principio es importante señalar las dos atribuciones esenciales de los jueces, destacándose entre estos aspectos, el hecho de decidir mediante sentencia las controversias y situaciones jurídicas sometidas a su conocimiento, así como contribuir a la armonía social mediante la conciliación o avenimiento de las partes en los casos que la ley lo permita, cuando no existe peligrosidad y el delito sea poco dañino. (Vásquez, 2006, p. 48)

Los aspectos medulares de este principio constituyen una figura intermedia fundamental si se quiere ver de esta lo relativo al compromiso con un árbitro como mediador, también un contrato de transacción y conciliación judicial, que se subdivide en tres fases, debe valorarse el avenimiento de las partes con la intervención del ente investigador o del juzgador, seguidamente se encuentra la renuncia de la acción pública por parte del órgano representativo de los aspectos sociales, finalmente, se localiza la homologación de la renuncia de la acción penal ante el juez; de esta cuenta se considera que esta nueva función judicial busca fortalecer el orden, la paz y sobre todo lo relativo a la concordia entre las personas.

d) Principio de eficacia

En torno a este principio, es preciso puntualizar que a raíz de la observancia de mecanismos de desjudicialización, así como de la introducción correspondiente de la concordia en materia penal, el Ministerio Público y los Tribunales de Justicia podrán dedicar esfuerzos y tiempo en la persecución y sanción de los delitos que afectan a nuestra sociedad. En este orden, complementa esta estimación la asignación al Ministerio Público las actividades de investigación criminal.

Dentro de este se requiere hacer énfasis en cuanto a que, en los delitos de poca o ninguna incidencia social, el ente investigador y juzgadores deben buscar el acuerdo mutuo, a efecto de solucionar de forma pronta la controversia suscitada.

Mientras tanto es consistente señalar que, en el caso de los delitos graves, tanto el ente investigador como los juzgadores deben aplicar su máximo esfuerzo en la investigación del ilícito y el consiguiente procesamiento de los sujetos activos.

e) Principio de celeridad

Este principio se refiere a que los procedimientos establecidos en el Decreto 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, promueven y facilitan la observancia de las actuaciones procesales, circunstancia que dinamiza el trabajo y persigue un notable ahorro en costos y tiempos.

f) Principio de sencillez

Dentro de las consideraciones a tomar en cuenta sobre este principio, se requiere señalar que la significación del proceso penal es de tanta trascendencia que las formas procesales deben ser simples y sencillas para expeditar dichos fines al tiempo que, paralelamente se asegura la defensa.

g) Principio del debido proceso

Sobre este principio en particular, se estima que este es un principio general del derecho, que establece que el Estado tiene la obligación de respetar la totalidad de los derechos que la ley le reconoce a un individuo.

Por lo general, el debido proceso se vincula al respeto por los derechos de una persona que, en el marco del procedimiento judicial, puede pasar de sindicado a procesado, luego a acusado y, finalmente, condenado. Todos estos pasos que llevan a la condena deben ser concordantes con la legislación y tienen que realizarse garantizando el debido proceso. Si el debido proceso no se cumple, se puede llegar a una condena injusta o contraria a la ley.

> El aparato estatal no puede ejercitar su derecho a la represión más que en la forma procesal y ante órganos jurisdiccionales establecidos en ley. Es importante señalar que si el hecho que motiva el proceso observa las siguientes condiciones: a) Que el hecho, motivo del proceso este tipificado en la Ley anterior como delito o falta, b) Que se instruya un proceso seguido con las formas previas y propias fijadas y con observancia de las garantías de defensa, justamente como se encuentra establecidos en los artículos 1 y 2 Código Procesal Penal, artículo 17 Constitución Política de la República de Guatemala, artículo 11 Declaración Universal de los Derechos del hombre, artículo 1 Código Penal. (Santos, 2007, p. 38).

h) Principio de defensa

Al respecto, se considera que este en gran medida consiste en que nadie podrá ser condenado ni privado de sus derechos sin antes haber sido citado, oído y vencido en un proceso judicial, está consagrado por nuestra Constitución y desarrollado debidamente en el Decreto 51-92, el cual contiene el Código Procesal Penal del país.

De acuerdo con lo anterior, se estima por consiguiente que este derecho asiste a una persona, física o jurídica, o bien de algún grupo en particular a defenderse ante un órgano jurisdiccional de los cargos que se le señalan con observancia plena de igualdad e independencia, en consecuencia, se trata de un derecho que se suscita en todos los órdenes jurisdiccionales y se aplica en cualquiera de las fases del procedimiento penal.

Este principio es localizable en el artículo 12 de la Constitución Política de la República y en esencia consiste en que nadie podrá ser condenado mucho menos privado de sus derechos, sin antes haber sido citado, oído y vencido en un proceso

judicial, de esta manera en el Código Procesal Penal en el cual se destaca que el procesado desde la primera actuación judicial hasta la eventual condena, posee una serie de derechos que le asisten y facilitan conocer todas las actuaciones y por ende contar con la respectiva defensa técnica, a exceptuando lo regulado en la Ley Contra la Narcoactividad, la cual contempla la reserva de actuaciones en las fases de investigación y preparatoria y el artículo 314 del Código Procesal Penal, que establece que el ente investigador puede solicitar la reserva correspondiente de las actuaciones, inclusive ante las partes, cuando aún no se dicta el auto de procesamiento.

En ese contexto, este derecho implica ser advertido del hecho que se imputa, declarar voluntariamente, hacer señalamientos en los actos del proceso, presentar pruebas e impugnar resoluciones, examinar y rebatir la prueba, conocer la acusación, formular alegatos y defensas, contar con asistencia técnica oportuna.

i) Principio de inocencia

Sobre este principio en particular, se regula que toda persona se presume inocente mientras no haya sido declarado responsable en sentencia condenatoria debidamente ejecutoriada, todo esto en función de lo preceptuado en el artículo 14 Constitución Política de la República de Guatemala, así como del artículo 11 de la Declaración Universal de los Derechos del Hombre. En consonancia con estos preceptos, resulta consistente señalar que el fortalecimiento de este principio requiere, entre otros aspectos, los siguientes.

a) La culpabilidad debe establecerse mediante sentencia judicial.
b) Que la condena se base en prueba que establezca con certeza el hecho criminal y la culpabilidad.
c) Que la sentencia se base en pruebas jurídicas y legítimas.
d) Que la prisión provisional sea una medida cautelar de carácter excepcional para asegurar la presencia del inculpado en el proceso y la realización de la justicia. (López, 2006, p. 45).

En cuanto a este apartado, es evidente que este principio se refiere esencialmente a los aspectos que tienen o guardan relación con una garantía fundamentales contemplada inicialmente dentro de la propia Declaración Universal de los Derechos Humanos y que luego fue adoptado dentro de otras legislaciones, entre estas la guatemalteca, a fin de garantizar a los procesados, la observancia plena de sus derechos más elementales.

j) Principio *favor rei*

Al respecto de este principio, este también es conocido como *in dubio pro reo* y es el resultado de la observancia del principio de inocencia, toda vez que, en caso de duda, y, por tanto, en sentencia, ante la duda sobre la comisión de un ilícito, por parte del imputado, se requiere decidir en favor del sujeto activo, porque el propósito esencial de todo proceso penal gira en torno a que no se condene a inocentes.

k) Principio *favor libertatis*

Este principio se refiere a hacer el menor uso de la prisión preventiva, pues con regularidad se ha impuesto desproporcionalmente, derivando en daños morales, sociales y familiares al sujeto por el tipo de hecho delictivo cometido no era necesaria la medida y en donde muchas de estas, finalmente, eran encontradas inocentes.

De esta manera, se persigue la regulación del acto de prisión y también su aplicación en casos de delitos graves, sobre todo cuando por las características del delito, se requiera preverse que, de no dictarse, el sujeto activo podría evadir la justicia.

Es preciso señalar que este principio tiende o está encaminado a reducir la prisión preventiva a una medida que asegure la presencia del imputado en el proceso, que este no obstaculice el proceso y asegurar la ejecución de la pena. De igual manera, cuanto sea necesaria la prisión preventiva, persigue que los actos procesales puedan encaminarse a la respectiva restitución de la libertad del imputado y, finalmente, también contempla la utilización de medios sustitutivos de prisión.

l) Principio de readaptación social

Dentro de los elementos que deben tomarse en cuenta y que este principio regula, debe observarse lo contenido en la Convención Americana sobre Derechos Humanos señala en el artículo quinto, inciso sexto, que las penas privativas de libertad tendrán como finalidad esencial la reforma y la readaptación de los condenados.

Acorde con la disposición anterior, existen numerosas críticas que pueden formularse desde perspectivas ideológicas a la reforma o readaptación social de las personas condenadas, en tal sentido resulta inobjetable que esta constituye la única finalidad aceptada en nuestro ordenamiento jurídico positivo para legitimar la pena de privación de la libertad. Este aspecto en gran medida, se estima que tiene sentido a partir de lo exigido por Constitución Política de la República de Guatemala y sobre todo en torno a lo contemplado en los artículos 5 y 6 de la Convención Americana de Derechos Humanos, 10.3 del Pacto Internacional de Derechos Civiles y Políticos y 40.1 de la Convención Internacional sobre los Derechos del Niño.

m) Principio de reparación

Entre los principios que rigen la materia relativa a la reparación o resarcimiento de los daños y perjuicios, ocupa un lugar esencial y preeminente en la generalidad de los sistemas jurídicos el denominado principio de la reparación integral. Este principio, conocido también en su expresión latina *restitutio in integrum*, se dirige a lograr la más perfecta equivalencia entre los daños sufridos y la reparación obtenida por el perjudicado, de tal manera que este quede colocado en una situación lo más parecida posible a aquella en la que se encontraría si el hecho dañoso no hubiera tenido lugar.

Cuando de daños patrimoniales se trata, se requiere necesariamente efectuar una apreciación concreta y precisa del perjuicio ocasionado o sufrido por el titular del interés afectado, apreciación que permite determinar el resarcimiento necesario, bien en forma específica, sobre todo para lograr la equidistribución entre este y el daño y consecuentemente, para alcanzar la tan deseada reparación integral.

1.5. Principios específicos

El Código Procesal Penal, vigente en el país, plantea en sus aspectos iniciales, los principios generales del derecho procesal penal, de esta manera estos han llegado a considerarse como uno de los puntos más discutidos, básicamente, porque se considera como tales los axiomas o máximas jurídicas que gradualmente se han ido recopilando de las antiguas compilaciones existente sobre el derecho en particular.

Se hace referencia a los principios generales; sin embargo, se requiere hacer énfasis en los principios especiales, los cuales se detallan a continuación:

a) Principio de oficialidad

A través de este principio se genera la obligatoriedad para el Ministerio Público a promover la investigación de eventos delictivos y sobre todo de impulsar la persecución penal, requiriendo como supuesto que el hecho investigado revista los caracteres de acción delictiva y la investigación deja intacto el derecho del agraviado a participar en el proceso en calidad de parte.

b) Principio de contradicción

Los aspectos esenciales de este principio señalan que, con base a la garantía constitucional, del derecho de defensa que asiste al imputado, la legislación adjetiva penal establece un régimen de bilateralidad e igualdad, en la relación jurídica procesal. Esto da oportunidad suficiente a las partes procesales, para oponerse en iguales condiciones de acusación y defensa. Las partes tienen amplias facultades para hacer valer sus derechos y garantías en el proceso penal, pues mientras el Ministerio Público ejerce la persecución penal; por otro lado, el imputado tiene la facultad de defenderse de la imputación que se le hace.

Las partes, tienen el derecho del contradictorio, de oponerse a la imputación que se les haga. Para que esto sea efectivo, se hace necesario, también, que ambas partes

procesales, tanto el acusado como la defensa, dispongan de estrategias y posibilidades de alegación, prueba e impugnación.

c) Principio de oralidad

Mediante este principio se hace hincapié en cuanto a que, la oralidad asegura el contacto directo entre los elementos probatorios y el juzgador, por ende, representa la forma natural de alcanzar la verdad, sobre todo de reproducir de forma congruente el hecho delictuoso, de valorar el estatus de las personas que proveen estos elementos. En especial la oralidad sirve para el resguardo correspondiente del principio de inmediación, la publicidad de los hechos y la individualización del acto normativo.

La oralidad como principio procesal, encuentra su fundamento en el artículo 362 del Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, que establece:

> El debate será oral. En esa forma se producirán las declaraciones del acusado, de los órganos de prueba y las intervenciones de todas las personas que participan en él. Las resoluciones del tribunal se dictarán verbalmente, quedando notificados todos por su emisión, pero constarán en el acta del debate.

d) Principio de concentración

Exige una aproximación temporal entre la recepción de la prueba y el pronunciamiento jurisdiccional que se base en ella. Por eso, los beneficios del principio se aseguran mediante la regla de que el debate debe realizarse durante todas las audiencias consecutivas que sean necesarias hasta su terminación.

Esta concentración de los actos que integran el debate asegura que la sentencia será dictada inmediatamente después de que sea examinada la prueba que ha de darle fundamento y de la discusión de las partes. La relativa unidad de tiempo que resulta de esta regla permite la actuación simultánea de todos los sujetos procesales y una valoración integral de las probanzas, alejando la

posibilidad de que se olvide el resultado de los elementos probatorios recibidos o los interprete de modo incorrecto.

Con este principio se procura, por un lado, evitar que el fraccionamiento de los actos del debate deforme la realidad con la introducción de elementos extraños y por el otro, asegurar que los recuerdos perduren en la memoria de los jueces en el momento de la deliberación y de la decisión, que es la actividad que encierra la tarea de síntesis de todo el juicio, siendo necesario que el juez en el momento de pronunciar el fallo, tenga vivo en la mente, todo lo que ha oído y visto.

Entonces, el debate y la substanciación de pruebas, médula espinal del juicio oral, deben realizarse con base a este principio, en forma concentrada en el tiempo y en el espacio determinado. Esto significa que no pueden llevarse a cabo en localidades diversas, salvo excepciones determinadas. La concentración procesal, está regulada por el Código Procesal Penal, en el artículo 360, al señalar que el debate continuará durante todas las audiencias consecutivas que fueran necesarias hasta su conclusión. (REDU, 2019).

La idea de este principio, en gran medida giran en torno a procurar que no se distorsione la secuencia de actos o etapas que se han ido realizando durante el mismo y que a través del mismo no se produzca algún tipo de separación de los actos de y ante los órganos jurisdiccionales correspondientes.

e) Principio de inmediación

Con la vigencia del principio de oralidad surge el principio de inmediación. Este principio aparece también en la fase probatoria y se une en forma inseparable a la oralidad, para funcionar como principios que dan fundamento al sistema acusatorio. En función de esta serie de elementos que se han vertido es razonable señalar que para conseguir el imperio de la verdad es necesario que los sujetos procesales reciban inmediata, directa y simultáneamente los medios de prueba que han de dar fundamento a la discusión y a la sentencia.

En este contexto, no puede consentirse que las actuaciones que dan base a la sentencia se lleven al cabo en ausencia de los jueces.

Este principio procesal localizado en el Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, exige que el debate se realice con la presencia ininterrumpida de los jueces llamados a dictar la sentencia, del Ministerio Público, del acusado, de su defensor y de las demás partes o sus mandatarios; los sujetos procesales principales, no pueden abandonar la sala donde se desarrolla el juicio, excepto las partes civiles.

f) Principio de publicidad

Este principio en particular sustenta el marco de sus actuaciones procesales en la Declaración Universal de los Derechos Humanos y se contempla de forma precisa en el artículo 10 de esta en la cual se establece:

> Toda persona tiene derecho, en condiciones de plena igualdad, a ser oída públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal.

g) Principio de fundamentación

De acuerdo con los principios planteados con anterioridad, a través del presente se obliga a precisar en los autos y las sentencias, de manera explícita, el motivo y la razón de la decisión, circunstancia que hace al juez reflexivo y lo conmina a prestar atención al debate y al examen de las leyes o doctrinas que tienen relación con la cuestión litigiosa. Establece el artículo 11 bis del Código Procesal Penal, los autos y las sentencias contendrán una clara, precisa fundamentación de la decisión, su ausencia constituye un defecto absoluto de forma.

h) Principio de doble instancia

La Constitución Política de la República de Guatemala establece que en ningún proceso habrá más de dos instancias, lo cual es un reconocimiento tácito de lo pactado por el país en tratados y convenios internacionales que garantizan el derecho de recurrir del fallo ante juez o tribunal superior.

En Guatemala, la doble instancia se identifica con el recurso de apelación especial que implica la revisión íntegra del fallo de primer grado, así favorezca o perjudique a quien lo haya interpuesto, incluyendo al procesado, lo cual viola el principio de *favor rei*, aspecto que corrige el actual Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, en el artículo 422 al establecer la *reformatio in peius*, cuando la resolución solo haya sido recurrida por el acusado o por otro en su favor, no podrá ser modificada en su perjuicio, salvo en lo que se refiere a la indemnización civil de los daños y perjuicios provocados.

Las características del sistema acusatorio implementado en la nueva legislación procesal penal, modifican las formas tradicionales de apelación en el país, porque como se dijo los tribunales de segunda instancia que conocen de las sentencias y autos definitivos no tienen potestad para corregir *exnovo* la causa y corregir por ese medio todos los errores de hecho y de derecho que pueda cometer el juez de sentencia. (REDU, 2019).

Este aspecto ha tenido especial trascendencia en el país, básicamente para limitar el hecho de que un mismo asunto sea ventilado o corregido por dos o más instancias, menos aun si fuera simultáneamente, por tal razón se asegura que una vez agotada la etapa anterior, debe ser otro órgano quien conozca lo que corresponde.

i) Principio de cosa juzgada

Debe recordarse que el fin específico del proceso judicial es la sentencia firme, que en el caso del derecho procesal penal absuelve o condena al acusado, equivale a término, límite, consumación, objeto o motivo último. Lo anterior significa que llega un momento en que las fases del proceso se agotan, en que la sentencia que lo concluye

es irrevocable en su forma, no susceptible de impugnación por haberse agotado o dejado de interponer los recursos pertinentes.

Atendiendo esta serie de elementos, resulta de suma utilidad hacer énfasis en cuanto a que materialmente se finalizan las posibilidades de efectuar otra evaluación del fallo y por ende no es factible iniciar un nuevo proceso por las mismas acciones entre las mismas partes y con el mismo fin.

> Este aspecto en concreto tiene excepciones cuando datos relevantes o causas desconocidas en el proceso fenecido o nuevas circunstancias evidencien claramente errores que hacen que la verdad jurídica sea manifiestamente distinta a lo ocurrido en la realidad objetiva, o se descubran actividades dolosas que muestran que el principio de cosa juzgada lesiona la justicia, procede el recurso de revisión, que más que un recurso es un procedimiento especial de reexamen de una sentencia ejecutoriada. (REDU, 2019).

En este orden de ideas, es importante señalar que este principio en particular, cobra sentido cuando ya se ha emitido alguna resolución o sentencia sobre el tema motivo de controversia y por consiguiente se estima que, por medio de este principio, no puede volver atrás o retomarse algún aspecto que oportunamente no se conoció.

1.6. Derecho informático

El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, que tiene en su haber antecedentes a nivel histórico.

> El derecho de la informática, como instrumento regulador del fenómeno informático en la sociedad, no ha sido estudiado del mismo modo que la informática jurídica, porque se ha dado más importancia a los beneficios que a los eventuales perjuicios que puedan traer consigo las computadoras respecto al derecho y la sociedad en

> general. Entre el reducido grupo de tratadistas sobre el derecho de la informática, algunos consideran a este una categoría propia que obedece a sus reglas, que surge como una inevitable respuesta social al fenómeno informático y que por ello es un derecho en el que su existencia precede a su esencia (Vivant, 1986, p. 104).

La conceptualización de este derecho permite hasta cierto punto un grado de creatividad amplio sin que trascienda a otros niveles mucho más prácticos o especulativos, de esta manera se estima necesario y consistente exponer un planteamiento mucho más concreto sobre este tema en particular.

En la opinión de Téllez (2008, p. 147)“es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática” (p. 14). En ese contexto, se considera como un conjunto de leyes plenamente estructuradas, en virtud que existen diversos ordenamientos jurídicos nacionales e internacionales que hacen énfasis preciso en el fenómeno de la informática.

De manera personal, puede señalarse al respecto que son normas generales a través de las cuales se integra plenamente la denominada política informática, de esta cuenta se infiere que esta rama del derecho se ha ido formulando paulatinamente por jueces, magistrados, tratadistas y estudiosos del tema, por otra parte, se refiere a hechos concretos que han resultado de la interacción de la informática con el ser humano.

Tradicionalmente, el derecho y las tecnologías de información y comunicaciones pertenecían a dos materias distintas, siendo resumidamente el primero una disciplina que estudia la regulación de la conducta humana en la sociedad y las segundas un conjunto de servicios, redes, aplicaciones y herramientas tecnológicas cuya incorporación en las actividades del quehacer productivo y social, redunda en la mejora de la calidad de vida de las personas.

Como antecedentes al respecto, puede mencionarse que desde que la informatización empezó a dar los primeros pasos comerciales en la década de los 60 y

70 del siglo pasado, se inició el desarrollo de soluciones informáticas aplicadas al sector de la justicia, tomando forma así lo que hoy se conoce como informática jurídica.

> Al respecto, es pertinente destacar que el primer contacto entre Derecho e Informática inicialmente limitó su enfoque al uso de las tecnologías para el mero almacenamiento de datos legales. Sin ser exhaustivos, se pueden identificar por lo menos tres etapas en este sentido. La primera, situada en los años 60-70, se dirigió a la construcción de bases de datos jurídicas a nivel de la administración pública. En la segunda etapa, años 80-90, la difusión de las computadoras permitió el uso individual de la tecnología para la recolección y la redacción de textos jurídicos: la tecnología entró en el mundo privado de los bufetes de abogados y jueces que escriben textos legales. En una tercera etapa, finales de los 90 en adelante, domina el uso de Internet. En esta etapa la difusión de tecnologías aplicadas al uso diario del derecho es global y permite intercambiar propuestas, contratos, documentos legales, etc., llegando a ser un recurso para el mismo gobierno electrónico, visto en términos generales como el uso de las TIC por parte del sector público con el fin de mejorar los servicios y aumentar la transparencia y la *accountability* de los gobiernos (Gamboa, 2010, p. 3).

En torno al derecho informático, los aspectos iniciales que deben tomarse en consideración que engloban al derecho informático, son inicialmente el concepto derecho, para conocer posteriormente el derecho informático.

> Atendiendo a su etimología la palabra derecho proviene de las voces latinas *directum* y *dirigere,* que significan: conducir, enderezar, gobernar, regir, llevar rectamente una cosa hacia un término o lugar señalado, guiar, encaminar; por lo que, en sentido lato, derecho quiere decir: recto, igual, seguido, sin torcerse a un lado ni a otro. La voz latina *jus*, con la que se designó en Roma al derecho, no es más que una contracción de *jussum*, participio del verbo *jubere*, que significa mandar. En sentido general podemos decir que el derecho es un conjunto de normas jurídicas que regulan las relaciones de producción, consumo, intercambio

> y distribución. Regula la conducta que deben observar las personas dentro de una sociedad en relación con el Estado, en sus relaciones económicas y con sus semejantes. Son las reglas que establecen el comportamiento de la persona dentro la sociedad (Bosch, 1997. p. 18).

Este planteamiento es esencial para poder conocer a profundidad el concepto de derecho informático, en virtud que, si no está claro el primero, se dificultaría disponer de mayores juicios lógicos para entender el funcionamiento de este apartado.

> El derecho informático es considerado como una ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) regulación del medio informático en su expansión y desarrollo y b) aplicación idónea de los instrumentos informáticos. Se le considera autónomo, aunque no es en sí una rama típica, pero si constituye conocimientos y estudios específicos que se encuentran relacionados al derecho y la informática y aunque no es tan desarrollado como otras ramas del derecho, si se puede hablar de conocimientos específicos que caracterizan a una rama del derecho como autónoma, como la existencia de un campo normativo, docente, institucional y científico. Generalmente, el nacimiento de una rama jurídica nace o surge a consecuencia de cambios sociales reflejados en las soluciones normativas al transcurrir los años; pero en el caso del Derecho Informático, no hubo ese transcurrir del tiempo en los cambios sociales, sino el cambio fue brusco y en muy poco tiempo, como consecuencia del impacto de la informática en la sociedad, alcanzándose sociedades informatizadas (Altmark, 1987. p. 64).

Esta rama del derecho en particular se estima que resulta ser una creación jurídica, se encarga de buscar soluciones a los retos planteados por la evolución de las aplicaciones de las computadoras electrónicas. Esta rama del derecho está en constante seguimiento y estudio de los avances, adelantos y transformaciones tecnológicas a fin de ir planteando las medidas adecuadas que permitan una armónica convivencia social.

Como consecuencia de lo anterior se ha llegado a considerar que esta es una nueva disciplina jurídica que tiene como fin inmediato el estudio de la informática y como objeto mediato la información, en tal sentido su método científico se caracteriza por desarrollar las instituciones jurídicas informáticas e interrelacionarlas sistemáticamente con la realidad.

> En fuentes abiertas o electrónicas, este aspecto se contempla así:
> Es el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones. Otros autores lo definen como conjunto de leyes, normas y principios aplicables a los hechos y actos derivadas de la informática. Es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de esta en las que existe algún bien que es o deba ser tutelado jurídicamente por las propias normas (previa.uclm.es, 2018, parr. 5).

En ese contexto, el derecho informático se ha constituido en una renovada área jurídica, focalizada en la regulación de lo relativo a la información que fluye en línea, es decir, a la informática y a la telemática, consciente de lo anterior en esta rama del derecho también se localizan sentencias sobre el ámbito informático y sobre todo los razonamientos focalizado en cuanto al análisis e interpretación, exposición y críticas hacia el sector normativo que proyecta esta rama del derecho en particular.

> A diferencia de la política informática, la legislación informática es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso de la informática, es decir, aquí se trata de una reglamentación de puntos específicos, pero esta circunstancia necesariamente implica las siguientes consideraciones:

a) Si se recurriese a un cuestionamiento de las reglas existentes para determinar si es posible su aplicación análoga frente al problema o si sería necesaria una ampliación en cuánto a su ámbito de cobertura.

b) Esperar la evolución de la jurisprudencia dada la creciente presentación de casos ante los órganos jurisdiccionales en los que se fijen pautas resolutorias o al menos conciliatorias.

c) Crear un cuerpo de nuevas reglas integrándolas a ordenamientos ya existentes, o que den lugar a una nueva ley de carácter específico. A nuestro parecer, esta última es la opción más indicada (Téllez Valdés, 2008, p. 147).

En concordancia directa con los preceptos vertidos con anterioridad, es consistente manifestar que esta rama del derecho, en esencia se ha tornado en interdisciplinaria, básicamente, porque tiene como aspecto medular el estudio y sobre todo el desarrollo de las tecnologías que vayan dirigidas a la investigación científica, particularmente de aquellas desavenencias jurídicas.

Atendiendo esta serie de preceptos, además, es de suma utilidad señalar que en el área del derecho informático se considera que efectivamente si existe legislación específica en otros países como España e incluso Colombia en la cual se contempla todo lo relativo al ámbito de las tecnologías, cosa contraria en Guatemala, donde aún es una deuda pendiente, aun cuando se han presentado diversas un par de iniciativas que tienen como propósito fundamental regular este tipo de actividades dentro de la vida cotidiana de las personas y como tal se ha prestado también a la comisión de diversos delitos, donde, definitivamente, intervienen una amplia gama de herramientas tecnológicas.

En consecuencia, resulta razonable señalar que toda la legislación que eventualmente pueda generarse al respecto debe sustentarse principalmente en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de diferentes naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

1.7. Informática jurídica

Atendiendo estos preceptos, se estima que en forma general la informática, se ha venido a constituir como uno de los fenómenos más significativos dentro de los diversos avances que ha tenido la humanidad, sobre todo en cuanto a dejar plasmado su particular incidencia en diversas áreas del conocimiento humano en general.

De acuerdo con el *Diccionario de la Real Academia Española* (2015) se entiende la informática como “el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores” (p. 856).

También se puede entender el concepto de informática como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores o computadores, con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Acorde con ello, es preciso manifestar que la informática es aplicada en numerosos y diversos sectores de la actividad humana, destacándose entre estos, la biología, física, química, meteorología, ingeniería, industria, investigación científica, comunicaciones, arte, nivel empresarial, gestión, entre otros de particular importancia.

En termino generales, es válido afirmar que la informática jurídica, viene a ser una técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica y la elaboración y aprovechamiento de instrumentos de análisis y tratamiento de la información jurídica necesarios para lograr dicha recuperación.

> Como muchas de las actividades del ser humano, la aparición de las computadoras en la vida diaria, produjeron efectos de diversos tipos, entre ellos, aplicaciones nuevas y una especie de aceleradores de las rutinas cotidianas posibles, pero como sabemos toda mejora parece insuficiente y se intenta seguir incorporando las

> rutinas humanas e imitar a la naturaleza, dentro de lo posible, para que sean desarrolladas por las máquinas computadoras, auxiliados por brazos mecánicos de todo tipo, así como también se producen muchos y complicados programas de computación no solo indispensable, sino, además, el más avanzado para cada una de las necesidades que como sabemos son hoy día completamente especializadas. Así tenemos que los principales efectos de la incursión de las máquinas son positivamente alentadores al elevar la producción personal y del sistema productivo tanto doméstico como el industrial, tecnológico, con extensiones en todas las disciplinas humanas, culturales, educativas, contemporáneas. (SEGOB, 2006, p. 16).

De acuerdo con el planteamiento anterior, se considera que uno de los usos más importantes de la informática es facilitar información en forma oportuna y verídica, lo cual, puede facilitar entre otras cosas la toma de decisiones en diferentes espacios, así como permitir el control de procesos críticos.

Para Rivero (1986), "no es sino la informática considerada como sujeto del derecho; es decir, como instrumento puesto al servicio de la ciencia jurídica" (p. 204).

En la opinión de Suñe (1986) "es la aplicación de los ordenadores electrónicos orientada a la resolución de problemas jurídicos" (p. 204).

En esencia, puede decirse que la informática jurídica consiste en una ciencia que forma parte de la Informática, es la especie en el género y se aplica sobre el derecho en particular, de manera que se genere el tratamiento adecuado y efectivo de la información que se produce en materia jurídica. De esta manera, es una ciencia que estudia en gran media, la utilización minuciosa de los recursos informáticos, fundamentalmente para la mejora de los procesos en el ámbito jurídico.

> Es la interrelación entre las materias informática y derecho que tiene como fin el análisis, la estructuración lógica y ordenada, la deducción e interpretación de la

> información jurídica a través de la utilización de la máquina computadora para su efectivo y eficaz tratamiento, administración, recuperación, acceso y control y cuyos alcances están predeterminados al auxilio en la toma de decisiones jurídicas (Riestra, 1995, p. 118).

En ese contexto, es importante puntualizar que esencialmente a través de esta definición se estima aunque sea de forma general que esta puede llegar a asegurarse que en esencia no es una rama del derecho, particularmente, porque su enfoque es fundamentalmente tecnológico, y no tiene contenido jurídico, de esta manera, esta área se focaliza en el uso de software y hardware como instrumentos del derecho y surge con la evolución correspondiente de los diversos dispositivos que son susceptibles de utilizar en la cotidianidad del individuo.

> Para Chouraqui (1974) este concepto se concibe y lo plantea de la siguiente manera
> “es la ciencia y la técnica del tratamiento lógico y automático de la información jurídica” (p. 24).

Atendiendo estos preceptos, es razonable considerar que el concepto de informática jurídica se ocupa de brindar soporte a la administración y gestión de las entidades, al punto que, dentro de sus aplicaciones, es susceptible de localizar programas para el seguimiento de casos y expedientes, control de archivos, control de clientes y facturación, notificaciones, estimaciones de impuestos, formularios electrónicos, entre otros de singular importancia para los propósitos que le atañen.

Al respecto, es importante señalar que la relación entre derecho e informática, regularmente presenta dos aspectos esenciales que deben considerarse en la investigación, en primer lugar, se estiman los aspectos normativos del uso de la informática, desarrollados bajo el derecho de la informática y la segunda la aplicación de la informática en el tratamiento de la información jurídica, a lo que en la actualidad se ha denominado como informática jurídica. Es de esta cuenta que, para el desarrollo de esta,

es necesario considerar ciertos elementos de origen como son la aplicación de la lógica del derecho o raciocinio jurídico.

En ese orden de opiniones, se estima, por lo tanto, que esta rama del derecho incorpora a los ordenadores todas las normas legales, particularmente lo relativo a la jurisprudencia y la bibliografía para por dotar al jurista de la documentación adecuada, actualizada sobre el tema planteado. Esta disciplina con regularidad hace acopio detallado de técnicas documentales, las cuales son referidas al tratamiento permanente y sistemáticos de documentos para la información especializada, esta circunstancia incluye la selección de documentos a partir de conocimientos lo más completos posible.

Como aspecto complementario, es preciso manifestar que también depende en gran medida del almacenamiento, circunstancia que se refiere a la acumulación de documentos originales o reproducidos, introducidos en la memoria, de modo que permitan las operaciones de recuperación y búsqueda fundamentales para su posterior localización, con lo cual se ha facilitado enormemente la labor de la humanidad en general y por ende de allí su influencia en las ciencias jurídicas y como gradualmente ha ido cobrando notoriedad dentro de las mismas.

Consciente de ello, merece destacarse que dentro del diseño de bases de datos utilizados para propósitos legales, así como del desarrollo de aplicaciones para esta rama en particular, existe una vertiente que ha ido cobrando auge últimamente y se refiere principalmente al uso de la lógica jurídica y razonamiento legal, en la que se destacan la simplicidad de sistemas de educación asistida por computadora.

Con lo anterior se considera que la tarea de la informática jurídica, en gran medida, consiste en conocer el funcionamiento de los recursos tecnológicos que sean susceptibles de emplear en el campo del derecho, particularmente para el diseño e impulso de nuevos mecanismos encaminada a transmitir y optimizar los recursos que permitan hacer un mejor uso y explotación de las leyes en el país.

Capítulo II
2. Delitos Informáticos

2.1. Antecedentes

Dentro de los aspectos iniciales de este capítulo, es importante señalar que los delitos informáticos, están directamente relacionados con el desarrollo de las tecnologías de la información y las comunicaciones, en consecuencia, se requiere abordar y abarcar lo que en la actualidad se denomina Ciberdelincuencia o Delincuencia Informática, desde sus inicios y la forma que ha evolucionado este fenómeno.

> En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia. (Camacho, 1987, p. 34.).

De acuerdo con este planteamiento, resulta lógico pensar, que siendo que en la actualidad la informática, las redes sociales, las comunicaciones a través de internet, no pueden quedar fuera de la actividad delictiva, aunado a que prácticamente todas las actividades que se realizan desde la forma en la que se comunica, se aprende y comercializa, hasta la forma en que nos entretenemos está íntimamente ligado a la tecnología, como no va a ser utilizada esta herramienta para realizar actividades ilícitas.

El surgimiento de este tipo de crímenes está estrechamente ligado con el desarrollo de la tecnología informática. Según Herrera (2010) “Las computadoras se han utilizado para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato, entre otros” (p. 49).

Indica Huerta (2011) “este fenómeno ha obligado al surgimiento de medidas legislativo-penales en los estados industriales donde hay conciencia de que, en los últimos años, ha estado presente el fenómeno delictivo informático” (p. 45).

Aunque es necesario destacar que a nivel nacional se carece de una ley especial que regule estas actividades ilícitas, únicamente se han agregado al catálogo de delitos penales, algunas figuras delictivas, pero estas no son suficientes para proteger a los ciudadanos del ataque a los diferentes bienes jurídicos que estas conductas lesionan.

Lo cierto es que todo esto ha sido utilizado y aprovechado por las diferentes estructuras que se dedican a delinquir, al abrirse un mundo de oportunidades en donde pueden aprovechar las diferentes debilidades tanto de las personas individuales que utilizan la red, como las de las empresas y entidades gubernamentales, que no invierten en seguridad informática, lo cual es aprovechado por estos nuevos delincuentes que utilizando sus conocimientos y habilidades en materia informática han logrado agenciarse de grandes cantidades de dinero y sobre todo de valiosa información almacenada en diversos dispositivos de almacenaje informático, información que posteriormente es vendida o utilizada por grupos del crimen organizado para poder realizar sus actividades ilícitas, circunstancia que ha provocado el origen de la denominada criminalidad informática o delincuencia informática

> Baón (1996), define a la criminalidad informática como: la realización de una forma de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (p. 7).

En función de este planteamiento, resulta consistente señalar que se puede determinar con relativa precisión que se está ante una inevitable dualidad, en cuanto a objeto e instrumento, particularmente, porque dentro de lo que se denomina actividades de índole ilícita, las computadoras o cualquiera de sus elementos o complementos que convencionalmente integran el software o hardware, puede ser utilizados para realizar conductas contrarias a derecho o bien pueden ser el objeto de las conductas reprochables, esta serie de aspectos valorativos, necesariamente se estima que conlleva una especialización específica en el momento de realizar las investigaciones para llegar

a establecer quién o en este caso quiénes son los responsables penalmente de realizar las actividades ilícitas..

Al respecto, Resa (2005) indica lo siguiente: "el crimen organizado no existe como tipo ideal, sino como un grado de actividad criminal o como un punto del espectro de legitimidad" (p. 9).

En esencia, es importante señalar que el crimen organizado recurre, a la falta de seguridad informática, a las debilidades de control de acceso a los sistemas de cómputo y a una tecnología moderna de comunicación en la internet para cometer sus ilícitos; pero, se debe empezar a combatir este problema de forma interna. Entonces, es necesario entender que este tipo de criminalidad ya es una realidad en Guatemala, donde existen varios grupos organizados que se dedican a utilizar las computadoras, la internet, las redes sociales y, en general, toda la tecnología, para cometer delitos; y, en realidad, la legislación y normatividad nacional no está adecuada para combatir de manera efectiva a estos criminales.

2.2. Definición de delito informático

El concepto de delito informático tienen varias formas de ser definido, derivado de su especialidad en cuanto a la forma que los diferentes tipos penales informáticos se perfeccionan en el mundo material, dejando de ser una abstracción legal para convertirse en delitos; partiendo de la idea general de establecer la definición de delito para poder desarrollar de mejor forma la definición de delito informático, en principio se puede definir al delito como toda acción u omisión típica, antijurídica y culpable; sin embargo, existe extensa doctrina nacional y extranjera que establece la definición de delito, la mayoría de ellas define al delito cuando cumplen los elementos positivos que lo constituyen, de ahí que se pueda establecer que es el delito.

> Es la conducta humana consciente y voluntaria que produce un efecto en el mundo exterior (acción), que se encuentra prohibida por la ley (tipicidad), la cual es contra derecho (antijuridicidad) y que la persona ha incumplido a pesar de que conoce y valora la norma (culpabilidad) (Barrios, 2011, p. 2.).

Algunos otros autores establecen que la persona debe estar en capacidad de comprender lo ilícito de su acción (imputabilidad). Existen diferentes teorías por medio de las cuales se puede dar una definición de esta institución; sin embargo, se considera que esta última es suficiente para desarrollar este tema.

Partiendo de la definición anterior, se debe establecer qué es un delito informático, al respecto, el autor mexicano Téllez (1999) señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)" (p. 12).

Se establece por medio de esta definición, esa dualidad señalada con antelación en cuanto que los diferentes medios informáticos, en principio instrumentos para incurrir en una conducta antijurídica; es decir, el mecanismo mediante el cual el sujeto activo del delito llega a la consumación de la actividad delictiva.

Es importante señalar que esas gamas de elementos informáticos pueden ser o son en la mayoría el centro del ataque o vulneración del sujeto activo, con el propósito de acceder al mismo, para dañar su integridad, obtener la información que contiene, modificar la información, utilizar la información para beneficio propio o de la organización criminal a la cual pertenece.

Davara (1996) define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea *hardware* o *software*" (p. 13).

Aquí se aprecia como este autor define al delito informático de una forma más técnica utilizando los términos hardware y software para englobar el objeto o instrumento de tipo penal informático, los cuales son utilizados en contra de los derechos del titular de un elemento informático.

> Es la acción u omisión, antijurídica y culpable, que se realiza por medio de un sistema que haga uso de las tecnologías de la información o un componente de este, o que lesione la integridad, disponibilidad o confidencialidad de la información (Alvarado R. y., 2008, p. 16).

Se puede evidenciar en esta definición que los autores utilizan el término tecnologías de la información y aquí se abarca un espectro mucho más amplio, ya no es únicamente el computador, con sus elementos auxiliares de entrada y de salida y el denominado procesador; ya se habla de tecnologías, que alcanza a todos aquellos dispositivos, desde las computadoras personales, tabletas, teléfonos, realidad virtual, relojes, incluso hasta la denominada inteligencia artificial, en la actualidad pueden ser utilizados como instrumentos del delito o como objetos de las conductas ilícitas

En forma básica, el autor Barrios (2006) define al delito informático, de la siguiente manera “las acciones prohibidas por la ley, que se comete en contra de uno o varios de los elementos que integran un sistema de información o los derechos que de este se deriven (protección de datos, intimidad o privacidad, derechos de autor” (p. 14).

En este caso, el autor utiliza sistema de información, con el cual se aprecia el conjunto de componentes internos y externos, que componen un sistema de manejo de información, tanto en lo que se refiere a su ingreso, procesamiento, egreso, almacenado y traslado de la información a través de estos sistemas y sobre los cuales existen o se han generado derechos individuales y colectivos, como la protección de los datos, protección a la intimidad, la protección a los creadores de programas de computación, las denominadas aplicaciones para equipos móviles, el derecho de las personas de

conocer los datos que tienen los diferentes registros públicos. En tal sentido, los delitos informáticos son conocidos también como cibernéticos o electrónicos y en todos se desarrollan acciones dolosas o culposas, tipificadas en la ley, en la que se tiene como instrumento u objeto del delito, cualquiera o todos los elementos de un sistema informático, que vulneren derechos fundamentales, el cual es sancionado con una pena.

2.3. Sujetos del delito informático

De esta suerte, el bien jurídico será, en definitiva, el elemento localizador de los sujetos y de su posición frente al delito. En este orden del titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente ser un tercero.

2.3.1. Sujeto activo

En el Código Penal guatemalteco, el sujeto activo por su participación en el delito se clasifica en autores y cómplices. En lo que se refiere a los delitos informáticos, las personas que los cometen, quienes tienen ciertas características, tales como: un alto grado de conocimientos técnicos especializados, recursos, habilidades, destrezas especiales, para el manejo de la informática y tecnologías de la información y comunicaciones (TIC); generalmente, por la actividad laboral que realizan, se encuentran en lugares donde se maneja la información de carácter sensible o bien, son hábiles en el manejo de los sistemas informáticos, aun cuando, en muchas ocasiones, sus actividades no faciliten la realización de este tipo de delitos.

Se ha logrado establecer que los sujetos activos de este tipo de delitos son de una gran diversidad y la diferencia entre ellos radica, en la naturaleza de los delitos cometidos, de tal manera que, el individuo que ingresa en un sistema informático sin intenciones de cometer algún delito es muy diferente de la persona que labora para una institución bancaria o inclusive en el aparato estatal para generar cualquier información

encaminada a desvirtuar, fraguar algún fraude u cualquier otra conducta que lesione un bien tutelado.

A pesar de lo anterior, teniendo en cuenta las características mencionadas de las personas que cometen los delitos informáticos, los estudiosos en la materia los han catalogado como delitos de cuello blanco; esto derivado que en la época que se empiezan a descubrir estas actividades se estableció que los sujetos activos que se dedicaban a cometer estas conductas son personas de cierto nivel socioeconómico y la realización de las conductas no puede explicarse por carencias económicas ni por mala habitación, por falta de recreación, por no tener un alto nivel de educación, un bajo nivel intelectual, menos aún por problemas emocionales.

Existen diferentes formas de denominar al sujeto activo de los delitos informáticos; sin embargo, no se pueden considerar sinónimos, entre las diferentes formas de sujetos activos se encuentran:

2.3.1.1. Hacker

Montaño (2008) cita a Rodao, quien define a Hacker de la siguiente manera “intruso o pirata informático, en la mayoría de los casos, son programadores o personas inadaptadas que se dedican a realizar conductas ilícitas utilizando las computadoras” (p. 23).

Este término ha sido utilizado para denominar a toda persona experta en una rama de la informática y las telecomunicaciones como programación, *software* y/o *hardware.*

Algunas características de un hacker son:

a. Su objetivo es adquirir conocimientos para sí mismo de manera autodidacta.
b. Son personas minuciosas con la tecnología, analizándola, descubriéndola hasta dominarla, modificarla y explotarla.

c. Se consideran obsesivos y compulsivos por acumular conocimiento y tener lo mejor en la tecnología.
d. Con un alto nivel de conocimiento informático.

b) k. Se preocupan por poner accesible otros conocimientos que, generalmente, son de interés público, los cuales son publicados en sus propias páginas de internet. (Chávez, 2012, p. 56).

De acuerdo con este planteamiento, es consistente señalar que la acción de introducirse en sistemas informáticos y redes privadas o públicas es conocida como hacking, actividad en la que el hacker utiliza agujeros o vacíos en la seguridad informática de los protocolos para poder acceder y navegar en internet, estos protocolos son conocidos como protocolo de control de transmisión, el cual se divide en control de transición, haciendo que se reciba la información, transmitiendo la dirección a donde deberá ser enviada, según la solicitud del usuario y mantener el orden de la información y el IP o protocolo de internet es una forma de identificación de equipos utilizados para la navegación, similar a un número telefónico que permite enviar y recibir información debido a que al dividir en bloques la información almacena la dirección de IP tanto del remitente como del destinatario.

Otra forma que un hacker pueda conocer estos protocolos es mediante las cookies, estos poseen una buena intención debido a que un usuario entra a una página y envía una solicitud para poder acceder a ella y esta, a su vez, otorga o no autorización para el acceso y utiliza las cookies para almacenar la información de los protocolos, algo así como una tarjeta de datos para la transmisión de información de ambas partes, con el fin de, que en un futuro, poder ingresar de nuevo en la misma página y no se tenga que hacer de nuevo todo el proceso de verificación y aceptación. Los hackers crean páginas señuelos con interés para el usuario el cual utiliza la excusa de las cookies para obtener esta información o incluso más información confidencial, sin que el usuario pueda darse cuenta, con el fin de encontrar víctimas para estudiar y encontrar agujeros o atajos en la seguridad en los usuarios.

Obtenida esta información, el hacker ingresa a la computadora e investiga el tipo de software al que se enfrenta y el equipo en el que se encuentra, ya adentro del sistema y conociendo el software, el hacker ingresa como si ya fuera un usuario legítimo o robando las claves de acceso en el momento de entrar e intenta obtener los privilegios de un administrador autorizado con el fin de tener acceso a toda la información disponible en el equipo de cómputo, con el objeto de evitar sospechas de existencia de intrusos en el sistema, los hackers buscan e intentan permanecer poco tiempo en ellos al día con lo que un ataque puede llevarse a cabo durante días o solo tocar los archivos de interés sin acceder un número determinado de archivos que levante sospechas, al terminar para no ser detectado conforme a su dirección de correo electrónico o dirección IP utiliza editores dentro del sistema infiltrado para borrar o cambiar su mismo correo o dirección de IP.

2.3.1.2. Cracker

De manera personal, puede enunciarse el término *crack* como una palabra proveniente del idioma inglés, la cual significa romper o partir, cambiar bruscamente y se ha venido a utilizar como un sustantivo para nombrar a las personas que se dedican a acceder en lugares prohibidos dentro del internet para destruir.

Estas personas son consideradas, en el ámbito informático, más peligrosas, pueden ser hackers al mismo tiempo, poseen gran capacidad de programación, amplios conocimientos en criptografías y criptoanálisis. Se dedican a acceder a sistemas informáticos prohibidos, tanto de empresas privadas como entidades de gobierno, nacionales y extranjeras, con el propósito de robar, destruir y distribuir programas comerciales pirateados, crean todo tipo de virus para su beneficio e incluso para venderlos a terceros, su intención es violentar los derechos de autor, más que por simple curiosidad y búsqueda de conocimiento como el hacker.

Existen diversos tipos de usuarios quienes, sin ser crackers, son considerados de gran peligrosidad usando el nombre de crakers siendo estos los Script-Kiddies, quienes se consideran crackers, pero poseen menores conocimientos que estos, presumen de

sus conocimientos utilizando programas de terceros para hacer daño que, en la mayoría del caso, son el reflejo de actos de vandalismo.

2.3.1.3. Phreaker

> Proviene de la palabra freak, la cual es una palabra en inglés, que significa que algo o un acontecimiento es altamente inusual o irregular, la palabra *phone* quiere decir teléfono y la conjunción de ambas palabras nos da como resultado la palabra *phreaker* la cual significa la manipulación de un teléfono o un sistema de telecomunicación de forma ilícita para hacer llamadas sin pagar por estas. (Chávez, 2012, p. 65)

Todo lo expuesto en los numerales anteriores, en esencia son actividades ilegales para enriquecerse, destruir o actos terroristas contra equipos informáticos, los cuales, en su mayoría, son sistemas de telefonía fija o móvil celular, televisión de paga para obtener servicio gratuito mediante tecnología de avanzada, comprada o creada por ellos mismos. En su evolución, se han enfocado en ingresar a sitios bancarios para robar cuentas bancarias y números de tarjetas de crédito o, incluso, para crear números de cuentas usando programas originales de las empresas de tarjetas de crédito y siempre son auxiliados con grandes sistemas de cómputo armados por ellos mismos.

2.3.1.4. Virucker

> En el año de 1939, el científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su teoría y organización de autómatas complejos, donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura. (Informatico, 2018, parr. 1).

A través de esta definición, se conocen los inicios del desarrollo de programas informáticos invasivos y que, eventualmente, podrían tomar el control de otros

dispositivos, aunque fue solo un intento, el cual posteriormente, desde los años noventa, adquirió mayor notoriedad, básicamente, porque se consumaba este hecho.

> En 1959, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, tres jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1949 (Informatico, 2018, parr. 2).

Con este planteamiento, se comprende que existe una relación directa con la aseveración de Newman, expuesto en el párrafo anterior, en virtud que, siguiendo los preceptos expuestos por este, se desarrollaron los primeros pasos para la creación de los juegos por computadora que en la actualidad se encuentran sumamente avanzados.

> Existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las IBM 360, emitiendo periódicamente en la pantalla el mensaje: *I'm a creeper... catch me if you can*! (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), porque por aquella época se desconocía el concepto del software antivirus. (Informatico, 2018, parr. 3).

Puede notarse a través de este planteamiento que ya para el año 1972, la industria IBM, fue una de las primeras víctimas de un virus informático, surgiendo a partir de allí la necesidad de disponer o desarrollar programas antivirus que permitieran contrarrestar esta práctica destructiva del software informático.

> En 1980 la red ArpaNet del Ministerio de Defensa de los Estados Unidos, precursora de internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo, algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron tres largos días en desarrollar el programa antivirus correspondiente; lo

que actualmente los desarrolladores de antivirus resuelven un problema de virus en contados minutos (Informatico, 2018, parr. 4).

A través de este registro, puede vislumbrarse abiertamente los inicios de lo que en la actualidad se conoce como internet, resultando ser un desarrollo inicialmente de indole militar y que fue extendiendose hasta determinar que es una herramienta global y esencialmente necesaria para el desarrrollo de diversas actividades cotidianas, laborales, industriales, comerciales, entre otras.

> Hacia 1984, el doctor Fred Cohen al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubo varios autores más que actuaron en el anonimato. El doctor Cohen ese mismo año escribió su obra Virus informático: teoría y experimentos, donde, además, de definirlos los califica como un grave problema relacionado con la seguridad nacional. Más tarde, el doctor escribió la obra: El Evangelio, según Fred (The Gospel according to Fred) y es aquí donde desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur. (Informatico, 2018, parr. 8).

Del planteamiento anterior se desprende el hecho de que hasta la fecha transcurren ya casi 35 años de que se generaron los primeros virus informáticos, afectando a cientos de usuarios y a miles en la actualidad, estimándose hasta cierto punto como necesarios para el desarrollo y optimización de las herramientas ofimáticas que son de uso común en las diversas actividades que desarrolla el ser humano.

> El comienzo de la gran epidemia fue en 1986 cuando se difundieron los virus rain, Bouncing Ball y Marihuana, los cuales fueron las primeras especies representativas de difusión masiva. Estas tres especies virales tan solo infectaban el sector de arranques de los disquetes. El 2 de noviembre de 1988, Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science de

> la Universidad de Cornell, difundió un virus a través de ArpaNet, logrando infectar 6,000 servidores conectados a la red. El reporte de diversas ciudades del mundo, a mediados de 1995, fue lo que detonó la aparición de una nueva familia de virus que no solo infectaban documentos, sino que, a su vez, sin ser archivos ejecutables podían autocopiarse infectando a otros documentos. Este virus fue llamado macro virus. En 1997, se disemina a través de internet el primer macro virus que infectaba hojas de cálculo, el cual fue denominado Laroux y en 1998; surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos (Informatico, 2018, parr. 12).

En esencia, con esta aseveración se vislumbra el despegue y posterior auge que iba representar la informatica para el ser humano y como esta iba a contribuir determinantemente con la globalización, facilitando el desarrollo de muchas otras areas técnicas, cientificas, laborales y academicas, que aunque ha estado sujeto a diveras complicaciones a raíz del surgimiento de los virus y piratas informaticos, se sabe en la actualidad de la enorme importancia que estas herramientas han tenido en el desarrollo y sostenibilidad del individuo en sociedad.

> En 1999, inició la propagación masiva en internet de virus anexados o adjuntos a mensajes de correo como el Melisa o el macro virus Papa. De esta cuenta, en noviembre de 1999 apareció el Bubble Boy primer virus que infectaba los sistemas con tan solo leer el mensaje de correo. Para junio del 2000 se reportó el VBS/Stages.SHS, primer virus oculto dentro de la extensión SHS (Informatico, 2018, parr. 12).

Acorde con lo expuesto en los parrafos anteriores, es conveniente puntualizar que los virus informaticos encontraron en la internet un conducto invasivo para diversos ordenadores a nivel mundial, labor que evidentemente estuvo a cargo de connotados piratas informaticos, quienes inclusive tuvieron alguna formación militar o instruidos por otros miembros de equipos de investigación tecnológica, muy estrechamente

relacionado con el ambito militar, circunstancia que contribuyó a la difusión y consecuentes complicaciones para los usuarios del internet a nivel global.

Lo descrito anteriormente es una breve reseña de dónde provienen los virus y sus creadores en el tiempo. Su forma de operar consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir virus y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus: los benignos que molestan, pero no dañan y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

2.3.1.5. Pirata informático

Entiéndase por pirata persona que se dedica a la piratería siendo esta la actividad relacionada con el asalto y robo de embarcaciones en el mar, según el sentido original del término.

Cuando se hace referencia a un pirata informático, se está hablando de alguien que toma de forma ilegal algo de un tercero en el mundo virtual.

> A nivel global, el uso del software ilegal está sujeto a sanciones y penalidades, que se agravan cuando el pirata se convierte en un comercializador de software copiado ilegalmente para lucrar en beneficio propio. De acuerdo con ello, una persona que se dedica a la alteración de cualquier aplicación informática es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor; hay que considerar también la piratería como descargar música de internet y grabarla en un CD para escucharla. (Sosa, 2019, párr. 1)

Se puede establecer, entonces, que existe una variedad de personas que pueden tener la calidad de sujetos activos en la comisión de un delito informático que utilizando todos sus conocimientos técnicos pueden ingresar de forma ilegal en sistemas informáticos e incluso en alguna conducta de la cual el legislador debe estar consciente para proponer y crear legislaciones que vayan adelante de esos delincuentes, pero que en el caso de Guatemala, está lejos de concretarse, pues a pesar de existir iniciativas al respecto en el Congreso de la República, las mismas no han podido convertirse en leyes.

2.3.2. Sujeto pasivo

El sujeto pasivo es la persona individual o colectiva, quien sufre las consecuencias de la comisión de un delito siendo la sociedad y la víctima o agraviado en primer término, pero, además, es necesario tomar en cuenta que, en principio, el sujeto pasivo del delito es la persona física o jurídica que resiente la conducta o actividad delictiva, es el titular del bien jurídicamente tutelado vulnerado o puesto en peligro por la conducta del responsable. Por medio del estudio del sujeto pasivo se posibilita conocer los diferentes ilícitos que se cometen a los activos informáticos, con objeto de prever las acciones ilícitas antes mencionadas debido a que muchos de los delitos son descubiertos por casualidad, desconociendo la forma de operar de los sujetos activos; es decir, la mayor parte de las veces no se tienen indicios de cómo lo realizan.

Debido a lo anterior, en Guatemala ha sido casi imposible establecer la verdadera magnitud de los delitos informáticos, porque la mayor parte de ellos no son descubiertos o no son denunciados a las autoridades competentes y si a esto se suma la falta de una adecuada legislación que proteja a las víctimas de estos delitos, la falta de preparación técnica y jurídica por parte de fiscales, investigadores y peritos para poder brindar más y mejores elementos de convicción a los encargados de la administración de justicia; aunado el temor, por parte de las empresas, a denunciar por las consecuentes pérdidas económicas, al quedar al descubierto que no cuentan con una plataforma de seguridad informática que proteja de manera eficientes los sistemas informáticos y, por ende, la información que se almacena y se procesa, entre otros más, trae como consecuencia

que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada cifra negra.

Es mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras o tecnologías de la información, que se puede alertar a las posibles víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática y si a esto se suma la creación de una adecuada legislación que proteja los intereses y derechos de los titulares de medios informáticos así como los que se originan del uso de estos, lo que se complementa con una eficiente preparación al personal encargado de la investigación y a la administración de justicia para atender estas conductas ilícitas, se avanzaría mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse no solo en Guatemala, sino a nivel mundial.

Los organismos internacionales han adoptado resoluciones similares, en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de las autoridades encargadas de hacer cumplir la ley, para detectar, investigar, prevenir y sancionar los delitos informáticos, surgiendo por consiguiente la necesidad de que dentro de la legislación guatemalteca resulte imperativo el establecimiento de un marco normativo en la materia.

2.3.3. Bienes jurídicos tutelados

Conocido también como, derecho protegido, bien garantizado, interés jurídicamente tutelado, objeto jurídico, núcleo del tipo, objeto de protección. Para que exista un delito es necesario la preexistencia de un bien protegido por la sociedad y que derivado de su importancia es necesario blindarlo a través del derecho penal con el objeto de que la sociedad sepa que en el momento de poner en peligro o causar un daño a al bien protegido será sancionado con una pena. Existen diferentes bienes que son jurídicamente protegidos por el Estado, entre los cuales se menciona la vida, el patrimonio, la seguridad, la administración de justicia, la economía, entre otros. “El bien jurídico constituye el punto de partida y la idea que preside la formación del tipo. Afirma,

además, que son bienes jurídicos aquellos intereses, de la vida, de la comunidad a los que presta protección el derecho penal" (Jescheck, 1981, p. 350).

El bien jurídico como objeto de protección del derecho penal es todo valor individual o colectivo que merece la garantía o tutela de no ser vulnerado por la acción de otra u otras personas. El objeto del bien jurídico encuentra su origen en el interés de la vida, previo al derecho, que surge de las reacciones sociales, aunque el interés vital no se transforma en bien jurídico hasta que es protegido por el derecho, es el derecho que elige y decide entre los diferentes intereses sociales, los que deben ser merecedores de una protección especial, de convertirse en bien jurídico, esto por medio del proceso que se realiza en el organismo legislativo, lo que se conoce como proceso legislativo.

Los bienes jurídicos que se vulneran en los delitos informáticos son estos que se protegen desde el punto de vista de los tipos penales tradicionales, reinterpretados desde el punto de vista teleológico; es decir, visto desde su fin, o que se les ha agregado algún elemento para poder ser perseguido penalmente, por medio de la investigación y ser sancionado por parte de los órganos jurisdiccionales en materia penal. Entre los bienes jurídicos que se protegen en materia de delitos informáticos, existen:

a) La reserva, la intimidad y confidencialidad de los datos, en el caso de los ataques informáticos en el campo de los registros o bancos de datos de personas individuales o jurídicas
b) La propiedad, tomando a la información como un bien merecedor de protección, así como a los elementos físicos o materiales que componen un sistema informático, el cual puede ser afectado por medio de ataques a sus componentes.
c) El patrimonio, debido a los constantes ataques y fraudes informáticos, que dan lugar al deterioro o detrimento del patrimonio de las personas jurídicas o individuales.
d) La seguridad o fiabilidad del tráfico jurídico y probatorio, lo que se evidencia en las falsificaciones de datos o documentos a través de medios informáticos.

La delincuencia informática no solo afecta o ataca un bien jurídico determinado, sino que la multiplicidad de conductas que se realizan también afecta a una diversidad de bienes protegidos.

En cada una de las modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial) como la hacienda pública, el sistema crediticio, el patrimonio, entre otros y la de interés macrosocial vinculado al funcionamiento de los sistemas informáticos. Los delitos informáticos afectan en un mismo momento diversos bienes jurídicos, características que los hace difíciles de perseguir y documentar en su totalidad.

2.3.4. Características de los delitos informáticos

Como conductas reprochables penalmente, los delitos informáticos tienen características propias que probablemente no se las encontramos en otro tipo de conductas delictiva, lo que hace necesario identificarlas con el objeto de poder prevenirlas y en su momento poder ser investigadas de manera eficaz. Entre las principales características de los delitos informáticos, existen:

a) Conductas criminales de cuello blanco, un número reducido de personas tiene la capacidad intelectual y económica para poder realizar estas conductas delictivas, dado que la tecnología ni está al alcance de cualquier persona y es necesario invertir tiempo y recursos económicos para poder aprender y desarrollar habilidades para el manejo de la tecnología; sin embargo cabe mencionar que en la actualidad, hasta personas menores de edad han demostrado un alto grado de conocimiento en el manejo de las nuevas tecnologías, sin que sea necesario un estatutos económico elevado, pero si con alto nivel de inteligencia que le permite poder manejar de mejor manera la tecnología.

b) De oportunidad y ocupación, la mayoría de estas conductas la realizan los sujetos activos en el momento de estar laborando en diferentes entidades ya sean públicas

o privadas, donde tienen el acceso a la información y aprovechan las oportunidades que se les presentan al conocer las debilidades de los entornos informáticos para poder consumar los hechos delictivos, utilizando los medios informáticos como instrumentos o bien atacar estos para su realización.

c) Flexibles en el espacio y tiempo; las conductas delictivas informáticas, pueden realizarse en segundos, a través de un “click” ya se puede consumar el hecho, además, no es necesario que le sujeto activo se encuentre en el lugar del hecho, para lograr su consumación, puede estar el sujeto activo en un país y la víctima estar en un país distinto a miles de kilómetros incluso, lo que ha acarreado problemas con los que se denomina territorialidad de la ley penal.

d) Provocan grandes daños económicos, la mayoría de los delitos informáticos tienen como fin principal afectar el patrimonio de las víctimas, uno de los puntos que son atacados por los delincuentes informáticos son las instituciones bancarias o financieras, derivado que muchos no cuentan con los mecanismos de seguridad o tienen mecanismos muy débiles para afrontar esta forma de delinquir, de igual las grandes empresas son atacadas constantemente con el objeto de obtener información sensible y valiosa para posteriormente vender esa información o pedirle a los empresarios grandes cantidades de dinero a cambio de devolverla.

e) Presentan dificultades para su investigación, debido a su carácter técnico y especializado aunado a la falta de regulación legal a nivel nacional e internacional y la falta de capacidades técnicas y económicas en la recolección y análisis de la evidencia digital.

f) Pluriofensivos, afectan o ponen en peligro a varios y diferentes bienes jurídicos, esto sin perjuicio que algunos de los bienes jurídicos estén independientemente protegidos por otro tipo penal.

2.3.5. Clasificación de los delitos informáticos

Existen clasificaciones doctrinarias y legales de los delitos informáticos, derivado de su especialidad y complejidad, se establece una clasificación atendiendo al carácter dual de las conductas ilícitas informáticas, ya sea como medio de cometer las conductas prohibidas o bien como objeto de estas conductas, también se pueden clasificar atendiendo al bien o bienes jurídicos tutelados.

Molina Salgado cita una clasificación de los delitos informáticos de la siguiente manera:

a) Como instrumento o Medio. En esta categoría se encuentran las conductas criminológicas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito
b) Como fin u objetivo. En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. (Molina, 2003, p. 105).

Esta clasificación hace referencia al aspecto dual de la delincuencia informática manifestada en los delitos informáticos. Los delitos informáticos pueden y son utilizados como instrumento para cometer diversos delitos, entre las formas que son utilizados como medio se puede mencionar: la falsificación de documentos por medio de las computadoras, como puede ser la clonación de tarjetas de crédito; la manipulación de los estados financieros, por medio de la computadora, lo que puede afectar el patrimonio de personas jurídicas o individuales; el acceso, lectura y sustracción de información confidencial; utilización o violación de códigos para ingresar a un sistema informático con instrucciones inapropiadas; alteración del funcionamiento de sistemas informáticos, acceso a áreas informatizadas en forma no autorizada, entre otros.

En lo que se refiere a la clasificación de los delitos informáticos de acuerdo con su fin u objeto, actividades que consisten en programación de instrucciones que producen un bloqueo total o parcial en un sistema informático, destrucción de programas, daño a

la memoria o a los sistemas de almacenamiento interno, secuestro electrónico de soportes magnéticos en los que se almacena valiosa información con fines de chantaje, canje, entre otros.

2.3.6. Clasificación de los delitos informáticos, según el Convenio sobre la ciberdelincuencia (Convenio de Budapest)

El Consejo de Europa en el convenio llamado Convenio sobre la ciberdelincuencia, el cual a la fecha ha sido ratificado por veintidós países europeos y otros veintidós lo han firmado y donde Guatemala no forma parte de este grupo; es un instrumento jurídico internacional que expone y describe una serie de conductas en materia informática, que clasifica como tipos penales.

Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest el 23 de noviembre de 2001, entrando en vigor el 1 de julio de 2004".

Es el único instrumento que cubre cada una de las áreas relevantes para la legislación en materia informática, refiriéndose básicamente al derecho penal sustantivo, derecho penal adjetivo y cooperación internacional.

El convenio busca aplicar con carácter de prioridad, una política criminal común con el objeto de proteger a la sociedad de la denominada y creciente delincuencia informática, a través de la legislación adecuada y el fomento de cooperación internacional derivado de su carácter transnacional, sostenido en la creencia de que la lucha contra este fenómeno criminal requiere de todo el apoyo y colaboración internacional.

El convenio clasifica los delitos informáticos en cuatro grupos, dependiendo el o los bienes jurídicos que protege:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los datos informáticos.
b) Delitos informáticos
c) Delitos relacionados con el contenido
d) Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines.

Puede notarse la gama de aspectos que deben tomarse en consideración el grado de incidencia que tiene estos delitos en la realidad guatemalteca, debiéndose destacar que afectan en algún momento la estabilidad económica, política, social y cultural de los ciudadanos afectados.

2.3.6.1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los datos informáticos

En esta clasificación se hace referencia a los tipos penales informáticos que vulneran lo que se denomina sistema informático, el cual se define de la siguiente manera:

> Una colección de personas, procedimientos, una base de datos y (a veces) hardware y software que colecciona, procesa, almacena y proporciona datos procesos de transacciones a nivel operacional e información para apoyar la gestión de toma de decisiones o constituirse en parte del producto o servicio. (Calderón R. C., 2018, párr. 2).

El sistema informático compuesto por el hardware y software, que consisten en los componentes internos y periféricos, con los cuales se pueden acceder y manipular el sistema informático, así como los diferentes programas de computación o sistemas operativos que posibilitan las realizaciones de operaciones y procesos.

En ese contexto, es menester señalar que el ataque al sistema informático afectará directamente la disponibilidad, la integridad y lo que se refiere a la confiabilidad de los contenidos en uno o varios sistemas informáticos los tipos penales que se describen en esta clasificación son los siguientes:

a) Acceso ilícito: El acceso deliberado e ilegitimo a la totalidad o a una parte de un sistema informático, ya sea infringiendo medidas de seguridad, con la intención de obtener datos informáticos.
b) Interceptación ilícita: Interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro de este, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.
c) Interferencia en los Datos: Comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
d) Interferencia en el sistema: Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.
e) Abuso de los dispositivos: Comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta. (Quirós, 2019, p. 2)

2.3.6.2. Delitos Informáticos

La comisión de estos tipos penales afecta a un bien que en los últimos tiempos ha adquirido una gran importancia como la información, Barrios (2011), la define como “el conjunto de datos alfanuméricos, numéricos o lógicos que representan la expresión de un conocimiento, que pueden utilizarse para la toma de decisiones” (p.23).

Al respecto del planteamiento anterior, resulta de suma importancia señalar que la información representada por medio o bien a través de datos informáticos, destacándose entre estos aspectos, la manipulación, alteración, sustracción o bien la supresión de la información, circunstancia que evidentemente puede causar perjuicios tanto legales como patrimoniales tanto a personas individuales como colectivas. Los tipos penales que se describen dentro del Convenio Sobre la Ciberdelincuencia, conocido también como el Convenio de Budapest, de forma general señala con precisión entre otros aspectos, los siguientes:

a) Falsificación informática. Introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que lo datos sean legibles o inteligibles directamente.
b) Fraude informático. Actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: introducción, alteración, borrado o supresión de datos informáticos; cualquier interferencia en el funcionamiento de un sistema informático; con la intención de obtener de forma ilegítima un beneficio económico para sí o para otras personas.

2.3.6.3. Delitos relacionados con el contenido

En esta clasificación regula lo que se refiere a la pornografía infantil, que de acuerdo con el Convenio de Budapest, se entiende como todo material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca menor adoptando un comportamiento sexualmente explícito; c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito las nuevas tecnologías actualmente son utilizadas para realizar este tipo de conductas han merecido que sean tipificadas y sean perseguibles penalmente, lastimosamente a nivel nacional no se le ha tomado la importancia debida, y no se tienen los mecanismos

necesarios tanto para su prevención como para su investigación y persecución, con la finalidad de proteger a los menores de edad contra estos ilícitos. (Magdalena, 2019, p. 5)

A nivel internacional, la pornografía infantil es un aspecto que ha tomado gran relevancia, el hecho que las nuevas tecnologías sean utilizadas para realizar este tipo de conductas ha merecido que sean consideradas conductas delictivas y sean perseguibles penalmente; protegiendo de esta forma la integridad de los menores de edad, quienes se han visto expuestos a ser víctimas de estos delitos.

El Convenio de Budapest, en el título 3, regula lo que se refiere a:

a) Delitos relacionados con la pornografía infantil. Comisión deliberada e ilegítima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos.

2.3.6.4. Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines

Este apartado hace referencias a acciones ilícitas que vulneren la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, que hasta la fecha ampara a nivel internacional el derecho de los autores; así como las asumidas por el Tratado de la Organización Mundial de Propiedad Intelectual (OMPI) sobre derechos de autor, de igual forma como las obligaciones asumidas en aplicación de la Convención Internacional sobre la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, Convención de Roma y del Acuerdo

sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y el Tratado de la Organización Mundial de Propiedad Intelectual (OMPI), sobre Interpretación o Ejecución y Fonogramas. (WIPO, 2019, p. 7)

2.3.7. Clasificación legal de los delitos Informáticos regulados en Guatemala

El Decreto número 33-96 del Congreso de la República de Guatemala, que entró en vigor el tres de julio de 1,996, adiciona al Código Penal lo relativo a los delitos informáticos. El cuarto considerando de este Decreto establece:

> Que los avances de la tecnología obligan al Estado a legislar en bien de la protección de derecho de autor en materia informática, tipos que nuestra legislación no ha desarrollado.

Los delitos informáticos se encuentran regulados en el Título IV de los delitos contra el patrimonio, con el objeto de proteger las creaciones de la propiedad intelectual, así como derechos humanos intrínsecos de las personas como la intimidad personal.

Para clasificar los delitos informáticos regulados en el Código Penal, se analizarán desde el punto de vista del bien jurídico en la norma tipo, para tener una visión más amplia de estos y lo que el legislador protegió en la ley.

2.3.7.1. Alteración de programas

> El Código Penal, en el artículo 14 adiciona el artículo 274 ”B” establece:
> “Alteración de programas. La misma pena. Del artículo anterior se aplicará al que altere, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras”.

El bien jurídico tutelado en el artículo 274 “B”, es uno de los elementos de los sistemas de información como lo es: las instrucciones o los programas de ordenador,

esta protección es en cuanto a su funcionamiento. Al respecto el legislador establece en cuanto a la inutilización de las instrucciones, se refiere a que con dolo no se permita utilizar una o varias de las aplicaciones o funciones del programa de ordenador y en cuanto a la inutilización de los programas que utilizan las computadoras se refiere a que estos no pueden ejecutarse o que se encuentran bloqueados.

En este caso, se puede mencionar la denominada bomba de tiempo, que consiste es un programa que se adhiere de forma oculta a los programas de ordenador de los sistemas de información, para que en determinado tiempo o situación generen un bloqueo al funcionamiento del sistema o impidan el acceso a usuarios autorizados.

En la mayoría de estos casos, el sujeto activo son los administradores del sistema, como alguna forma represiva contra los propietarios de empresas; también se dan casos externos, pero, llevan de por medio la comisión de otros ilícitos como estafa y extorsión, al exigir cantidades dinerarias con el objeto de no continuar con el daño a los sistemas informáticos.

2.3.7.2. Delito de reproducción de instrucciones o programas de computación

El artículo 15 del Decreto 33-96 del Congreso de la República, adiciona el artículo 274”C”, al Código Penal el cual estable:

> Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

En este caso, el bien jurídico tutelado son los derechos de autor y derechos conexos del creador del programa de ordenador o la persona a quien cedió sus derechos. En materia de programas de ordenador la persona individual o jurídica titular de los derechos de autor (morales, patrimoniales, conexos) o sus herederos, gozan del derecho exclusivo

a su reproducción, distribución, importación y exportación de copias, accesos, traducción, entre otros derechos.

Lo anterior queda establecido en la Ley de Derechos de Autor y Derechos Conexos Decreto 33-98 del Congreso de la República de Guatemala y determinado en los contratos que celebre con quien cede algunos de los derechos de que goza en su calidad de autor. Se ha podido establecer con base a la información y estadísticas que proporcionan los medios de comunicación y los entes interesados, que el delito de reproducción de instrucciones o programas de computación es el delito informático más cometido a nivel mundial. El acceso a equipo de computación o sistemas informáticos, facilitan la comisión de este delito; a ello se le suma la falta de conocimiento en materia informática en aspectos técnicos y legales, el alto costo de algunos programas de ordenador y los errores en la redacción de los contratos de desarrollo y de licencia.

2.3.7.3. Programas destructivos

El Decreto 33-96 del Congreso de la República de Guatemala en el artículo 19 adiciona el artículo 274" G" al Código Penal, el cual establece:

> Programas destructivos. Será sancionado con prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación. En este caso se protege, de los programas destructivos fundamentalmente dos elementos de los sistemas de información, que son: a) Los registros y b) los programas de ordenador (software).

Existen programas informáticos denominados virus electrónicos, virus digitales o programas perjudiciales.

> En palabras de Téllez (2004): Los virus se definen como, los programas de ordenador que tienen por objeto introducirse en los sistemas informatizados para

causar algún daño a la información, al sistema operativo, a los programas en general y se considera que algunos pueden llegar a dañar el hardware. (p. 26).

Estos programas han causado pérdidas patrimoniales a nivel mundial que se calculan en millones de dólares de los Estados Unidos de América. En Guatemala ha tenido consecuencias de factor económico considerable, pero no existen estadísticas o estudios al respecto para los usuarios.

Entre los programas informáticos perjudiciales, algunos dañan a la propia computadora, mientras que otros utilizan la computadora para atacar otros elementos de la red; es decir, son utilizadas como instrumento o medio; estos programas pueden permanecer inactivos hasta que se desencadena por algún motivo, por ejemplo, una fecha determinada, causando graves daños modificando o destruyendo datos.

Otros programas parecen benignos, pero cuando se activan, desencadenan un ataque perjudicial (los denominados caballos de Troya); otros programas (denominados gusanos) no infectan programas con virus, pero crean réplicas de ellos mismos, estas crean a su vez nuevas replicas y de ese modo se termina por invadir el sistema. Por esta razón las personas que utilizan los sistemas de información deben protegerse, según el nivel de riesgo, con un programa antivirus; los niveles de seguridad dependen de la información y de la interconexión con otras redes.

El tipo penal se perfecciona cuando el programa destructivo se distribuye o se pone en una o varias computadoras, en una red interna o externa o la internet, aquí es cuando concurren todos los elementos que describe el tipo penal, aunque este no logre el daño que se tiene propuesto en virtud de detección o se elimine por un antivirus o se impida el ingreso a la red por cualquier medio.

2.3.7.4. Destrucción de registros informáticos.

"El Decreto Número 33-96 del Congreso de la República de Guatemala, en el artículo 13 adiciona el artículo 274 "A" al Código Penal el cual establece:

Destrucción de registros informáticos. Será sancionado con prisión de seis meses a cuatro años y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos.

La pena se elevará en un tercio cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial. El bien jurídico se define como registro informático, que consiste en la base de datos creada por el sistema informático utilizada para la toma de decisiones.

El artículo 274 "A" establece tres verbos rectores destruyere, borrare o de cualquier modo [...]; en ese sentido destruir información se refiere a que el sujeto activo del tipo penal destruya la información, lo que equivale a cambiar su naturaleza de tal forma que no pueda recuperarse por medios electrónicos (el original instalado). Al establecer borrare, se refiere a eliminar de forma física de los dispositivos de almacenamiento la información.

La frase o de cualquier modo deja abierta una variedad de posibilidades, como en el caso que con intención se grabe información sobre la existente, o utilice algún dispositivo para afectar el acceso a los registros informáticos.

Aunque la victima cuente con una copia de seguridad de la información, no es causa para eximir de responsabilidades al sujeto activo. El artículo 274 "A" también divide los registros en privados y públicos, considerando como un agravante cuando es contra los registros públicos.

Debido a ello, se estima que en ausencia de legislación que determine que debe entenderse por registro públicos se interpreta que se refieren a los registros informáticos a cargo de la administración pública y que contienen datos personales. Otro criterio establece que se refiere a la naturaleza de los datos o información; es decir, que los registros serán públicos aun cuando sean almacenados, procesados y/o automatizados por un ente privado.

2.3.7.5. Uso de información

El Decreto Número 33-96 del Congreso de la República de Guatemala en el artículo 18 adiciona el artículo 274 “F” al Código Penal el cual establece:

> “Uso de Información. Se impondrá prisión de seis meses a dos años y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos”.

En este caso se puede determinar que se protegen dos aspectos:

a) Los registros informáticos, en lo que se refiere a la utilización no autorizada y
b) El acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos.

Los cuales se desarrollan a continuación.

a) Registros informáticos

La persona que crea un registro informático de datos lícitos, tiene la facultad de disponer de quienes tendrán autorización para hacer uso de este. La utilización autorizada de los registros puede ser directa al computador que los tiene almacenados, en línea (red interna y externa) e inclusive pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas e

inclusive un usuario autorizado para acceder al sistema, pero no para utilizar de forma distinta los registros informáticos.

Cuando un sujeto sin la autorización del titular de ese registro informático hace uso de este, estaría incurriendo, entonces, en el delito de uso de información. El artículo 274 “F”, contiene una forma de redacción muy limitada y puede hacer incurrir a los encargados de administrar justicia en error. En el caso de utilizar esos registros informáticos en otro sistema de información automatizado, se estaría incurriendo en el delito establecido, le genere ese uso lucro o no. Se puede dar la situación de que sea una persona, quien extrae el registro y otra persona la que lo utilice en su sistema, esto puede estar en concurso con otros delitos.

El simple uso de ese registro informático lo que convierte al mismo en delito, en virtud que es necesario determinar algunas características de esa información (que sean datos automatizados) para establecer si es ilícita o no esa conducta. Un ejemplo claro es cuando una persona visita un sitio web por motivos de investigación, trabajos académicos, estudios y en su trabajo hace uso de un registro informático sin la autorización, pero hace la correspondiente referencia.

b) Acceso no autorizado a los bancos de datos o archivos electrónicos

Para poder ingresar a un sistema de información se debe estar autorizado, esta aprobación de acceso consiste, en el permiso que se le otorga a un usuario para poder hacer uso del sistema de información.

Un ejemplo de autorización a un sistema informático es el que se utiliza en las entidades bancarias: en estos casos los trabajadores tienen autorización para ingresar a determinados niveles del sistema; el receptor pagador del banco tiene acceso para administrar e ingresar información al sistema en el ingreso o retiro de cantidades en las cuentas bancarias, pero no puede acceder a los estados de cuenta de la persona titular de la cuenta, el jefe de la agencia bancaria si tiene esta última competencia, pero no

puede otorgar transferencias electrónicas por determinados montos, las cuales deben ser autorizadas por el superior de este y así consecutivamente (según esté diseñado el sistema). Cuando el acceso al sistema lo realiza una persona que no está autorizada se encuadra esa acción a este delito. Es importante señalar que el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, inclusive si no realiza ninguna acción con la información.

2.3.7.6. Manipulación de información

El Decreto Número 33-96 del Congreso de la República de Guatemala en el artículo 17 adiciona el Articulo 274 “E” al Código Penal el cual establece:

> Manipulación de Información. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica. Este tipo penal lo comete el titular, propietario o usuario de los datos, cuando utilizando programas de computación o registros informáticos diseñados para incumplir obligaciones con el Estado o engañar a otras personas altera la información automatizada.

Este tipo penal parte de dos supuestos: el primero ocultar que se refiere a esconder los datos para que no puedan ser encontrados; el segundo alterar o distorsionar se refiere a cambiar los datos o darles a los datos un valor distinto al real. Además, debe determinarse el grado de participación de la persona que es autor o creador del programa de computación que permite esa administración ilícita de la información, la participación de la persona que ingresa la información y la persona que la utiliza; en el caso del autor del programa la norma establece: al que utilizare [...], si el programador se limita a diseñar el programa conforme la solicitud del contratante no tendría ninguna responsabilidad en virtud que él no lo utiliza.

En cuanto a la persona que ingresa los datos, tampoco tendría responsabilidad, porque ingresar datos para esconderlos, duplicarlos o alterados, no es un delito. La persona que los utiliza, que realiza la acción de ponerlos en conocimiento del Estado o de otra persona es la que comete el ilícito. Si el que ingresa los datos tiene conocimiento posterior del hecho tipificado como delito tendría la calidad de encubridor y si tiene conocimiento que van a ser utilizados con fines ilícitos tendría participación como autor o cómplice, según el caso.

2.3.7.7. Registros prohibidos

El Decreto Número 33-96 del Congreso de la República de Guatemala en el artículo 16 adiciona el artículo 274 “D” al Código Penal el cual establece:

“Registros prohibidos. Se impondrá prisión de seis meses a cuatros años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas. El bien jurídico es la intimidad de la persona, pero para poder definir de mejor forma este bien jurídico es importante determinar que son datos personales.

Al respecto la Ley de Acceso a la Información Pública Decreto 57-2008 del Congreso de la República de Guatemala en el artículo nueve numeral 1 define los datos personales como:

> Los relativos a cualquier información concerniente a personas naturales o identificables. Se entiende entonces que los datos personales es la Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

La Ley de Acceso a la Información Publica también regula una definición de datos sensibles o datos personales sensibles, en el artículo 9 numeral 2, el cual establece:

> Que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico , las ideologías y opiniones políticos, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencias o vida sexual, situación moral y familiar u otras cuestiones intimas de similar naturaleza".

Entonces datos sensibles son aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

> Se define como intimidad o privacidad, el derecho del individuo a ejercer el control de aquella información de sí mismo, que desee compartir con otros, de la cantidad que de esta facilite a otros del momento en que desee hacerlo. La violación a esta norma surge cuando se crean bases o bancos de datos que al ser administrados de forma inadecuada o bien adquiridos de una forma ilegal, que entren en la esfera de la intimidad de las personas se estaría cometiendo el delito de registros prohibidos. (Portillo, 2012, p. 23).

Con esta aproximación, se estima que se proyecta una definición generalizada de lo que debe concebir como intimidad y que es lo que se estima y debe proteger en gran medida el derecho, pues en el proceso de interactuar en redes informáticas, es uno de los aspectos que puede resultar vulnerado.

2.4. Iniciativas para su tipificación en Guatemala

"En el Congreso de la República de Guatemala, existen actualmente tres iniciativas de ley que tienen por objeto, tipificar conductas delictivas realizadas por medio de las tecnologías de la información, conocidas convencionalmente como -TIC-, pero que

por diversas circunstancias continúan entrampadas, limitando la regulación eficiente y eficaz de todos los aspectos estrechamente vinculados con la informática".

2.4.1. Iniciativa de ley contra el cibercrimen 4054

"La iniciativa de Ley contra el Cibercrimen identificada con número el 4054 fue conocida en el Congreso de la República el día dieciocho de agosto de dos mil nueve. Dentro de la exposición de motivos, se menciona lo siguiente: que, con el crecimiento exponencial de usuarios de Internet, se abre la puerta a la comisión de un mayor número de ciberdelitos [...] lo que remarca la importancia de contar con medidas especiales de prevención, detección e inicio de acciones judiciales contra los ciberdelincuentes".

"A diferencia de otros delitos, el cibercrimen cuenta con características distintivas comunes como son la novedad, la potencialidad lesiva, la cualificación técnica del autor, su dimensión transnacional, su constante evolución y, derivado de todo ello, la dificultad de su persecución. Con el incremento del uso de Internet como medio para realizar transacciones en línea en las que los usuarios deben indicar datos personales, los delincuentes informáticos buscan la forma de acceder a esa información con el objetivo de utilizarla posteriormente, ya sea con fines lucrativos o de otra índole. La Delincuencia informática ha evolucionado en forma exponencial en las últimas décadas; de los denominados hackers tradicionales la amenaza ha pasado a estructuras organizadas que utilizan la más alta tecnología para llevar a cabo delitos informáticos organizados, sistemáticos y complejos para su persecución penal".

"Existe la necesidad que en Guatemala exista una normativa legal que tipifique y regule las distintas conductas antijurídicas a través de la Internet, que se regulen los medios de investigación especial que han de aplicarse para la investigación de un hecho delictivo cometido en estas circunstancias".

"La iniciativa de ley 4054 contiene una serie de tipos penales que no se encuentran regulados dentro del Código Penal, como los códigos de acceso, clonación de

dispositivos de acceso, acceso ilícito, acceso ilícito para servicios a terceros, dispositivos fraudulentos, interceptación e intervención de datos o señales, daño o alteración de datos, sabotaje, atentado contra la vida de la persona, robo mediante la utilización de alta tecnología, obtención ilícita de fondos, estafa especial, chantaje especial, robo de identidad, falsedad de documentos y firmas, uso de equipos para invasión de privacidad, comercio ilícito de bienes y servicios, difamación especial, injuria pública, atentado sexual, pornografía infantil, delitos relacionados con la Propiedad Intelectual y afines, y delitos de telecomunicaciones".

"Se regula la creación una Comisión contra Crímenes y Delitos de Alta Tecnología (CDAT), con la finalidad coordinar y cooperar con gobiernos e instituciones nacionales e internacionales para prevenir y reducir la comisión de actos ilícitos de alta tecnología en la República de Guatemala y en el resto del mundo".

2.4.2. Iniciativa de ley de Delitos Informáticos o Cibercrimen 4055

"El proyecto de ley de Delitos Informáticos o Cibercrimen, el cual está identificado con el número 4055 del Congreso de la República de Guatemala, tiene como objeto y finalidad proteger":

a) "Los derechos de las personas en cuanto a la integridad, disponibilidad y confidencialidad de los sistemas que utilicen tecnologías de la información y sus componentes, a fin de garantizar certeza jurídica en las transacciones propias del comercio electrónico y, así, armonizar y contribuir con las disposiciones internacionales relacionadas con la prevención y sanción de los delitos informáticos".
b) "Contrarrestar los ataques cibernéticos de conformidad con la normativa nacional e internacional".

Al analizar el contenido del proyecto de ley 4055, se puede entender que esta ley pretende proteger los bienes jurídicos siguientes:

a) “La información: en cuanto a sus atributos consistentes en la integridad, disponibilidad y confidencialidad”.
b) “El patrimonio: el proyecto de ley busca sancionar todos aquellos actos de transferencia patrimonial no consentida por el propietario, así como lo relativo al daño informático”.

Se incluyen dentro del proyecto de ley 4055, normas relativas a la seguridad del Estado y se regulan delitos contra el pudor y el honor de las personas.

Acorde con esto, la República de Guatemala, así como los demás Estados debe poner la importancia debida y atención en lo que se refiere a Ciberseguridad, los ataques cibernéticos pueden afectar a la infraestructura estratégica de cualquier país, incluido Guatemala, relacionadas con sectores de mucha importancia, como el transporte, las telecomunicaciones, servicios de electricidad, de agua potable, el sistema financiero, servicios de salud, entre otros.

Los delitos informáticos trascienden el mundo virtual y afectar en el mundo material, en el mundo de los átomos, esto se evidencia por ejemplo en un ataque informático al sistema que controla la red de semáforos de una ciudad o como los casos más comunes al sistema informático de una institución bancaria o financiera.

2.4.2.1. Ámbito de aplicación del proyecto de ley 4055

Es compleja la aplicación de una ley que tiene por objeto sancionar actos realizados en un espacio virtual o el denominado ciberespacio, derivado de que constituye un espacio físico o geográfico. “Goodman (Alvarado, 2008) define el ciberespacio como “un ambiente intangible; no es un mundo de átomos y células, sino digital. Los bytes no tienen peso, olor ni color y viajan a la velocidad de la luz” (p.26).

Se hace una referencia abstracta del mundo digital el cual no se puede tocar, oler o sentir, se sabe que existe por sus manifestaciones en el mundo exterior, pero es

imperceptible a nuestros sentidos, ahí radica su complejidad en cuanto a su persecución y procedimiento probatorio.

La red informática mundial, conocida como internet, es utilizada como un medio de comunicación internacional, carece de límites políticos, límites geográficos; pero aun así todos los actos realizados a través de la internet no deben atacar o vulnerar derechos fundamentales de las personas, como el honor, la dignidad, la propiedad ni debe vulnerar las leyes, las buenas costumbres ni la moral.

Brenna (2001) comenta sobre la internet e indica que: "esta consiste en un espacio no territorial, no geográfico y que, por su sola existencia genera interrogantes y problemas al mundo legal conocido, fuertemente atado a lo geográfico por la cuerda de las soberanías" (p. 26).

Se hace una referencia al principio territorial de las leyes, principalmente a la ley penal de cada país, aún y cuando existe el principio de extraterritorialidad el cual describe los casos en que una ley penal puede aplicarse fuera de los límites geográficos existentes, pero en el caso de los delitos informáticos estos principios son complicados de aplicar, al estar la internet carente de fronteras físicas.

El territorio de un Estado no puede confundirse como espacio geográfico, entendiendo que el concepto de territorio es más complejo, comprende todos los lugares a los que se puede extender la soberanía de un Estado, lo que incluye, ordenadores, redes y sistemas informáticos.

No se pretende profundizar en la discusión de los alcances extensivos de la soberanía del estado sobre la internet o sobre la existencia de una soberanía digital, debido a las asignaciones de dominios para cada país. Algunos países como Colombia, por ejemplo, han declarado que los dominios con el sufijo de su país constituyen bienes de interés público, para que estos no sean comercializados, por considerar que identifican a un país o región. Lo que realmente resulta importante, en la esfera jurídica,

es la determinación del lugar de origen y de producción de las consecuencias jurídicas del tipo penal informático, debido a que, esos lugares si constituyen parte de un espacio territorial, donde existen normas de derecho emanadas de un Estado.

El único aspecto de atención es en cuanto a los límites de la soberanía de un Estado pues una investigación profundiza en las redes de otro Estado. Todos estos inconvenientes podrían solucionarse con una normativa en materia de cooperación internacional o asistencia jurídica mutua. El concepto de ciberespacio no debe causar ningún tipo de confusión en cuanto a la determinación del lugar donde se comete la acción ilícita informática o del lugar donde surte sus efectos. Internet tiene obligadamente, una infraestructura física ubicada en determinado lugar y es precisamente en ese lugar de ubicación donde podemos establecer el origen del delito o sus consecuencias.

Dentro de la Teoría General de la Ley Penal, el Código Penal regula, específicamente en los artículos 4 y 5, lo relativo al ámbito espacial de validez de la ley penal, se estudia el ámbito de aplicación de la ley por actos realizados dentro y fuera del territorio nacional, por parte de autores y cómplices de acuerdo con el grado de participación de los sujetos activos, como una manifestación de la soberanía del Estado.

En ese sentido en materia de delitos informáticos debe tomarse en consideración el siguiente ámbito de aplicación de la ley.

a) Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional. En este caso el sujeto activo se ubica dentro del territorio nacional y origina la acción delictiva haciendo uso de redes y sistemas que utilizan tecnologías de la información del lugar en el cual surta efectos. Corresponde a los peritos en informática forense que participen en la investigación criminal, con la colaboración de los proveedores de servicio de internet, determinar el lugar físico en el cual se originó la acción delictiva. Actualmente del lugar físico se podría establecer por diferentes métodos o formas de seguir el trazo o ruta utilizada por

el sujeto activo, pudiendo ser mediante un informe de la IP (número identificador designado computador en una red), utilizada en el caso concreto.

b) Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero produciendo efectos en el territorio nacional. La acción delictiva opera a la inversa que, en caso anterior, surtiendo efectos en el territorio nacional. Como ejemplo de este caso sería cuando se conozca una acción delictiva de fraude informático originada en el extranjero, pero afectando el patrimonio ubicada en el territorio nacional.

c) Cuando el origen o los efectos de la acción se produzcan en el extranjero utilizando medios que se encuentran en el territorio nacional. El origen o los efectos de la acción delictiva se producen en el extranjero, pero se utilizan medios o equipos ubicados en el territorio nacional. Como en el caso de las redes robóticas (botnets), donde las instrucciones o programas pudieran tener origen en el extranjero, utilizando computadoras o equipos ubicados en Guatemala, para cometer delitos que surten efectos en el extranjero.

d) Cuando se caracterice cualquier tipo de complicidad desde el territorio guatemalteco. La ley penal establece que son cómplices, entre otros, quienes proporcionen, informen o suministren medios adecuados para realizar el delito o quienes sirvieren de enlace o actúen como intermediarios entre los partícipes, para obtener la concurrencia de estos en el delito. De esta manera es razonable que, para poder caracterizar cualquier tipo de complicidad, desde el territorio guatemalteco, debemos de sujetarnos a lo que establece el artículo 37 del Código Penal. Sería el caso las alianzas para ataques cibernéticos que promueven los hacker-activistas, para dañar algún sistema informático, un caso concreto es el ataque a los sistemas informáticos de la Oficina Federal de Investigación, organizado por el grupo Anonymous, en donde participaron cerca de diez mil personas de diferentes países, haciendo uso de más de veintisiete mil ordenadores o equipos de cómputo.

e) El proyecto de la ley 4055. Este regula que cuando el origen o los efectos hayan sido producidos en el extranjero, serán competentes los tribunales guatemaltecos, en el caso que en el extranjero no se hubiese dictado sentencia firme por el mismo hecho o el sujeto activo hubiere evadido la persecución penal en tribunales extranjeros. (Alvarado R. y., 2016, p. 76).

2.4.2.2. Delitos de acción pública

El catálogo de tipos penales que regula el proyecto de ley 4055, se establece que: Son de acción pública, lo que significa que son actos delictivos que deben ser perseguidos penalmente de oficio por el titular de la acción penal; es decir, el Ministerio Público, no siendo necesaria la denuncia por parte de la víctima o agraviado.

Para lograr una mejor y efectiva investigación, por parte del Ministerio Público, se determinó que resultaba necesario que los delitos informáticos fueran considerados delitos de acción pública, esto debido a que los ilícitos informáticos atentan contra bienes jurídicos colectivos como los del patrimonio.

La iniciativa de Ley identifica con el número 5254, fue presentada al pleno del Congreso de la República con fecha ocho de marzo de dos mil diecisiete y en la exposición de motivos se hace referencia al acelerado avance de la tecnología en la mayoría de los ámbitos de actuación de los ciudadanos del país y el aumento en el uso de las tecnologías de las comunicación e información, lo que ha causado el aumento de hechos ilícitos donde son vulnerados bienes relacionados con la información, la informática, la intimidad de las personas, entre otros y donde los medios informáticos son utilizados como instrumentos para cometer estas conductas ilícitas".

Se hace referencia en la iniciativa de ley, que en la tipificación actual de los delitos informáticos contenidos en el Código Penal, no responde a las modalidades de los ilícitos que se cometen a través de las redes o sistemas informáticos, haciendo énfasis que a

nivel internacional se encuentran reguladas una serie de conductas ilícitas informáticas actualizadas y que a nivel nacional es necesario que se actualice la legislación en materia de delitos informáticos y se adecúe al Convenio Sobre Ciberdelincuencia de Budapest, suscrito en el año 2001, el cual es no ha sido ratificado por Guatemala y en la iniciativa se sugiere la adhesión ratificación de este Convenio para lograr la cooperación internacional y contribuir al combate de los delitos informáticos a nivel global.

2.4.3. Iniciativa de ley 5254 sobre ciberdelitos

La iniciativa de ley 5254 da una relevante importancia a lo establecido en el Convenio Sobre Ciberdelincuencia de Budapest, considera que lo regulado en el Convenio se debe tomar en cuenta su texto sin reservas de ningún tipo, derivado que responde a la búsqueda de protección a la sociedad frente al fenómeno de la Cibercriminalidad.

Al hacer un análisis, se establece que esta contiene una serie de definiciones, con el objeto de una mejor interpretación y entendimiento de esta, toda vez que por la materia que se está regulando existen conceptos muy técnicos que son necesarios desarrollar, definiciones que también son desarrollados en el Convenio Sobre Ciberdelincuencia. La iniciativa enumera los bienes jurídicos que se pretenden proteger siendo estos: los datos personales y la intimidad informática, la indemnidad sexual de los menores, la confidencialidad, la integridad y la disponibilidad de la información y datos contenidos en sistemas informáticos o sistemas que utilicen tecnologías de la información y las comunicaciones o transmitidos por esos medios, así como los bienes, activos y pasivos patrimoniales representados en las transacciones u operaciones o financieras que se realicen por esos medios; importante es que en esta iniciativa se amplían los bienes jurídicos a los que se regulan actualmente en el Código Penal en materia de delitos informáticos, incluso en la iniciativa se regula la derogación de los artículos 274 “A”, 274 “B”, 274 “E” y 274 “F”, derivado que la iniciativa regula conductas que se asemejan a las establecidas en el Código Penal, pero descritas de una forma más técnica y adecuada a la actualidad, por lo que se hace necesaria la derogación de estos tipos existentes.

También se regula lo relativo a la territorialidad y extraterritorialidad de la ley en materia de delitos informáticos, toda vez que al ser el ciberespacio el lugar donde ocurren la mayoría de las acciones ilícitas informática, siendo un espacio no material, puede que los hechos se cometan en diferentes países, ya sea porque autor y víctima estén en países diferentes o bien que se utilicen o se afecten bienes plataformas informáticas en diferentes países; regula también la responsabilidad de las personas jurídicas, incluyendo a los proveedores de servicios cuando se establezca la participación de representantes de estas entidades en la comisión de delitos informáticos.

En la iniciativa se establece que la acción para perseguir estas conductas es de oficio, siendo obligación del Ministerio Público el inicio de la persecución al solo tener conocimiento por cualquier medio de la posible comisión de una de las conductas reguladas en la iniciativa de ley a excepción del delito de *Acceso ilícito,* regulado en el artículo 8, que regula que la acción será pública dependiente de instancia particular, salvo que se vean afectados datos protegidos por la ley o afectaciones masivas.

Los tipos penales que regula la iniciativa de ley son estos que están descritos en el Convenio, a excepción de los descritos en los artículos 13, 18 y 19 el primero Apropiación de identidad ajena, se encuentra dentro de los delitos informáticos propiamente dichos y describe la conducta que realiza una persona, quien con dolo sin estar autorizado o excediendo la autorización que poseyere, sin el consentimiento del titular de la identidad y con el fin de cometer un delito, obtenga o adopte la identidad de un tercero, por medio de un sistema informático o que haga uso de las tecnologías de la información y las comunicaciones.

El artículo 18 hace referencia al tipo penal de Acoso por medio cibernéticos*,* comete este delito, quien, por medio de sistemas informáticos o cualquier medio de comunicación electrónica, de forma recurrente o repetitiva, acose a una persona por medio de ataques personales o divulgación de información confidencial o falsa; y el artículo 19 regula el tipo penal de Delito contra la integridad sexual de una menor o contacto a menor con fines sexuales a través de las Tics., describe este tipo penal aquella

conducta cometida por una persona mayor de edad que contacta a una menor de edad utilizando las tecnologías de la información y las comunicaciones, con el objetivo de ganarse la confianza de la menor y concertar un encuentro en un lugar físico, para cometer cualquier delito que atente contra la sexualidad de la menor, regulado en el Código Penal".

En los tres casos se observa que el medio utilizado para cometer el ilícito son los sistemas informáticos o las tecnologías de la información y las comunicaciones; en el primero, con el objeto de obtener una identidad de un tercero para poder cometer otro hecho ilícito; en los dos últimos casos que se encuentran regulados en el Capítulo III de los Ciberdelitos contra las personas, los sistemas informáticos y las Tics. son utilizados como instrumentos para consumar el delito, en ambos, se protege la indemnidad sexual de las personas, principalmente la de las menores de edad.

Se regula dentro de la iniciativa, aspectos procedimentales en cuanto al resguardo, presentación y secuestro de datos informáticos, con el objeto de obtener indicios para el desarrollo de la investigación; sin embargo, no regula aspectos técnicos para el adecuado manejo, manipulación y embalaje de los indicios digitales, para asegurar su preservación, no contaminación ni alteración.

Se estima que uno de los aspectos de relevancia que contiene la iniciativa de ley, es la creación del Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica, ante incidentes informáticos-Guatemala, CSIRT-GT, organismo que se encargará de forma permanente a detectar y dar atención eficaz y eficiente a las emergencias y casos de Ciberseguridad, así como realizar acciones de prevención de ataques a los usuarios de sus sistemas informáticos y sus datos. Será una dependencia del Ministerio de Gobernación, será el ente encargado de la Ciberseguridad a nivel nacional y deberá hacer las alianzas a nivel internacional con otros equipos de respuesta para poder combatir y prevenir en forma global el fenómeno de la cibercriminalidad.


ESCUELA DE ESTUDIOS DE POSTGRADO
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
USAC
SECRETARÍA

Capítulo III
3. La evidencia digital

3.1. Antecedentes

En torno a este apartado histórico de lo que se conoce como evidencia digital, se debe realizar primero un análisis a la institución de la prueba penal, es pertinente señalar algunas concepciones doctrinarias, a fin de contrastar el momento histórico en el que se dieron los primeros pasos sobre su consideración dentro de un litigio, conflicto o debate como se le conoce en la actualidad.

> Desde el surgimiento de las primeras formas o intentos de derecho positivo, por ejemplo: El denominado Código de Hammurabi, que era un conjunto de reglas escritas en una estela de piedra, del pueblo sumerio, en el cual predominaban sanciones draconianas, como la llamada Ley del Talión; se aprecia, que ya se manifiesta, aunque de manera muy embrionaria el derecho a probar. En efecto, en dicho conjunto de normas, tan antiguo, denominado por muchos primitivo, se vislumbra ya la necesidad de probar, en un afán humano tan importante como la vida misma: determinar a los responsables de un crimen sin perjudicar a los inocentes. Allí igualmente, se vislumbran, primitivos afanes, por defender lo que hoy en día conocemos como un principio sustancial, que se encuentra hondamente ligado al derecho penal y a la prueba: el Principio de Presunción de Inocencia. (Ortíz Nishihara, 2017, parr. 3). (párr. se tilda)

Es una forma generalizada de concebir los registros históricos de la prueba penal, en ese orden de ideas, se requiere profundizar en torno a estos preceptos, para el efecto, se plantea la siguiente definición:

El derecho penal resulta tan antiguo como la humanidad, básicamente, porque rige o regula en esencia el accionar del ser humano, consecuentemente se aplica cuando se realizan acciones y/o omisiones que ponen en peligro un bien jurídico protegido por

alguna ley en particular; el derecho penal empezó a evolucionar luego de suscitarse el periodo o época de la venganza privada, en donde cada uno se procuraba justicia por mano propia. Esta circunstancia fue posteriormente atenuada por la ley del talión que era una venganza proporcional al daño ocasionado al sujeto pasivo, surgiendo luego otra forma de venganza privada, conocida oportunamente como la composición, la cual se presentaba cuando el ofensor entregaba al ofendido o a su familia cierta cantidad de bienes o especies para no padecer en carne propia, la venganza de los ofendidos.

De ahí que tanto en la venganza privada cómo en la venganza divina la aplicación del derecho penal, la prueba se obtenía en forma primitiva por medio de supersticiones y los jueces se apegaban a encontrar la verdad de los hechos delictivos a través de la manifestación de la divinidad, no utilizando la razón para la solución de los diversos casos sometidos a su conocimiento, siendo esto una forma de derecho penal primitivo, en sus manifestaciones sustantiva, adjetiva y probatoria.

El derecho procesal penal fue evolucionando de conformidad con los sistemas políticos que surgieron durante la historia, por lo cual en esta evolución se llegó al punto en que los jueces tenían que aplicar la razón en la valoración de los elementos de prueba en los hechos penales sometidos a su conocimiento, apareciendo los sistemas inquisitivo y acusatorio; es a partir de estos sistemas donde surgió netamente la institución que hoy se denomina prueba penal.

Se comprende con mucha mayor precisión, los aspectos que engloban el concepto de prueba, esencialmente en cuanto a sus registros históricos, cuando se inició con su utilización y que demuestra la forma en que gradualmente se ha ido perfeccionando y en el caso de la legislación guatemalteca, hasta quedar plasmado en el Decreto Número 51-92 Código Procesal Penal.

> Un adagio latino, por demás evidente, proclama: *demonstrationis veritas* (prueba es la demostración de la verdad). Lo arduo, dada la infinidad de las convicciones humanas, consiste en establecer cuando está algo demostrado; si bien el problema

> se reduce en lo procesal, por cuanto la parte triunfa cuando logra que el juzgador admita como real lo que ella afirma o que desconozca lo que ella niega. Las partidas entendían por prueba la averiguación que se hace en juicio de alguna cosa dudosa o bien la producción de los actos o elementos de convicción que somete el litigante, en la forma que la ley previene, según derecho, para justificar la verdad de los hechos alegados en el pleito. (Turtón Ávila, 2011, p. 68).

De acuerdo con esta concepción, es importante señalar que el estudio de los elementos de prueba a través del desarrollo evolutivo del derecho penal, ha variado considerablemente desde su inicio hasta la época actual, esto es debido a que en sus inicios o en la llamada época de la venganza privada, donde las personas en virtud de la violencia que existía, no hacían mayor cosa por averiguar la verdad de los hechos, sino se dedicaban a ocasionar un daño como el que se les había causado, con sus propias manos, por lo que no existían normas jurídicas que regulaban como se debía de probar los delitos u ofensas que cometían las personas dentro de la sociedad.

En la segunda época del derecho penal, se consideraban únicamente las pruebas que recaudaba la iglesia a través de sus sacerdotes en los juicios divinos, sin importar los procedimientos a través de los cuales se incorporaban al proceso, en ese contexto, eran formas muy violentas, sin que la contraparte pudiera hacer efectivo el principio de defensa.

Durante la época de la venganza pública, aparecen las primeras leyes penales, en donde se regulan la totalidad de los elementos probatorios, pero el principal siguió siendo la confesión, la cual podía ser obtenida a base de la tortura u otras formas violentas que en la actualidad son abiertamente ilegales.

El concepto de prueba penal ha sido desarrollado por varios autores, para Eugenio Florián (1995) “se entiende por prueba todo lo que en el proceso penal puede conducir a la determinación de los elementos necesarios al juicio con el cual termina” (p..305);

Acorde con ello, se considera entonces que la prueba en el proceso penal, como anteriormente se expuso, es el instrumento indispensable para comprobar la hipótesis planteada por el ente acusador en el proceso penal, sin prueba no es posible fundamentar una sentencia condenatoria.

De acuerdo con Cafferata (1998) “Todo lo que pueda servir para el descubrimiento de la verdad acerca de los hechos que en aquel son investigados y respecto de los cuales se pretende actuar la ley sustantiva” (p. 4).

Con este planteamiento se refuerza el hecho de considerar que el proceso penal es el medio por el cual se hace cumplir el derecho penal sustantivo, toda vez que la ley sustantiva contiene el catálogo de conductas prohibidas, que en caso de realizarse alguna de estas conductas el responsable resulta merecedor de una sanción, conocida como pena. Se puede entonces definir a la prueba penal como todo elemento objetivo tangible o intangible, cuya incorporación y diligenciamiento controlado por un juez sirve para el establecimiento de la verdad en un proceso penal.

Existen diferentes acepciones de lo que se conoce como prueba, incluso se ha llegado a utilizar como sinónimos; sin embargo, son aspectos deben ser estudiados en forma separa, por lo que resulta no hacer relación de acepciones, sino aspectos que integran el concepto de prueba. De ahí que se pueda distinguir entre órgano de prueba, medio de prueba, elemento de prueba y objeto de prueba.

En primer lugar, se hace referencia a elemento de prueba, es lo que se conoce como prueba propiamente dicho, indica Vélez Mariconde (2006) “Es todo dato objetivo que se incorpora legalmente al proceso, capaz de producir un conocimiento cierto o probable acerca de los extremos de la imputación delictiva” (p. 19). Elemento de prueba, hace referencia a la prueba en sí misma, es el resultado del acto de producción de la prueba, es todo dato, señal o rastro el cual es introducido de forma legal al proceso, que contribuye al convencimiento del juez para resolver los casos penales.

Órgano de Prueba, se denomina de esta forma al sujeto que proporciona dentro de un proceso penal, elementos que ayudan al conocimiento de los hechos objeto de la investigación. Su principal función es la ser un intermediario entre la prueba y el juez; puede como un testigo, por haber percibido a través de sus sentidos alguna circunstancia de utilidad para la averiguación de la verdad, también como perito, una vez sea requerido ya sea por el Ministerio Público o por orden de juez, para que utilizando su conocimiento extraiga de un elemento datos útiles y necesarios para el esclarecimiento de los hechos.

Otros aspectos que se deriva del concepto de prueba es el Medio de Prueba, se denomina de esta forma al procedimiento establecido en el Código Procesal Penal, para que ingrese al proceso un elemento de prueba, el cual se encuentra fuera de él, ingrese al proceso para ser conocido por los jueces y demás partes. En este sentido la ley regula la forma en que ha de introducirse cada medio de prueba en particular. En el Código Procesal Penal aparecen como medios de prueba el testimonio, el dictamen pericial, el documento, así como las actividades que se realizan con autorización judicial en el caso de las diligencias de inspección y registro.

El último aspecto que se puede estudiar del concepto de prueba es el Objeto de la Prueba, se hace referencia a todo aquello que puede ser probado, todo sobre lo cual debe o puede recaer la prueba. En cualquier proceso penal, la prueba deberá de versar sobre la existencia de un hecho que reviste las características de delictivo, la prueba debe dirigirse a individualizar plenamente a las personas que participaron en el hecho, ya sea en su calidad de autor o de cómplices, así como las circunstancias que agraven, atenúen, o en algún caso justifiquen la acción realizada, debe ser objeto de prueba la extensión del daño que se ha causado por la conducta delictiva, así como las circunstancias de tiempo, modo y lugar.

La prueba es el único medio confiable que existe para alcanzar dicha reconstrucción anteriormente mencionada de manera demostrable y comprobable. Todo ello es determinante para la convicción de la culpabilidad que se necesita para poder condenar basándose en la prueba que se encuentre incorporada al proceso.

La prueba es todo aquello que puede ser de utilidad para poder descubrir la veracidad relacionada a los hechos que dentro del proceso penal guatemalteco se investigan y en relación de lo que pretende una actuación de ley sustantiva. Es el único medio eficaz para el descubrimiento de la justicia y por ende de la verdad y también constituye la mejor garantía en contra de todas aquellas arbitrariedades existentes de las decisiones judiciales.

3.2. Definición

Previo a abordar el concepto de evidencia digital, resulta necesario realizar un breve recorrido por los principales elementos que han influenciado y determinado lo que en la actualidad se considera como evidencia o prueba dentro del proceso penal, para el efecto es necesario iniciar con lo relativo al concepto de indicio para posterior al de prueba indiciaria.

Según Dellepiane (2005) “indicio es todo rastro, vestigio, huella, circunstancia y en general, todo hecho conocido, mejor dicho, debidamente comprobado, susceptible de llevarnos por la vía de inferencia, al conocimiento de otro hecho desconocido” (p. 101).

En relación con este planteamiento, el hecho considerado en concreto debe estar debidamente probado, para que adquiera la categoría de prueba, en el momento procesal oportuno y que ese hecho comprobado en virtud de una inferencia lleva al conocimiento de otro hecho desconocido; en esencia, la prueba indiciaria consiste en una actividad probatoria de naturaleza necesariamente discursiva e indirecta, cuya fuente es un dato comprobado y se concreta en la obtención del argumento probatorio mediante una inferencia correcta, que posteriormente va adquiriendo un sustento mucho más concreto, hasta convertirse en prueba.

Sobre el concepto de prueba indiciaria, Desimoni (1993) expone al respecto, lo siguiente "es la reunión e interpretación de una serie de hechos y circunstancias relativos

a un injusto determinado que se investiga, a efectos de intentar acceder a la verdad de lo acontecido por vía indirecta" (p. 98).

El autor pretende exponer que a través de la prueba indiciaria lo que se hace es probar directamente los hechos mediatos para deducir de estos aquellos que tienen un gran significado para la causa que se pretende probar.

> La prueba circunstancial se basa en el valor incriminatorio de los indicios y tiene, como punto de partida, hechos y circunstancias que están probados y de los cuales se trata de desprender su relación con el hecho inquirido, esto es ya un dato por complementar, ya una incógnita por determinar, ya una hipótesis por verificar, lo mismo sobre la materialidad del delito que sobre la identificación del culpable y acerca de las circunstancias del acto incriminado. (Nación, 2011, p. 3).

La prueba circunstancial puede ser explicada de una mejor manera con huellas dactilares, que pueden probar la presencia de una persona en particular en la escena del delito o su contacto con un objeto utilizado en el delito.

El proceso penal está invariablemente dictado a la toma de una decisión jurisdiccional, que solamente puede referirse a un punto de hecho o a un punto de derecho. La decisión se refiere a un punto de hecho cuando se trata de saber si este es verdadero o no, caso en el que solo se puede tener como base a las pruebas. Cuando se trata de saber cuál es la ley aplicable en un supuesto determinado, el derecho que concede o la obligación que impone, la decisión se refiere a un punto de derecho. Para tomar una decisión, el juez debe tomar todas las pruebas, estudiarlas, compararlas y decidir su fuerza probatoria. Puede entenderse la prueba como un elemento verdadero que es motivo de credibilidad sobre la existencia o inexistencia de otro hecho. Es por ello por lo que Las decisiones judiciales son conclusiones que se basan en pruebas, es decir, dado un hecho se concluye la existencia de otro. La prueba directa es la que, generalmente, consiste en una afirmación pura y simple de algo que ha llegado al conocimiento de alguien a través de sus propios sentidos, aunque no siempre es así.

Es esencial que la prueba por indicios como actividad probatoria es utilizada ante la insuficiencia o falta de pruebas directas, los que debidamente acreditados pueden servir de base para desvirtuar la presunción de inocencia. En términos generales se puede conceptuar al indicio como el hecho o dato conocido indubitablemente probado y por el que a través de un razonamiento lógico o presunción se acredita la existencia de otro hecho desconocido, pero que está íntimamente vinculado al primero.

En segundo lugar, el indicio como razonamiento o proceso lógico inherente a su esencia exige la conexidad indispensable entre el acto inicial y el hecho a probar, recordemos que lo que se quiere lograr con el indicio es probar un hecho que no cuenta con medios directos que permitan conducir a concluir un resultado, careciendo en un primer momento el cognoscente de medios que permitan captar la convicción del hecho central a probar.

3.2.1. Prueba indiciaria

En cuanto al manejo de la evidencia digital, se ha indicado que no existe un manual o un protocolo para el manejo de esta, manual que debe ajustarse a ciertas normativas nacional o internacionales, con el objeto de asegurar sus características propias para que puedan ser valoradas dentro de un proceso penal, principalmente en la etapa en donde se origina la prueba, en la etapa de juicio.

A nivel nacional con la entrada en vigor de la Ley para el reconocimiento de las comunicaciones y firmas electrónicas, Decreto número 47-2008 del Congreso de la República, regula aspectos procedimentales para reconocer jurídicamente el valor de las comunicaciones electrónicas, definiendo a estas como toda comunicación que las partes hagan por medio de mensajes de datos. Durante el desarrollo de una investigación criminal, se puede llegar a contar con elementos de investigación que aportarán información para el esclarecimiento de un hecho categorizado como delictivo, en este proceso suele tomarse como sinónimos los términos indicio, evidencia y prueba; en ese

sentido, indicio puede ser definido como acepción de prueba o bien en el de objeto, huellas, signo, rastro; es decir, de simple hecho o conducta.

En materia probatoria penal no se puede hablar de presunción, derivado que cualquier resolución que se emita utilizando como fundamento una presunción violenta los principios de inocencia y de defensa, al dar por acreditados hechos, sino se presenta prueba en contrario. En otras ramas del derecho se denomina *presunción,* en sentido propio, a una norma legal que sustituye en forma absoluta la demostración del hecho, pues se tienen por acreditado si se establecen la existencia de las circunstancias que basan la presunción y sin admitir demostración en contrario.

Regularmente en la jurisprudencia y en la ley, se utiliza de manera incorrecta el término presunción, como sinónimo o equivalente a indicio, tratando tal vez de captar con el término presunción, la conclusión a que se puede llegar partiendo de un indicio. Es importante señalar que indicio y presunción, son dos conceptos diferentes, el problema ha surgido cuando en muchas ocasiones se utilizan como sinónimos.

La presunción tiene su base en el silogismo, o razonamiento deductivo y se rige por el principio de identidad. El silogismo funciona de acuerdo con el axioma, lo que se afirma de un universal, debe afirmarse de cualquiera de los singulares, al ser utilizado como silogismo, la premisa mayor es el principio general (universal); la premisa menor es un hecho conocido (singular) y la conclusión es el hecho que se desea probar.

Como ejemplos de presunciones en el Código Procesal Penal, se pueden indicar, *la presunción de inocencia,* utilizando el sistema de silogismos, la identidad entre el contenido universal o general (premisa mayor), “si todos los hombres son de ordinario inocentes”, con el contenido de lo singular (premisa menor), “cualquier hombre es inocente”, salvo prueba en contrario. En ese sentido la presunción no necesita probarse, ya está normado en la ley.

Se ubica otro ejemplo de presunción en lo que se refiere al peligro de fuga en el momento de establecer la medida de coerción por aplicar a una persona, quien ha sido ligada a proceso por un delito grave, establecido en el artículo 264 del Código Procesal Penal, se presume que el sindicado de un delito grave intentará eludir la acción de la justicia o el algún momento entorpecer las investigaciones influyendo en testigos o peritos. En este caso la premisa mayor, que todos los sindicados de delitos graves presentan un peligro de fuga u obstaculización a la averiguación de la verdad, por lo que una persona ligada a proceso por un delito grave presenta peligro de fuga o de obstaculizar la averiguación de la verdad en la investigación

Otro ejemplo, se da en los casos en los que se realzan allanamientos a inmuebles por parte de agentes de la Policía Nacional Civil, sin autorización judicial, cuando ocurre alguno de los casos previstos en la artículo 190 del Código, donde se establecen las presunciones en los numerales 2) y 3), cuando se denuncien que personas extrañas han sido vistas mientras se introducían en un lugar y existan indicios manifiestos que cometerán un delito; en este caso se utiliza la frese indicios manifiestos, se entiende en este caso que se presume que cometerán un delito, se puede apreciar el uso del término *indicio,* como sinónimo de presunción, de ahí que se confunda que se habla de lo mismo. El otro caso establece que se podrá ingresar a un inmueble cerrado, cuando se persiga a una persona para su aprehensión, por suponérsele participe de un hecho graves, en este caso se utiliza la frase suponérsele, entendiéndose que se presume que la persona pudo haber participado en un hecho calificado como grave.

Se puede apreciar en estos ejemplos que la presunción, aunque no literalmente, se puede extraer al interpretar la ley, por lo que releva la necesidad de presentar prueba para demostrarlo, en cambio el indicio necesita producirse como prueba. Se debe entender como indicio, como parte del presente trabajo de investigación resulta importante entender esta institución y diferenciarla de las presunciones.

Según Mittermaier (1877) “su nombre mismo lo expresa (index), el indicio es, por decirlo así, el dedo que señala un objeto” (p. 309).

Con esta aseveración, se estima que es una definición sencilla, pero hace referencia al carácter de indicador de una circunstancia u objeto que puede llegar a tener relevancia dentro de una investigación criminal.

Otra conceptualización doctrinaria al respecto y en opinión de Cafferata (1998) “El indicio es un hecho (o circunstancia) del cual se puede mediante una operación lógica, inferir la existencia de otro” (p. 86).

A través de un análisis se puede llegar a establecer la existencia de un dato que no se conoce, utilizando el indicio, como dato conocido, con el objeto de establecer la forma en que pudo haber sido cometido un hecho delictivo. Es común denominar indicio, a un objeto conocido, como puede ser una mancha de sangre, que en este momento solamente es el hecho indicador, partiendo de este hecho conocido, para llega al hecho desconocido, en este caso el delito.

Según Malatesta (Malatesta, 2002) un indicio es “el raciocinio probatorio indirecto que mediante la relación de causalidad, deduce lo desconocido de lo conocido” (p. 255).

Este autor hace referencia a un aspecto muy importante para establecer el concepto de indicio, la relación de causalidad, por medio de la relación causa y efecto se puede llegar a establecer un hecho desconocido, que en este caso sería el hecho delictivo.

De acuerdo con el punto de vista de Rocha (1997) el indicio se comprende así “es una circunstancia cierta de la que se puede sacar por inducción lógica, una conclusión acerca de la existencia o inexistencia de un hecho a probar” (p. 35).

Aquí se ubica una diferencia más con lo que se refiere a las presunciones, las cuales se basan en el método de deducción, mientras que, según esta definición los indicios se basan en el método inductivo; es decir, de lo particular a lo general.

Para Calderón (2013) el indicio “comienza como un hecho, que el investigador considera relevante para efectos de establecer la verdad, pero que en ocasiones puede no avanzar hasta tener calidad de prueba” (p. 37).

Para un investigador criminal, una mancha de sangre, un objeto, una huella dactilar, o una conducta de una persona, puede ser un hecho de relevancia para la investigación; pero después del análisis inductivo o en el caso de la prueba pericial luego de los diferentes análisis forenses, pueden ser descartados como parte o instrumento del hecho criminal , por lo que no pueden servir de fundamento o base para conducir al hecho desconocido o como anteriormente se denominó el hecho delictivo.

En el caso de los *indicios,* el proceso de razonamiento es inductivo, deriva que parte de casos particulares o singulares, casos aislados, para luego una regla de la experiencia, sea científico o incluso cotidiana. En este punto se podría tomar como ejemplo lo que la doctrina a denominado la *res furtiva* o la tenencia de la cosa robada, que se ha considerado como un *indicio* de la participación de una persona en un delito de robo. Esto se fundamenta en una regla que se extrae de la observación de casos particulares, que pueden formularse de la siguiente forma: “quien tiene en posesión una cosa robada es de ordinario la persona, quien participó en la sustracción ilegal de la cosa ajena”. Este ejemplo es una forma sencilla de tratar de explicar el análisis inductivo que se debe realizar de los *indicios.*

Pero, se debe tomar en cuenta que en la realidad existen otras circunstancias que deben ser valoradas en estos casos, particularmente en el caso expuesto, el tiempo y el lugar en que se observa la tenencia de la cosa robada. Si el tiempo es menor entre el la sustracción y el tiempo en que se verifica la tenencia de la cosa robada y si se le agrega en un lugar próximo al lugar en donde la cosa fue sustraída.

En este caso, la relación lógica de causalidad entre el hecho indicador y el hecho indicado se hace más certero, porque se reduce a lo mínimo otras posibles causales del hecho indicador, hable aquí como hecho indicado, el hecho del robo del hecho indicador,

la tenencia de la cosa sustraída. Visto de esta forma se podría modificar la regla de la experiencia en el sentido que, la cosa robada encontrada inmediatamente en un lugar de donde fue extraída y en posesión de una persona, es un *indicio,* de la participación en el delito de robo por el poseedor de la cosa robada.

Como anteriormente se expuso, en materia penal en Guatemala no puede hablarse de *presunciones,* resulta ser el *indicio,* resulta ser el *indicio* el medio de prueba, el instrumento idóneo para establecer la relación de causalidad entre el hecho indicador y el hecho indicado. La fuerza probatorio del *indicio*, está relacionado directamente con la fuerza de la relación lógica de causalidad entre el hecho indicador y el hecho indicado.

Calderón (2013) vuelve a referir que “el grado de fuerza de ese vínculo, se determina por el carácter constante o solo ordinario de la relación específica entre lo conocido y lo desconocido. Lo constante genera un nexo necesario y lo ordinario una relación contingente” (p. 41).

Esto quiere decir que el vínculo constante va a tener como consecuencia un coherencia entre el hecho indicador con el indicado, mientras que el carácter ordinario tiene como consecuencia accidental, en criminalística este concepto hace referencia a la evidencia material o indicios materiales.

En este aspecto se habla de rastros, de objetos, los cuales pueden ser completos como lo sería un arma de fuego, una arma blanca, estos permiten establecer relaciones causales directas, diferente es cuando solo se localizan fragmentos o partes de estos objetos, como lo sería un proyectil o una impresión dactilar, los cuales un mínimo de investigación para llegar a determinar relaciones causales.

Como ejemplo sería que si se localiza un casquillo o una impresión digital, que requieren análisis forenses para establecer esos nexos causales. Como sería también una fotografía digital o un archivo en pdf. que requieren de análisis forenses informáticos para establecer esos nexos causales.

En ese sentido, los objetos o rastros pueden constituir hechos indicadores y como tales, en su análisis les he aplicable la lógica inductiva, propia de los *indicios.*

Al definir el *indicio* como prueba, esta comprende a los hechos indicador e indicado en sus nexos lógicos causales, como consecuencia los objetos, vestigios, rastros se apoyan en el método de la inducción para establecer el nexo de causalidad.

Para terminar con este breve análisis de lo que se conoce como *prueba indiciaria,* lo Corte Suprema de Justicia ha establecido jurisprudencia de esta institución como se establece en la Sentencia de Casación, expediente número 1766-2015, sentencia de Casación del 31/08/2017, que indica:

> El juicio de la Sala, al revisar la plataforma probatoria en que se basó el Tribunal de Sentencia para emitir un fallo condenatorio, constató que esta está construida sobre la base de pruebas testimoniales, periciales y documentales, especialmente las declaraciones de los peritos y como ya se indicó, con estas se acreditó la participación del procesado en la comisión del ilícito imputado. Sobre esta base, el tribunal construyó de manera consistente, lógica y con suficiente fundamento su decisión [...] Lo relevante en estos casos es la ejecución de los hechos para establecer la participación directa y que ello es justamente la concertación para participar en el hecho del juicio y fue esta una inferencia inductiva justa, que no admitió encontrar una causa con mayor robustez lógica". Por lo que a nivel nacional se puede entender que los jueces en el momento de dictar sus diferentes fallos han fundamentado estas en la *prueba indiciaria,* haciendo referencia a las diferencias con las *presunciones*, al establecer el método inductivo como forma de analizar los *indicios*.

Derivado de esta serie de preceptos, se considera por consiguiente que la evidencia digital o la prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio. En ese contexto, previo a la aceptación de la evidencia digital, un tribunal

determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o el original es requerido.

Con regularidad en cualquier legislación, la evidencia que carece de valor probatorio es inadmisible y las reglas de la prueba permiten que sea excluida de un procedimiento o afectadas por el expediente u objetada por oposición de un abogado. Una prueba digital puede ser aceptada si el valor de esta puede ser sopesado frente a su naturaleza perjudicial. Se considera que el problema con los datos digitales es que son elementos no tangibles. Pertenece a la categoría de pruebas frágiles y volátiles, junto con cosas tales como huellas en la nieve, porque son fácilmente destruidos o modificados. El problema con esto es que para que la evidencia sea admisible, la parte que la introduce debe demostrar que no ha sido alterada o modificada desde que fue recogida en la escena del crimen.

> La evidencia digital se constituye en todos aquellos datos e información histórica y presente almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia. (Del Pino, 2007, p. 10).

De acuerdo con este planteamiento, se estima que en esencia la evidencia de índole digital no es más que aquella información almacenada en algún tipo de dispositivo electrónico, que mediante el expertaje correspondiente, puede pasar a formar parte del cúmulo de elementos de convicción que puede y son susceptibles de utilizar en el proceso penal correspondiente.

Para López Delgado (2007) la evidencia digital se concibe como “es el conjunto de datos en formato binario, esto se comprende en los archivos, su contenido o referencias a estos, que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático” (p. 19).

Se comprende a través de este planteamiento que en esencia este aspecto guarda estrecha relación con el planteamiento anterior, únicamente que, expresado de una forma diferente, pues utiliza para el efecto un lenguaje técnico, pero que siempre es un tipo de información almacenada en algún dispositivo electrónico.

> La evidencia digital como objetos de datos en relación con la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento de multimedia, que no son más que cadenas de unos y ceros; es decir, de información binaria o digital grabada en un dispositivo magnético (como discos duros o los disquetes), en uno de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD). (Reyes, 2007, p. 34).

Justamente como se ha venido exponiendo, el concepto de evidencia digital siempre hace énfasis a la información que es susceptible de localizar en dispositivos de almacenamiento, con la salvedad que en esta definición se hace énfasis en los tipos específicos de unidades en que se puede localizar, denominando con nombre propio a dichos elementos a fin de generar una mayor comprensión sobre este aspecto.

Se puede decir entonces que la evidencia digital consiste en una serie de datos almacenados en un sistema informáticos o dispositivos tecnológicos, conectados o no a una red, los cuales pueden ser el objeto del delito o bien el instrumento de la comisión de este; datos que mediante técnicas informática especiales pueden ser recolectados y analizados para el esclarecimiento de un hecho delictivo.

Estos datos pueden consistir en imágenes, archivos de música, de video, mensajes de texto, correos electrónicos, archivos multimedia, aplicaciones, etc., los cuales se pueden encontrar en dispositivos de entrada o de salida de un sistema informático, o dispositivos mixtos, así como de almacenamiento, teléfonos móviles, memorias, discos duros, cámaras de foto, de video, impresoras, escáner, relojes digitales, consolas de video juego; en fin, todo objeto que sirva para transmitir, almacenar o procesar

información en formato electrónico o digital y en la actualidad no únicamente en objetos materiales, sino, además, en la plataforma denominada la nube o *e cloud*, espacio virtual en donde se puede almacenar información y ser descargada en cualquier lugar donde se pueda tener acceso a internet.

3.3. Características

Los elementos característicos de la evidencia digital son los que, a partir de la doctrina, han sido determinados para la prueba en general, pues no puede concebirse que la evidencia digital, al ser un elemento de prueba pueda tener características diferentes a las ya establecidas genéricamente para la prueba.

Es necesario enfatizar en los preceptos contenidos en los artículos 181 y 183 del Decreto Número 51-92 Código Procesal Penal, donde se señalan las características que debe tener la prueba para ser admisible.

a) Objetiva: no debe ser fruto del conocimiento privado del juez ni del fiscal, sino que debe provenir al proceso desde el mundo externo, siendo de esta manera controlada por las partes. El Código Procesal Penal, en su artículo 181 limita la incorporación de la prueba de oficio a las oportunidades y bajo las condiciones previstas por la ley.
b) Legal: debe ser obtenida a través de medios permitidos e incorporada de conformidad a lo dispuesto en la ley.
c) Útil: es aquella que sea idónea para brindar conocimiento acerca de lo que se pretende probar.
d) Pertinente: el dato probatorio deberá guardar relación, directa o indirecta, con el objeto de la averiguación. La prueba podrá versar sobre la existencia del hecho, la participación del imputado, la existencia de agravantes o atenuantes, el daño causado, etc.

e) No abundante: será abundante cuando su objeto haporquedado suficientemente comprobado a través de otros medios de prueba.
f) Relevancia: es relevante cuando se funda un juicio de probabilidad, la idoneidad convencional es conocida como relevancia o utilidad de la prueba. La prueba debe ser relevante, es decir, que el elemento de prueba que se incorpora al proceso no solo debe tener relación con el hecho que se investiga, sino que, además, debe permitirle al juez que la valora, obtener un grado de certeza y probabilidad sobre la verdad formal de los hechos.

Al recibir la noticia criminal el fiscal correspondiente tiene el primer acercamiento a los hechos penalmente relevantes que se supone han ocurrido en el ámbito de su competencia en la sociedad y frente a los que, utilizando los medios de acreditación obtenidos a través de actos de investigación, tiene el deber de lograr el mayor conocimiento posible para tomar las decisiones que correspondan. Si decide ejercer la acción penal, esto es, poner en control de la investigación al juez mediante la acusación; tendrá que presentar al juez el conocimiento de los hechos.

La evidencia digital es única, cuando se la compara con otras formas de evidencia. A diferencia de la evidencia física, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único es su potencial de realizar copias no autorizadas de archivos, sin dejar rastro alguno. La evidencia digital posee, entre otras, las siguientes características:

a) Es volátil
b) Es anónima
c) Es duplicable
d) Es alterable y modificable
e) Es eliminable

Tales características sugieren la exigente labor requerida por los especialistas cuando tenga que llevarse adelante investigaciones sobre la delincuencia informática, en

procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada en la escena del crimen

Se requiere tratamiento especial a tiempo de manejar la evidencia digital durante el juicio, más allá del cumplimiento de las normas formales, pues estas deben estar articuladas con los esfuerzos de conservación y seguridad de los estándares internacionales.

De manera general a la evidencia digital también se le conoce como prueba electrónica, en su acepción general dentro del ámbito probatorio, puede ser considerada como cualquier información almacenada o transmitida en forma digital, la que una de las partes podrá utilizar en el juicio.

Dentro del campo de la criminalista podemos identificar la informática forense, la que va adquiriendo inusitada importancia, debiéndose resaltar su carácter científico, por ello, tiene sus fundamentos en las leyes de la electricidad, de la física y el magnetismo, siendo importante puntualizar que es con base a fenómenos electromagnéticos que la información puede ser almacenada; por ello se afirma con certeza que la informática forense colabora en la investigación de delitos cometidos por organizaciones criminales, apoyándose en el método científico.

Los delincuentes hoy están utilizando la tecnología para facilitar la comisión de infracciones y eludir a las autoridades. Este hecho ha logrado que las Tecnologías de la Información y la Comunicación se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

La obtención de Información demanda que los investigadores forenses encargados de la recolección preservación, análisis y presentación de las evidencias digitales hagan una labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal.

3.4. Clasificación

La importancia de la tecnología en las actividades judiciales en cualquier ámbito, ha ido cobrando notoriedad paulatinamente en virtud de la relevancia de la carga de la prueba y esencialmente en torno a la libertad de la prueba contenido en el artículo 182 del Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, el cual regula que se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso por cualquier medio de prueba permitido, estimándose en consecuencia que dentro de estos aspectos se incluyen los elementos o dispositivos electrónicos o digitales, el paulatino incremento en el uso de las tecnologías y comunicaciones en el país, constituyen mecanismos óptimos y consecuentemente susceptibles de ofrecerse como medios probatorios.

La utilización de mecanismos digitales o electrónicos como elementos de prueba dentro de un proceso penal en particular, ha creado una mayor brecha sobre los medios que oportunamente pueden incluirse como prueba para dirimir una controversia y que a la larga ha venido a beneficiar al sistema de justicia en general, básicamente, porque estos elementos han implicado nuevos medios de investigación, mucho más útiles, versátiles y decisorios, en virtud que muchos de estos aspectos son considerados como medios de prueba científicos, minimizando con ello la subjetividad en la prueba que recurrentemente se generaba hasta hace una década.

En ese sentido, el uso de nuevos medios de investigación en el proceso penal obliga a la adopción de una serie de reflexiones sobre el papel del Estado en el derecho en el moderno proceso penal, en virtud que al mismo le han correspondido una serie de cambios acorde con las nuevas tareas que se le han confiado en el campo de la seguridad interna del Estado y del combate del crimen organizado en la circunscripción geográfica de la República de Guatemala.

Las nuevas herramientas tecnológicas, que se utilizan cotidianamente, permiten que se pueda reconstruir fácilmente donde se encontraba la víctima o el victimario, antes,

durante y después de la comisión de un evento delictivo, reflejándose en tal sentido la serie de actividades que realiza y con quiénes se comunica, entre otros aspectos de relevancia.

Tanto teléfonos fijos y móviles, laptops, tarjetas de accesos a edificios, cámaras de seguridad, discos externos, los CD, los DVD, dispositivos extraíbles, impresoras, faxes, memorias de máquinas fotográficas, escáneres, memorias portátiles e inclusive los desplegados telefónicos, han permitido la desarticulación de estructuras criminales, fundamentalmente, porque en estos vienen incluidos las referencias geoposicionales de los objetivos y que en determinado momento permiten establecer su ubicación en el momento de suscitarse un evento delictivo en particular.

Este enorme abanico de posibilidades tecnológicas, son solo algunos de los mecanismos que son susceptibles de utilizar diariamente en la vida personal y laboral; consecuentemente con ello, es necesario también hacer uso de estos dentro de los diversos diligenciamientos que deben atenderse en el proceso penal en general, resultando de ahí su importancia como mecanismos complementarios y necesarios para garantizar la eficiencia y eficacia de las actividades efectuadas en el marco de las actividades requeridas.

A continuación, se describe una clasificación de los dispositivos tecnológicos que se encuentran estrechamente relacionados con el ámbito de la informática, en consecuencia, se considera que pueden llegar a considerarse indicios o vestigios criminales que posteriormente pueden convertirse en evidencia digital, dentro de estos aspectos se señalan al respecto los siguientes dispositivos:

a) Dispositivos de salida

Son aquellos que permiten la comunicación entre la computadora y el usuario y la información sale en lugar de entrar, de entre esta gama de elementos se encuentran pantallas o terminales, impresoras y altavoces, plotters, visualizadores, tarjetas de sonido, altavoces y auriculares.

b) Dispositivos de entrada

Son aquellos que sirven para introducir datos a la computadora para su proceso. Los datos se leen de los dispositivos de entrada y se almacenan en la memoria central o interna. Los dispositivos de entrada convierten la información en señales eléctricas que se almacenan en la memoria central. Dentro de estos dispositivos se localizan por ejemplo teclados, dispositivos apuntadores, ratones (mouses), joystick (controles para videojuegos), escáneres, cámaras web (webcam), pantallas táctiles, teclados, lápices ópticos, gamepad, lectores de códigos de barras, lectores de códigos QR, sensores de huellas dactilares, cámaras digitales y micrófonos, entre otros.

c) Dispositivos mixtos

Se consideran dispositivos mixtos, por ejemplo, la memoria RAM, un grabador de los CD o los DVD, el disco duro, un modem, principalmente, porque todos pueden enviar o recibir datos de la Unidad Central de Procesos (CPU), de esta cuenta se considera que son susceptibles de localizar dentro de estos elementos, Fax-Módem, tarjeta de red, tarjeta de sonido.

d) Unidades o dispositivos de almacenamiento

Dentro de estos elementos, se destacan principalmente los discos duros internos y externos, debiéndose señalar que los discos duros tienen una gran capacidad de almacenamiento de información, pero al estar alojados normalmente dentro de la computadora (discos internos), no son extraíbles fácilmente.

Para intercambiar información con otros equipos (si no están conectados en red) se tienen que utilizar unidades de disco, como los disquetes, los discos ópticos (CD, DVD), los discos magneto-ópticos, memorias USB o las memorias flash, cintas magnéticas, memorias flash, entre otros.

El disco duro almacena casi toda la información que se maneja al trabajar con una computadora. En él se aloja, por ejemplo, el sistema operativo que permite arrancar la máquina, los programas, archivos de texto, imagen, vídeo, etc. Dicha unidad puede ser

interna (fija) o externa (portátil), dependiendo del lugar que ocupe en el gabinete o caja de computadora.

Un disco duro está formado por varios discos apilados sobre los que se mueve una pequeña cabeza magnética que graba y lee la información. En ese sentido, se considera que este componente, al contrario que el micro o los módulos de memoria, no se pincha directamente en la placa, sino que se conecta a ella mediante un cable. También va conectado a la fuente de alimentación, pues, como cualquier otro componente, necesita energía para funcionar.

3.5. Procedimientos para su recolección y embalaje

Los aspectos relativos a la recolección y el embalaje de los indicios digitales, se encuentra a cargo de técnicos criminalistas de la Dirección de Investigaciones Criminalísticas del Ministerio Público, específicamente de la Unidad de Recolección de Evidencias, quienes efectúan la documentación y recolección de los vestigios que oportunamente son susceptibles de localizar en cualquier escenario criminal, desde luego que todo ello bajo las directrices y supervisión de un fiscal, quien está a cargo del procedimiento en su totalidad.

La Dirección de Investigaciones Criminalísticas estará integrada por un cuerpo de técnicos en distintas ramas, dependerá directamente del Fiscal General de la República. Tendrá a su cargo el análisis y estudio de las pruebas y otros medios de convicción que coadyuven al esclarecimiento de los hechos delictivos que investiguen los órganos del Ministerio Público.

La Dirección de Investigaciones Criminalísticas del Ministerio Publico jerárquicamente se encuentra organizada de la siguiente manera:

Director: Quien es el encargado de tomar decisiones tanto administrativas como operativas en las áreas de investigación criminal y recolección de evidencias.

Subdirectores:

Investigaciones: Es el encargado de la toma de decisiones en el área de investigaciones, para ello cuenta con diferentes grupos de investigadores que brindan el apoyo a las diferentes fiscalías en todo el territorio nacional.

Recolección de Evidencias: Es el encargado de la toma de decisiones en el área de la Unidad de Recolección de Evidencias, tiene bajo su dirección todos los grupos de recolección de evidencias que apoyan a las diferentes fiscalías en todo el territorio nacional; asimismo, al grupo de recolección de evidencias designado para la fiscalía de la mujer, Hospital Roosevelt, Hospital General San Juan de Dios y Organismo Judicial.

Sub Coordinadores: Son los encargados de proveer a los diferentes grupos de Recolección de Evidencias los insumos necesarios para su perfecto funcionamiento, para ello realizan la organización mensual del rol de trabajo de cada uno de los grupos.

De igual manera, se encuentran los subcoordinadores del área de investigaciones, quienes son los encargados de asignar casos a los investigadores que estén bajo su coordinación, para su desempeño se les proveerá de vehículos para la realización de las diligencias que estos realicen en todo el territorio nacional.

El fin primordial de la Unidad de Recolección de Evidencias del Ministerio Publico es el de recolectar y remitir las evidencias y otros medios de convicción que coadyuven al esclarecimiento de los hechos delictivos que investiguen los órganos del Ministerio Público y sus funciones se desarrollan bajo la conducción del Fiscal a cargo del caso.

Está compuesta por el Gabinete Técnico, el cual a su vez se compone de las Unidades de Monitoreo y Unidad Recepción, Análisis, Control y como dependiente directo de esta unidad se encuentra el Archivo e Información.

Todas las diligencias que se realizan dentro de la Dirección de Investigaciones Criminalísticas son llevadas a cabo por la existencia de solicitud por escrito que sea realizada por el agente o auxiliar fiscal que esté encargado del caso en el que solicite la investigación, peritaje o cualquier otra diligencia.

En torno a la recolección de la evidencia digital en la República de Guatemala, no se cuenta con un manual que contenga los procedimientos en específico para efectuar la documentación de la totalidad de dispositivos electrónicos que son susceptibles de localizar en los diversos escenarios que tienen a bien documentar.

La unidad en mención, encargada de recolectar lleva registro y control de las acciones realizadas por parte del personal en la escena del crimen o recolección de indicios, con el objeto de verificar el cumplimiento y calidad del trabajo realizado, conforme los procedimientos establecidos, además de velar por la entrega oportuna de los informes de los casos asignados por grupo e individual; y el adecuado funcionamiento de las instalaciones, equipo y mobiliario necesario para el cumplimiento de su función.

Desarrolla el procesamiento de la escena del crimen y la recolección de indicios, bajo la dirección del fiscal responsable del caso y ejecutando las medidas dictadas para proteger y aislar indicios en los lugares en los que se esté investigando un delito, a fin de evitar contaminación o destrucción de rastros, evidencias u otros elementos materiales; elaborando los informes correspondientes, inmediatamente después de procesar la escena del crimen, de conformidad con disposiciones específicas; registrando y controlando las acciones realizadas por parte del personal en la escena del crimen o recolección de indicios, entregando de manera oportuna los informes de los casos asignados, por grupo e individual.

Se cuenta con la Instrucción del Ministerio Público 166-2013, Manual de Normas y Procedimientos para el Procesamiento de la Escena del Crimen, en este no se localiza ningún apartado procedimental que permita efectuar con objetividad, precisión y efectividad, la documentación de indicios digitales en el país, estimándose en tal sentido que es en torno a estos preceptos que giran los aspectos medulares de la presente investigación, principalmente, porque no se cuenta o detalla con precisión, los mecanismos a utilizar para la documentación de la evidencia digital que se localiza constantemente en plena era de la información, donde cada vez más es susceptible de localizar todo tipo de indicios de esta naturaleza y la importancia que tiene esta para el esclarecimiento de la verdad en el país.

3.6. Documentación y cadena de custodia

La Unidad de Recolección de Evidencias, se encarga de la inspección, recolección, clasificación y protección de las evidencias que coadyuven al esclarecimiento de un hecho delictivo. Tiene competencia en la capital, en lo referente a la escena del crimen y/o lugar del hallazgo en cuanto a cadáveres; y competencia en todo el territorio nacional en cuanto a las demás diligencias que correspondan al ámbito de su función.

El Manual de Normas y Procedimientos para el Procesamiento de la Escena del Crimen contiene procedimientos básicos sin entrar en detalles técnicos que son propios del personal que integra los equipos de escena e incluye los formatos de los documentos que se utilizan para la documentación de esta. Un aspecto a destacar en la importancia del cumplimiento y exacta ejecución que deben dar los fiscales, agentes fiscales y auxiliares fiscales al uso del manual, radica en que el formato de procesamiento, además de alimentar el banco de información de la Dirección de Investigaciones Criminalísticas, que podrá ser utilizado por las distintas fiscalías, facilitará realizar un control sobre la adecuada actuación de las personas que intervienen en el procesamiento de este tipo especializado de diligencia.

Los técnicos en escena del crimen del Ministerio Público tienen un marco de atribuciones de vital importancia, porque todo lo que realicen en la escena repercutirá en todas las etapas de la investigación; es decir, su labor depende del éxito o el fracaso de la investigación, porque ellos son los encargados de localizar, documentar y embalar todos los indicios en la escena del crimen. Para que ellos fijen o localicen todos los indicios depositados en la escena del crimen deben ser muy minuciosos y exhaustivos en el lugar de los hechos.

Deben evitar rotundamente la duplicidad de funciones que suele conllevar errores graves y mucho en torno a la documentación y consiguiente inicio de la cadena de custodia, la cual en la actualidad se desarrolla de forma improvisada, que si bien reúne las características esenciales en la descripción generalizada de los indicios, no se cuenta con un criterio definido para solicitar los peritajes correspondientes al laboratorio de informática forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF), hacia donde se trasladan oportunamente por los técnicos embaladores de la Unidad de Recolección de Evidencias.

Por ello, la cadena de custodia es un mecanismo de control y registro que se aplica al indicio, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente, deba ordenar su conclusión.

La cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, empaque y traslado; lugares y fechas de permanencia y los cambios que en cada custodia se hayan realizado; igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos, que si bien se cumple de forma generalizada, no se dispone de un procedimiento específico que regule estos aspectos y los elementos que debe contener la descripción de los indicios o evidencia digital en el país.

La cadena de custodia es un procedimiento de control que se emplea a fin de garantizar que no habrá un vicio de los elementos de investigación, como puede ser la alteración, daños, reemplazos, contaminación o destrucción del material probatorio. Esta cadena se lleva a cabo en etapas, empezando con la extracción o recolección de la prueba, preservación y embalaje, transporte, traspaso, en su caso, a laboratorios para su análisis y, custodia y entrega de los análisis o material probatorio, que oportunamente se presente u ofrezca ante los órganos jurisdiccionales correspondientes, de lo anterior es que resulta fundamental disponer de un procedimiento en concreto para documentar e iniciar la cadena de custodia, que si bien se inicia en todos los casos, se efectúa de forma muy general y sin ninguna formalidad.

Capítulo IV

4. Incidencia de la evidencia digital en casos concretos en Guatemala

4.1. La investigación criminal en delitos informáticos

En torno al presente apartado, se describen los principales elementos concernientes a la investigación criminal aplicada en materia de delitos informáticos, para el efecto, es pertinente señalar algunas consideraciones generales el concepto de investigación desde el punto de vista eminentemente criminal, tomando en cuenta que es un aspecto esencial para la identificación, documentación y recolección de la totalidad de indicios o vestigios criminales que son susceptibles de localizar en los diferentes escenarios criminales que se suscitan en el país.

En el ordenamiento jurídico guatemalteco, los aspectos regulatorios de la investigación criminal se encuentran contenidos en el Decreto 15-2012 Ley de la Dirección General de Investigación Criminal y a lo interno de la normativa institución de la Policía Nacional Civil, a través de la Orden General Número 12-2009 Organización y Designación de Funciones de la División Especializada en Investigación Criminal Subdirección General de Investigación Criminal de la Policía Nacional Civil.

La acepción o concepto de investigación criminal, en esencia describe los conceptos, investigación, métodos, técnicas, procedimientos, objeto, ciencia, criminología y criminalística, siendo de importancia para el desarrollo de una buena investigación, la creciente sensación subjetiva de inseguridad ciudadana y el privilegio que esta ocupa para las políticas de del contexto guatemalteco, se ha impulsado la planificación y el desarrollo de una serie de modificaciones en las articulaciones de las instituciones, orientadas a la obtención de un clima objetivo y subjetivo de seguridad ciudadana como fin último del bien común.

Atendiendo estos preceptos, es importante manifestar que tomando en consideración esta serie de definiciones planteadas, se infiere que la investigación

criminal suele ser comprendida como aquella actividad técnica y científica, de recolectar evidencia física y los elementos materiales probatorios que permitan conocer y comprender un hecho delictivo; asimismo, suele ser conocido como la fase del proceso penan en la que se liga a una persona, a partir de una actividad investigativa y los hallazgos que de ella se deriven, en un proceso penal.

Montiel (2007) la define de la siguiente manera: Es el conjunto de diligencias, pesquisas, indagaciones y experticias técnicas, tendientes a establecer un hecho criminal, a identificar y localizar a los partícipes o autores y hacerse de los elementos de prueba de su presunta participación en un hecho punible. (p. 7).

En ese contexto, es importante señalar que la investigación criminal al igual que la criminalista es una ciencia, debido que para su aplicación se deben aplicar un método de rigurosidad de la técnica y la aplicación de unos principios que de no ser científicos deben ser legales, debido a que como bien sabemos está orientada por los principios que rige la actividad penal.

En el contexto del marco jurídico guatemalteco, el artículo cuatro del Decreto 152012 Ley de la Dirección General de Investigación Criminal, establece que la Investigación Criminal comprende el desarrollo de las actividades pertinentes para reunir los elementos que permitan el esclarecimiento de los hechos delictivos y la individualización de los presuntos responsables, a efecto que el Ministerio Público ejerza eficaz y eficientemente la acción penal.

La investigación criminal es un tipo de intervención altamente calificado y sustentado en bases técnico-científicas, dadas la complejidad y especificidad propias de la investigación de crímenes de diversa índole. De esa cuenta es importante hacer énfasis en que la investigación criminal es un proceso esencial y auxiliar del sistema penal en Guatemala.

> La primera fuerza policial en Guatemala nació aproximadamente en 1872 con características de policía urbana y bajo el nombre de Guardia Civil y aunque en 1881 el régimen liberal fundó la primera Policía Nacional, se puede afirmar que fue hasta en los años veinte, bajo la dictadura del presidente Manuel Estrada Cabrera (1898-1920), cuando comienza a asumir funciones de investigación criminal, debido a que hasta esa fecha fue creado el órgano de investigación criminal: la Policía Secreta, que después pasaría a llamarse Policía Judicial. Sin embargo, desde su nacimiento comienza a atrofiarse la naturaleza de la investigación, pues tuvo características de una policía política, utilizada como instrumento de represión para los opositores, constituyéndose a partir de aquella época en una práctica de las fuerzas nacionales de seguridad. (Monterroso, 2003, p. 15).

La definición anterior brinda a grandes rasgos una perspectiva de los inicios de la investigación criminal en el país, fundamentalmente, porque la policía se encuentra estrechamente relacionado con los procesos de investigación que se desarrollan en el entorno de la criminalidad, esta situación tiene cabida en el contexto jurídico de Guatemala, principalmente por los últimos avances en materia de investigación criminal en el país; acorde con este planteamiento es necesario profundizar un poco más en este aspecto y para el efecto se presenta el siguiente concepto.

La extensión del concepto de investigación criminal viene definida por la realización de todas las actividades y la puesta en práctica de técnicas que conduzcan al fin perseguido que, con mayor precisión, debe establecerse en logar el conocimiento cierto de todos los hechos de interés para calificar las conductas típicas del derecho penal, así como las circunstancias relativas a estas; es decir, lo que en derecho procesal penal se considera como la verdad material.

Consiente de esta situación, resulta de suma utilidad puntualizar en cuanto al hecho concreto de que diferente de la investigación, pero estrechamente conectada a ella, hasta el punto de ser consecuencia, a veces, de la misma actividad, debemos considerar la prueba de los hechos, que intuitivamente consiste en la comprobación de esa verdad

material, pero formalmente requiere la aportación de los vestigios o elementos cuya consideración jurídica constituirá tal prueba en el juicio oral, si se obtiene la convicción del juzgador.

Acorde con el desarrollo y planteamientos de estos preceptos, se infiere por consiguientes que la investigación criminal se expresa como una ciencia, un arte y una técnica, en una convergencia de la criminalística a través del estudio de la escena; la vinculación de las ciencias puras que aplicadas en el desvelamiento del delito surten un adicional etimológico llamado forense, pues el dictamen técnico-científico de un planteamiento sometido al análisis de un profesional en cualquier arte o ciencia, se denomina pericia, perdiendo así la el fin puro como ciencia para aportar en el esclarecimiento del delito.

Entonces, en la presente opinión, se dice que la investigación criminal radica en auxiliar con los resultados de la aplicación científica de sus conocimientos, metodología y tecnología, a los órganos que procuran y administran justicia a efectos de darles elementos probatorios identificadores y reconstructores y conozcan la verdad de los hechos que se investigan. Se infiere con esta teoría que la investigación criminal básicamente está enfocada en auxiliar con los resultados base de análisis técnicocientífico, metodología y tecnología, a los órganos que cumplen funciones de policía judicial y a los que les corresponden administrar justicia, a efecto de darles elementos probatorios, identificadores y reconstructores conducentes a establecer la verdad de los hechos que investigan.

En síntesis y considerando detallar con claridad el propósito fundamental de esta disciplina, la investigación criminal es una actividad práctica efectuada por empleados y funcionarios del sistema de justicia en general, principalmente por empleados del Ministerio Público, Instituto Nacional de Ciencias Forenses, Organismo Judicial e Instituto Nacional de la Defensa Pública Penal y en menor escala por Abogados litigantes particulares, efectuando para el efecto una serie de actividades o diligencias, destacándose entre estas, las siguientes: inspecciones, análisis, registros, identificación,

individualización, seguimiento, incautación, solicitud de exámenes a personas y elementos, así como el estudio de la naturaleza del hecho, entre otros.

Algo que si es definitivo es que el investigador debe ser capaz de organizar las diferentes manifestaciones de proceder, saber preguntar y lograr las diferentes manifestaciones y buenas contestaciones. Un justo acercamiento de toda la escena y la existencia de otros factores, investigar constantemente mejorando su habilidad para develar la historia en cada escenario. De ese modo, de lograr mayor conocimiento y estar mejor equipado para capturar al delincuente del crimen.

También al analizar un informe o declaración, lo hace independientemente de los factores de este. Esto permite percibir si el declarante está mintiendo, u omitiendo información y se busca las pistas dejadas por el sospechoso en forma no determinada.

En el contexto de la investigación criminal, es necesario que el investigador, para llevar a cabo su trabajo investigativo, debe hacer uso de los distintos métodos que le proporciona la lógica, dentro de los cuales se encuentran el método científico, el inductivo, el deductivo, el analítico, el sintético, el comparativo y el ecléctico; destacándose que con ellos puede llevarse a buen término la investigación en el país.

> El método científico: el método científico tiende a reunir una serie de características que permiten la obtención de nuevo conocimiento científico. Es el único procedimiento que no pretende obtener resultados definitivos y que se extiende a todos los campos del saber.
>
> El método es un proceso de elaboración consiente y organizado de los diferentes procedimientos que orientan para realizar una operación discursiva. Por ello, las etapas del método científico se corresponden de manera general con las del proceso del pensamiento reflexivo, como son: advertencia, definición y comprensión de una dificultad; búsqueda de una solución provisional; comprobación experimental de la solución adoptada; verificación de los resultados

> obtenidos y diseño de un esquema mental en cuanto a situaciones futuras para las que la situación actual será pertinente. (Téllez, 2007, p. 45).

En resumen, puede exponerse que la investigación criminal mediante la aplicación de los métodos inductivos y deductivos, desde un inicio en el sitio del suceso y apoyada en los métodos, técnicas e instrumentos que proporciona la criminalística, puede realizar estudios preliminares y análisis sobre la forma y factores que se manifestaron para la ocurrencia de los hechos, es decir, el modus operandi utilizado, instrumentos utilizados, hasta llegar a la colección y suministro de las evidencias de interés criminalístico, que puedan llevar a la identificación del o los autores.

4.2. Peritaciones en materia de delitos informáticos

Dentro de los preceptos iniciales que se requieren abordar se encuentra primeramente lo relativo al delito, en virtud que para que exista un indicio que posteriormente se convertirá en medio de prueba, se requiere necesariamente de la existencia de un evento delictivo, toda vez que sin el cual no tendría razón de ser la existencia de la prueba en particular; de tal manera que resulta consistente puntualizar en los principales preceptos doctrinarios que giran en torno a la teoría del delito y en cierta medida a sus elementos.

> La teoría del delito tiene como objeto analizar y estudiar los presupuestos jurídicos de la punibilidad de un comportamiento humano sea a través de una acción o de una omisión, en estos términos dicho análisis no solo alcanza los delitos, sino incluso a todo comportamiento humano del cual pueda derivar la posibilidad de aplicar una consecuencia jurídico penal, entonces, será objeto de análisis de la teoría del delito aquello de lo cual derive la aplicación de una pena o una medida de seguridad, así como los casos extremos en los que, no obstante, existir una lesión o puesta en peligro de un bien jurídico, el comportamiento humano resulte justificado, no reprochable o bien, no punible. (Plascencia, 2004, p. 1).

La concepción del delito necesariamente requiere de igual forma que exista una afectación a un bien jurídico tutelado, de tal forma que la construcción del concepto de bien jurídico, dentro del derecho penal liberal, tiene como finalidad, la imposición de barreras al Estado en el desarrollo de su política represiva. Bajo esta óptica, el concepto de bien jurídico fundamental se construye como un criterio para la menor criminalización posible, para el mantenimiento y mayor extensión de la esfera de autonomía de las personas.

Desde este punto de vista, es también concebido en estrecha relación con la persona, individual o colectivamente considerada, como referente material de protección, y no una herramienta de conformación social, dirigida a promocionar la confianza en la norma jurídica. Se trata de una realidad, y no de una realidad normativa o fenómeno aséptico, sino de una herramienta de análisis constitucional que puede operar dentro de la teoría del delito, para valorar casos concretos.

Sobre el delito, se expresa en las palabras de Orozco (2007) lo siguiente “es la conducta humana que consiste en una acción u omisión de carácter antijurídica, típica, cometida por una o más personas imputables y con culpabilidad” (p. 1).

En consonancia con la serie de preceptos vertidos con anterioridad, resulta consistente exponer que la teoría del delito en sí se ocupa esencialmente de las características comunes que debe tener cualquier hecho para tomarse o valorarse como delito, independientemente de la tipología de que se trate.

Resulta lógico pensar, que siendo que en la actualidad la informática, las redes sociales, las tecnologías de la información y las comunicaciones, así como todas las actividades que se realizan a través de internet, no pueden quedar fuera de la actividad delictiva, aunado a que prácticamente todas las actividades que realizamos desde la forma en la que nos comunicamos, aprendemos, comercializamos hasta la forma en que nos entretenemos está íntimamente ligado a la tecnología, como no va ser utilizada esta faceta de la humanidad para realizar actividades ilícitas.

El surgimiento de este tipo de crímenes está íntimamente ligado al desarrollo de la tecnología informática. Las computadoras se han utilizado para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato, entre otros.

En la concepción de Huerta (2011) “este fenómeno ha obligado al surgimiento de medidas legislativo-penales en los estados industriales donde hay conciencia de que, en los últimos años, ha estado presente el fenómeno delictivo informático” (p. 45).

Por toda esta gama de aspectos es que se considera de utilidad efectuar el abordaje preciso de este apartado, tomando en cuenta la importancia que conlleva la utilización de la tecnología para dirimir las controversias dentro del proceso penal, particularmente donde es apenas uso reciente la tecnología, tal es el caso de la República de Guatemala.

En este proceso adquiere vital importancia la labor que efectúa el laboratorio de informática del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF), en virtud que los peritajes en material informático está a cargo de esta entidad, importante destacar que el Ministerio Público a través de la Dirección de Investigaciones Criminalísticas, dispone de una Unidad de Asistencia Técnica -UAT-, adscrita al área de informática forense de esta dirección; sin embargo esta únicamente efectúa la extracción de la información contenida en los dispositivos que le son remitidos, por ejemplo la mensajería en ambas vías, imágenes, videos, documentos y cualquier otro archivo que pudiera alojarse en dispositivos electrónicos.

En contraparte el laboratorio del INACIF, si lleva a cabo el análisis minucioso del contenido; es decir, que realiza la interpretación del contenido de la información, en tanto que la unidad de investigación del ente investigador, únicamente efectúa el vaciado de la información y lo almacena en dispositivos extraíbles como discos duros portátiles, memorias USB, tarjetas SD, Discos Compactos -CD-, Discos DVD, Discos en formato Bluray, todo depende de la cantidad o peso de la información que se extraiga de los dispositivos que le son remitidos por la fiscalía correspondiente y a quienes debe

consiguientemente remitir el informe pericial de los resultados que se obtuvieren en el análisis del dispositivo o elemento tecnológico en particular.

4.3. Alcances de la investigación y peritaciones

Como postulante de la presente tesis es necesario enfatizar que el uso de tecnología en la investigación criminal, genera un valor agregado a esta y como consecuencia de ello se está en capacidad de coordinar, analizar, evaluar y dictaminar sobre un hecho punible, a través de los indicios encontrados en el lugar de los hechos, de tal manera que el rol de investigador tiene una responsabilidad única, en virtud que es quien ofrece al fiscal y este luego al juez las pruebas necesarias para la sentencia.

Por ejemplo, por mencionar un caso del uso de la tecnología en materia de investigación criminal; para el Instituto Nacional de Ciencias Forenses, en la actualidad es mucho más fácil identificar huellas dactilares dejadas en las escenas del crimen gracias al sistema automático de identificación de huellas dactilares también conocido como AFIS por sus siglas en inglés, este aspecto cobra relevancia al puntualizar que en el pasado, se tomaban las huellas dactilares de los sospechosos usando tinta negra.

El método actualizado implica rodar los dedos y palmas de los sospechosos en un formato de ficha dactilar, procedimiento efectuado por un técnico de la Unidad de Recolección de Evidencias del Ministerio Público; luego son enviadas al laboratorio de dactiloscopía del instituto en mención donde se digitalizan dichas impresiones, generando imágenes que son escaneadas e introducidas al sistema AFIS para que sean comparadas con más de dos millones de huellas dactilares en una base de datos, alimentada inicialmente con información del Registro Nacional de las Personas (RENAP) y secundariamente con información del Sistema Penitenciario guatemalteco; dicho sistema identifica cualquier coincidencia con cualquier persona, cuyos registros se encuentran en la base de datos de las instituciones citadas con anterioridad.

A pesar de que en la última década en Guatemala se han producido notables avances en materia de investigación criminal, con el fortalecimiento de instituciones vinculadas al sector justicia, refiriéndose al Ministerio Público como titular de la Investigación criminal, Instituto Nacional de Ciencias Forenses y Organismo Judicial; continúa evidenciándose notables inconsistencias en torno a la investigación en material criminal, de esa cuenta es el principal problema del sistema en general.

En tiempos en los que los volúmenes de información integran enormes archivos, se hace necesario un tratamiento más complejo de la información, esperando encontrar relaciones eficientes y comportamientos en los datos que no pueden identificarse mediante un tratamiento estadístico clásico.

Las técnicas estadísticas clásicas se centran, generalmente, en procedimientos confirmatorios, mientras que los sistemas de explotación de información son exploratorios, pudiendo validar comportamientos ya conocidos como también plantear nuevas hipótesis.

Derivado de esta consideración es importante recapitular un poco en este aspecto se debe tener plena conciencia que de la efectividad en el procesamiento de la información recabada en la investigación criminal, se desprende una serie de eventos colaterales, que coadyuvan o bien van en detrimento del esclarecimiento de un evento delictivo, puesto que tanto las herramientas tecnológicas como el uso adecuado que se le brinde por el equipo humano que tiene acceso a esta, se origina tanto los buenos resultados como también puede contribuir con la fuga de esta información a incrementar la impunidad en el país.

Se han realizado esfuerzos conjuntos entre el Registro Nacional de las Personas (RENAP), Ministerio Público y Policía Nacional Civil para disponer de la base de datos del registro citado; sin embargo, por cuestiones administrativas y/o burocráticas, aun no se dispone de la integración total de este sistema; en ese sentido la Fiscalía debe efectuar requerimientos por escrito a fin de obtener la identificación de una persona en

particular, circunstancia que resulta onerosa en recurso material como en tiempo, impactando directamente en los tiempos y movimientos que se desarrollan en el proceso de la investigación penal en el país.

4.4. Limitaciones de la investigación y peritaciones

Dentro del campo de la criminalística podemos identificar la informática forense, la que va adquiriendo importancia, resalta su carácter científico, por ello, tiene sus fundamentos en las leyes de la electricidad, de la física y el magnetismo, siendo importante puntualizar que con base a fenómenos electromagnéticos que la información puede ser almacenada; por ello se afirma con certeza que la informática forense colabora en la investigación de delitos cometidos por organizaciones criminales, apoyándose en el método científico.

La evidencia digital permite acreditar hechos que conllevan efectos jurídicos. A título de ejemplo, estos pueden ser: fugas de información confidencial, alteración de documentos electrónicos, empleo sin autorización de creaciones protegidas por la propiedad industrial o intelectual, actuaciones de competencia desleal, etc.

Los anteriores pueden desencadenar procesos judiciales de tipo mercantil, civil, laboral o social, administrativo y penal. Sin embargo, la evidencia digital también puede evitarlos, pues permite acreditar el cumplimiento de las obligaciones derivadas de un contrato. Las evidencias digitales se alojan en servidores de correo electrónico, teléfonos móviles, dispositivos USB, discos duros de ordenadores de puestos de trabajo, Internet, entre otros de especial importancia.

Debe recordarse que los delincuentes hoy en día están utilizando la tecnología para facilitar la comisión de hechos ilícitos y eludir a las autoridades. Este hecho ha logrado que las Tecnologías de la Información y la Comunicación se convierten en herramientas necesarias en auxilio de la justicia y la persecución de delito y el delincuente. La

obtención de Información demanda que los investigadores forenses encargados de la recolección preservación, análisis y presentación de las evidencias digitales hagan una labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal.

Dentro de las principales limitaciones para la investigación y las peritaciones, es importante destacar que, así como a la cotidianeidad en la utilización de múltiples dispositivos electrónicos, las autoridades encargadas de la investigación criminal han demostrado un enorme interés en poder acceder y analizar toda esa abundante información digital que diariamente manejamos y utilizarla para la investigación de toda clase de delitos.

En este orden de ideas, es importante señalar que otras de las limitaciones específicas respecto a la identificación y cualificación oportuna de los medios electrónicas o digitales, se encuentra lo relativo a la ausencia de legislación sobre delitos informáticos y por ende se considera que tiene sus repercusiones jurídicas, económicas y sociales en el país, básicamente, porque la informática es aplicada en muchas áreas de la actividad humana, como industria, investigación, entretenimiento, comunicaciones, transportes, química e ingeniería, entre otras.

Es precisamente ese flujo de información, lo que ha propiciado el incremento paulatino de ilícitos informáticos, tales como: producción, oferta, difusión y adquisición de contenidos pornográficos, distribución de material racista, amenazas o intimidación en redes sociales, suplantación de identidad y de páginas electrónicas, extorsión en línea; siendo solo algunos de los delitos que no están tipificados en Guatemala y que ocurren cotidianamente, generando enormes repercusiones en el ámbito jurídico y económico por el costo que debe asumir el Estado o particulares y sociedades, porque son determinados sectores los que reciben el mayor impacto, como la niñez y adolescencia, todo porque la única reseña sobre delitos informáticos, se encuentra en el artículo 274 “A”, “B”, “C”, “E”, “F”, “G”, del Decreto número 17-73 del Congreso de la República de Guatemala, Código Penal, relativo a la destrucción de registros

informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información y programas destructivos, que vienen desde 1996 y que resultan demasiado ambiguas en la actualidad.

En ese contexto, es importante destacar que la inclusión de nuevas tecnologías en un sistema con prácticas propias de sistemas escritos y secretos como en el contexto Latinoamericano, no tiene mucho sentido por cuanto pueden mejorarse los equipos informáticos, a su vez también puede gradualmente eliminarse el expediente físico y cambiarlo por uno virtual, puede incluirse en general nuevas tecnologías para mejorar la gestión, pero ello no cambiará la lógica del secreto, de la burocracia, no mejorará la publicidad y transparencia necesarias en un sistema judicial democrático, no mejorará la situación del víctima en el proceso, no eliminará la delegación de funciones y la lejanía del juez con las partes y con el caso en general y lo más importante, no cambiará el hecho de que esos sistemas no respetan derechos fundamentales internacionalmente reconocidos como el debido proceso.

Es importante destacar que la investigación criminal, si bien ha tenido notables avances, muchos de ellos gracias al manejo de la evidencia digital, resulta de interés puntualizar que continúan existiendo notables deficiencias técnicas para la identificación, documentación y recolección de todo tipo de material indiciario digital; es en torno a estos preceptos que se considera que la principal limitación de la investigación gira en torno al desconocimiento por parte de los técnicos en investigaciones criminalísticas de la Unidad de Recolección de Evidencias del Ministerio Público, sobre los procedimientos a seguir para la recolección, embalaje y custodia del material digitak que es susceptible de localizar en los escenarios criminales que acontecen en la realidad guatemalteca.

Este aspecto constituye una labor pendiente en materia de investigación criminal, pues en tiempos donde la globalización ha invadido con material tecnológico cada esquina de las ciudades, es inconcebible que no existan mecanismos de recolección de

elementos de investigación digital como acontece en otras ciudades o Estados, donde se prioriza ampliamente esta labor investigativa.

La investigación de la delincuencia informática no es una tarea fácil, porque la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan rastros digitales, que suelen ser volátiles y de vida corta, en ese sentido se considera que también se plantean problemas legales en relación con las fronteras y las jurisdicciones donde es susceptible de aplicar la investigación criminal forense y que apenas empieza desarrollarse en Guatemala.

Acorde con esta aseveración y a fin de reforzar esta, es importante destacar que el Instituto Nacional de Ciencias Forenses de Guatemala (INACIF), inauguró en el mes de abril de 2017, el laboratorio de informática forense, el cual contribuirá al análisis de la evidencia que se localice en dispositivos electrónicos.

El laboratorio en mención fue financiado con el apoyo de la Instancia de Coordinadora de la Modernización del sector justicia, la Oficina Internacional de Asuntos Antinarcóticos y Procuración de Justicia (INL) y Agencia de los Estados Unidos para el Desarrollo Internacional (USAID).

Este laboratorio contribuye a fundamentar bien los casos con la prueba objetiva para las sentencias, ya sean condenatorias o absolutorias. En tal sentido, la prueba científica es el aporte hacia persona que se le reclama un hecho punible. Comprende cualquier instrumento digital que tenga información almacenada y que represente evidencia en cualquiera de los juicios que ocurren en el país, tales como pedofilia, pornografía, económicos, entre otros muchos más.

De esa cuenta se considera que dicho laboratorio surgió a raíz de que la utilización de la tecnología de información y comunicación permite almacenar, procesar y transportar datos en forma fácil, rápida y cómoda, pero con esto se aumentan los delitos informáticos que generan daños sensibles, por ello era necesario contar con este

laboratorio. En ese contexto, cuando se hace el análisis deben tener cuidado para no alterar el documento, por eso se debe generar una copia exacta y trabajan sobre esta para recuperar la imagen se fue borrada o extraer los archivos que estén allí.

Importante hay que destacar que dentro de la labor que tiene a bien desarrollar este laboratorio, se puede obtener fotografías, audios o documentos comprimidos siempre que estén almacenados dentro del dispositivo. Otros de los servicios que puede brindar el laboratorio son la búsqueda y extracción del historial de navegación de internet, así como la recuperación de archivos en el espacio no asignado del medio de almacenamiento. En el caso de redes sociales se puede establecer el IP o bien verificar la propiedad intelectual de los documentos.

Dentro del artículo 28 del Acuerdo No. CD (INACIF) 027-2012, Reglamento de Organización y Funcionamiento del Instituto Nacional de Ciencias Forenses de Guatemala, se establece que es la dependencia encargada de realizar peritajes mediante la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos. Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de estos, sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. Es así como el conocimiento informático forense abarca no solamente del software, sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información, entre otros.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats, entre otros. Con esta gama de posibilidades y actividades que desarrolla dicho laboratorio, se considera que constituye un amplio abanico de elementos que son susceptibles de solicitar ante dicho laboratorio

por las diferentes fiscalías del Ministerio Público, pero que por el desconocimiento o falta de la técnica adecuada para recolectar, embalar y remitir los indicios identificados en el lugar del delito, no se envían a este laboratorio, sino que lo que se realiza es efectuar un embalaje general y con la mínima descripción, a fin de que sea recibida por la Unidad de Asistencia Técnica, ubicada como dependencia de la Dirección de Investigaciones Criminalísticas, pues los requisitos para recibir los indicios recolectados son mínimos, mientras que por parte del laboratorio de informática forense del Instituto Nacional de Ciencias Forenses, existe todo un protocolo que debe seguirse para que pueda recibirse cualquier dispositivo, por mínimo que sea el peritaje a realizar o desarrollar dentro del medio electrónico que se les hace llegar.

Tal y como se ha venido exponiendo, la evidencia digital constituye toda información o registro almacenado en un computador o dispositivo informático que puede ser extraído y ser utilizado como prueba o evidencia soporte en un proceso legal, de esta forma se estima que otras de las falencias o debilidades en el mecanismo actual de identificación, documentación y recolección de este tipo de indicios, es lo relativo a la cadena de custodia, básicamente, porque a través de esta se asegura la integridad del indicio y le brinda certeza jurídica al mismo, desde su recolección en el lugar de los hechos, hasta su valoración por parte del tribunal o juzgador.

Sin embargo, todos estos aspectos no se cumplen con precisión dentro del mecanismo vigente de recolectar y trasladar los indicios respectivos, por lo tanto, la información que pudiera contener este tipo de material indiciario, pierde su fidelidad o confiabilidad, al mantener sus características originales, evitando con ello, alteraciones, sustituciones o cualquier tipo de contaminación durante la investigación y ya dentro del proceso judicial, en el cual se encuentra incluida como parte del cumulo de elementos probatorios.

En ese sentido, es importante también tener en cuenta que este tipo de información o datos se encuentran almacenados o registrados en dispositivos magnéticos o digitales que requieren de un correcto almacenamiento y organización con el fin de contar con

todas las características que garanticen la inocuidad y la esterilidad técnica en el manejo de estos durante las diferentes etapas y procesos que requieran de su consulta. El cumplimiento estricto de los pasos y procedimientos establecidos en la cadena de custodia permite garantizar la idoneidad de la prueba dentro de un proceso judicial, penal

Se ha establecido que, para ser admitida o tenida en cuenta como prueba dentro de un proceso, la evidencia digital debe cumplir con los siguientes aspectos: a) Autenticidad

b) Confiabilidad
c) Suficiencia
d) Conformidad con las leyes.

La autenticidad de la evidencia se refiere a que esta se haya generado y referenciado en los lugares relacionados con el caso o proceso examinado. Se refiere también a que esta no haya sufrido alteraciones y que por tanto corresponde a la realidad de la situación examinada. Derivado de ello, es importante que toda evidencia digital cumpla con estos cuatro conceptos con el fin de garantizar que una prueba basada en evidencia digital soporte total y adecuadamente un hallazgo o situación evidenciada en un proceso penal.

Por otro lado, la confiabilidad de una prueba se relaciona con el hecho de que la evidencia recolectada y aportada a un proceso proviene de una fuente creíble y verificable. En cuanto a la suficiencia, se busca que se presente la cantidad necesaria de material probatorio que permita asegurar que la situación presentada como delito o que represente una falta a la normatividad vigente, pueda ser soportada en las pruebas de manera completa y clara. Por último, las leyes establecen que los mecanismos y métodos utilizados para la recolección, preservación y análisis de la evidencia digital, se ajuste a la normatividad del país o lugar donde se presenta. No obstante existir lineamientos y estándares internacionales, se debe tener en cuenta que su aplicación se ajuste a la legislación o normatividad relacionada para el caso y lugar de los hechos.

Otra de las limitaciones para la investigación criminal y esencialmente en torno a las peritaciones que se realizan en materia de recolección de indicios o material electrónico, se encuentra la ausencia de adopción dentro de la legislación guatemalteca.

Como se ha establecido, la Unidad de Recolección de Evidencias del Ministerio Público no cuenta con un manual o protocolo para el adecuado manejo de la evidencia digital, en una escena del crimen o como parte de las diligencias de investigación, ya sea en la comisión de delitos informáticos o cuando se utiliza un sistema informático o las denominadas tecnologías de la información y las comunicaciones, para consumar un hecho delictivo donde pueda ser afectado cualquier bien jurídico.

Al hacer una revisión de la legislación vigente, se ha establecido que el Decreto número 47-2008, “Ley para el reconocimiento de las comunicaciones y firmas electrónicas”; contiene una serie de normas que sirven de base para el reconocimiento jurídico de las comunicaciones electrónicas, si bien es cierto este Decreto regula cuestiones relacionadas principalmente con el comercio electrónico, esta puede dar una guía legal para poder elaborar procedimientos para el manejo y presentación de lo que se conoce como mensajes de datos, un concepto que se relaciona con lo que se conoce como evidencia digital.

En primer lugar, la ley contiene una serie de definiciones que ayudan a la mejor interpretación de esta, para efectos del presente trabajo entre los conceptos más destacados se encuentran, lo que se debe entender como *Comunicación electrónica,* que la ley la define como toda comunicación que las partes hagan por medio de mensajes de datos y este último que considero que tiene relevancia para la presente investigación, *mensajes de datos,* los cuales la ley los define como, el documento o información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (IED), el correo electrónico, el telegrama, el télex o el telefax. Como se puede entender de estas definiciones es que las comunicaciones electrónicas están formadas por mensajes de datos y los mensajes consisten en toda esa información que se traslada por medio de

sistemas informáticos y que esta puede ser enviada, generada, o recibida y sobre todo almacenada, en diferentes tipos de soportes, principalmente, electrónicos, ópticos o magnéticos; se puede asegurar con toda certeza que la mensaje de datos y evidencia digital son conceptos similares, la diferencia aquí es que el concepto de mensajes de datos se relaciona con aspectos de comercio o comunicación, según la ley y la evidencia digital, hace referencia a aspectos probatorios en ambientes jurídicos, pero que en cualquier caso lo que la ley busca es darle esa eficacia jurídica a los mensajes de datos que componen las comunicaciones electrónicas.

Aspecto importante es que la ley regula en los artículos 11, 12 y 13, aspectos procesales en cuanto a la admisibilidad y fuerza probatoria de las comunicaciones electrónicas, el criterio para valorar una comunicación electrónica como prueba y la forma de conservación de las comunicaciones electrónicas; normas que pueden servir de base para la elaboración de protocolos para el adecuado manejo y conservación de la evidencia digital, los requisitos que se deben cumplir para que esta pueda ser admitida y valorada de un proceso legal; y en el caso que nos ocupa dentro de un proceso penal.

En primer lugar, la ley establece que las comunicaciones electrónicas serán admisibles como medios de prueba, que no podrá negársele fuerza probatoria a estas en cualquier actuación ya sea de índole administrativo, privada y para efectos de la presente investigación en cualquier actuación judicial, incluyendo entonces el área penal, hace mención que las comunicaciones electrónicas pueden ser presentadas y considero que así debe ser, en su forma digital.

Establece la ley que para valorar la fuerza probatoria de un mensaje de datos, se utilizaran criterios reconocidos por la legislación, en el caso que sea diligenciada dentro de un proceso penal se utilizara el sistema de la sana critica razonada, además, se debe establecer la fiabilidad de los mensajes de datos en tres aspectos, el primero de la forma que es el mensaje de datos se haya generado, archivado o comunicado, el segundo de la forma en que se haya conservado la integridad de la información, el tercero la forma en que se pueda identificar a su iniciador; es decir, identificar el origen de la

comunicación que contiene los mensajes de datos y la ley establece cualquier otro factor pertinente.

Por último, la ley regula lo relativo a la forma en que las comunicaciones electrónicas y sus respectivos mensajes de datos deben ser conservadas para poder ser admitidas y valoradas en cualquier proceso legal, llenando tres requisitos, el primero que la información que contengan sean accesibles para su posterior consulta, lo que refiere a la disponibilidad de la información y llenar los requisitos de contradicción y derecho de defensa; el segundo que la comunicación electrónica sea conservada en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que se reproduce con exactitud la información, aspecto que se refiere a la integridad de la información y por último que se conserve si es posible, toda información o dato que permita determinar el origen, el destino del mensaje, la fecha y la forma en que fue enviado o recibido, con lo que se pretende establecer la relación entre sujetos dentro de un proceso, en el caso del proceso penal, puede ser entre sujeto activo y pasivo o un tercero que tenga relación o participación dentro del hecho que se investiga.

Esta ley ofrece una guía de aspectos básicos y generales a considerar para la admisión, valoración y conservación de la evidencia digital dentro de un proceso penal, claro está, la ley es de carácter administrativa, pero contiene aspectos muy puntuales para el correcto manejo y presentación de la evidencia digital; sin embargo es necesario el desarrollo de estas normas para poder elaborar un manual con aspectos técnicos que permitan cumplir con los requisitos que en la ley se plantean, toda vez que en una investigación criminal se deben garantizar los principios propios del proceso penal, con el objeto de resguardar la presunción de inocencia, el derecho de defensa, el debido proceso, por lo que sigue siendo necesario que se creen esos protocolos para el manejo de la evidencia digital, tomando en consideración está normativa vigente.

Complementando lo anterior se considera que la Norma ISO/IEC 27037:2012, norma internacional provee orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar

su valor probatorio. Se orienta su uso a las investigaciones, en las cuales interviene el uso de recursos electrónicos o digitales.

En función de los elementos vertidos con anterioridad, es importante señalar que, dentro de esta normativa de estandarización internacional, se definen dos roles de especialistas en el manejo y administración de las evidencias electrónicas:

a) Digital Evidence First Responders (DEFR). Experto en primera intervención de evidencias electrónicas.
b) Digital Evidence Specialists (DES). Experto en gestión de evidencias electrónicas.

La norma ISO / IEC 27037:2012 se enfoca en el tratamiento de los siguientes dispositivos:

a) Medios de almacenamiento digitales utilizados en ordenadores tales como discos duros, discos flexibles, discos y magneto ópticos, dispositivos de datos con funciones similares.
b) Teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria.
c) Sistemas de navegación móvil.
d) Cámaras digitales y de video (incluyendo CCTV).
e) Ordenadores de uso generalizado conectados a redes
f) Redes basadas en protocolos TCP/IP y otros
g) Dispositivos con funciones similares a las anteriores.

De esta cuenta se estima que esta norma en esencia está orientada al manejo de la evidencia digital, buscando garantizar que dicha evidencia se ajusta a los requerimientos judiciales. De igual manera, se le considera como una norma de amplia aplicación, en virtud que cubre una variedad de dispositivos y situaciones a examinar.

La norma establece los principios de relevancia, confiabilidad y suficiencia de la evidencia obtenida a partir de dispositivos informáticos. De esta manera, los principios señalados es la relevancia, que se refiere a que la evidencia digital obtenida debe estar relacionada con los hechos investigados.

La confiabilidad es otros de los principios regulados dentro de esta norma en concreto y este se refiere a la certeza que la evidencia digital obtenida no ha sido alterada en ningún caso, desde su identificación, recolección, preservación y análisis hasta su presentación en el proceso en que es requerido.

En ese orden se presenta también la suficiencia, el cual se refiere a que la evidencia por si misma debe ser suficiente para explicar el hecho evidenciado y el cual es sujeto de análisis. Continúa estableciendo esta norma ISO sobre la evidencia digital que para el manejo de la evidencia se requiere disponer de tres etapas en particular, refiriéndose expresamente a la recolección, adquisición y preservación.

De acuerdo con estas consideraciones, es de suma utilidad puntualizar en cuanto a que la totalidad de las acciones que se realizan, relacionadas con la recaudación, manejo y cuidado o preservación, se requiere de la minucia respectivo y por consiguiente es razonable para el efecto efectuar el detalle respectivo.

4.5. Evaluación de casos concretos

De acuerdo con el contexto de los preceptos vertidos con anterioridad, es consistente en el presente apartado efectuar el detalle breve, pero conciso de tres casos concretos, en los cuales se ha evidenciado la importancia o trascendencia que tiene la evidencia digital para encauzar positivamente o dirimir el litigio que es sometido a consideración de los órganos jurisdiccionales correspondientes, en virtud que como se ha ido exponiendo es de vital importancia en una actualidad invadida o sumergida en dispositivos electrónicos o digitales, los cuales pueden ser determinantes para identificar

innumerables elementos probatorios decisivos, en virtud que para los criterios de los juzgadores, este tipo de pruebas es relevante e inclusive fundante para las decisiones dentro de las sentencias respectivas.

Caso concreto No. 1

Dentro del expediente número C01074-2013-00363, correspondiente a la sentencia emitida por el Tribunal Octavo de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente, con fecha uno de abril del año 2014, en proceso donde resultó ofendido el Banco de Desarrollo Rural Sociedad Anónima y aparecen como sindicados dos personas de sexo femenino, por los delitos de casos especiales de estafa y uso de información, ambos en forma continuada.

Los eventos se suscitaron cuando una de las acusadas teniendo la función de gerente de una agencia bancaria en la Ciudad de Guatemala, abusando de sus atribuciones y aprovechándose de las funciones inherentes a su cargo, omitió intencionalmente los procedimientos establecidos por la entidad bancaria agraviada, mediante ardid hizo incurrir en error a la entidad agraviada, pues en conjunto con una persona de sexo femenino, también trabajadora de dicha entidad, consultaron si autorización y de manera injustificada, la información de los registros informáticos del Banco, de los titulares de la cuenta de depósitos monetarios 3-291-00090-9, a fin de solicitar un talonario de 40 cheques con números correlativos del 2561 al 2600, sin que los titulares de dichas cuentas lo hubieren solicitado ni tampoco tuvieren conocimiento ni estuvieren presentes, haciéndole creer al Banco que fueron los clientes, quienes oportunamente los solicitaron, cuando en realidad, valiéndose de su posición efectuaron el trámite de forma paralela.

Después de haber consultado y utilizado la información de la cuenta, utilizaron nuevamente los usuarios y huellas dactilares para solicitar en el sistema informático, que el referido talonario de cheques fuera enviado a la Agencia número 800, en la zona 17, donde se entregaron dichos talonarios a una persona de sexo masculino que no era el

titular de la cuenta, posteriormente de ese talonario de cheques fue utilizado para efectuar el cobro por un tercero por un monto de Q.260,000.00, con lo cual se defraudó el patrimonio del titular de la cuenta, además, se incumplió el procedimiento en dicho pago, pues no se efectuó la llamada correspondiente al titular de la cuenta para informarle que se efectuaría el pago del cheque en mención.

Luego del cobro en mención, la persona que lo efectuó realiza un depósito por Q.245,000.00 a su propia cuenta y posteriormente giró otros 3 cheques a nombre de terceros para cobrar esos montos. Por esa razón el Banco tuvo que ser solidariamente responsable con el titular de la cuenta afectada y reintegrar el monto defraudado, por esta razón y con base a la prueba producida en la audiencia del debate valorada positivamente, conforme las reglas de la sana critica razonada, se tienen por acreditados los hechos siguientes: Que los procesados con el propósito de defraudar el patrimonio de la entidad Banco de Desarrollo Rural sociedad Anónima y desempeñando el puesto de Gerente de Agencia, abusó de sus atribuciones y aprovechándose de las funciones de su cargo omitió intencionalmente los procedimientos establecidos por la entidad bancaria.

De esta forma a través de los elementos de prueba respectivos el tribunal les brindó amplio valor probatorio, destacándose entre estos: constancias del control de operaciones de auditoría interna de BANRURAL, con los usuarios utilizados para canalizar la información bancaria, se le brinda valor probatorio; a las constancias de bitácora de consultas de la cuenta de positivos monetarios efectuadas con el usuario CCMS, reporte de consultas de firmas por cliente de la cuenta, se les otorga valor probatorio, puesto que fueron extendidas por funcionario del banco.

Al historial del sistema de cómputo de Banrural de solicitud y activación de chequeras de cuenta de depósitos monetarios, se le otorgó valor probatorio, en virtud que fueron extendidas por funcionario del banco y acreditan las transacciones relacionadas con su cuenta monetaria.

Caso concreto No. 2

En cuanto al presente caso, es importante destacar que este corresponde al número único de expediente 01071-2013-00436. REF. C-03-2014 Of. 1. Del Tribunal tercero de sentencia penal, narcoactividad y delitos contra el ambiente del Departamento de Guatemala, con fecha 27 de marzo del año 2014, se tiene que el tribunal unipersonal procedió a dictar sentencia en contra de una persona de sexo masculino por el delito de Extorsión.

El detalle de los hechos indican que con fecha 23 de julio del año 2013, ante el Ministerio Público se presentó una persona de sexo masculino a presentar denuncia, porque cuando se encontraba realizando ruta de venta de productos de una empresa de productos alimenticios, sobre la 32 Avenida B, 20-02, zona 7 de Villa Hermosa, Municipio de San Miguel Peta, se le acercó una persona de sexo masculino de tez clara, con vestimenta de marero, playera floja de color negro y pantaloneta floja de lona, cuando la víctima se dirigió a pie a una tienda, ingresó con él a la tienda, se le acercó y le entregó un teléfono celular de color negro marca VERIKOOL, indicándole que recibiera el teléfono porque iba a recibir una llamada por lo que por temor aceptó el teléfono, luego ingresó una llamada del número 55180529, donde una voz de sexo masculino le exigió la cantidad de 4 mil quetzales de enterada y luego debían de pagar la cantidad de 300 quetzales semanales, accediendo a pagar a dicha demanda los días jueces de cada semana, los 300 quetzales.

Seguidamente se nombró a un agente investigador de la Unidad Contra el Desarrollo Criminal de las Pandillas de la Policía Nacional Civil, quien asesoró y brindó lineamientos a seguir por la víctima, con la finalidad de iniciar la investigación correspondiente y realizar un operativo para lograr la captura del extorsionador, por lo que el día 12 de septiembre del año 2013, se reprodujeron dos billetes de diez quetzales que sirvieron para simular la cantidad exigida por el extorsionador.

En la sentencia se valoraron los elementos probatorios recibidos en el juicio oral y público con eficacia condicional, encaminados a la averiguación de la verdad tomando en cuenta los principios de la sana crítica razonada

En ese contexto de la información extraída del teléfono aportado por la víctima, la información se obtuvo manualmente, destacando la fecha y hora que le aparecen registrados a la mensajería en ambas vías y que fue presentado gráficamente por la Fiscalía, se le brindó valor probatorio, tomando en consideración que permitió el esclarecimiento de un hecho delictivo a través del flujo intercomunicacional.

También se le dio valor probatorio a un teléfono celular de color negro marca VVIO con línea MOVISTAR; un teléfono celular de color negro en el cual se lee VERIKOOL perteneciente al operador MOVISTAR, prueba que se valoró en virtud de ser un elemento importante para tener por acreditada la existencia del delito cometido por el acusado y que al ser incorporado por su exhibición en la audiencia del debate se pudo establecer que esta tiene concordancia con lo declarado por los testigos.

Del análisis tanto individual como integral de la prueba producida en la audiencia del debate oral y público, tomando en cuenta los principios de presentación, proposición y sistemas de valoración probatoria conforme a los lineamientos legales, el tribunal determina que los hechos contenidos en la acusación y en el auto de apertura a juicio y que se le endilgan al acusado han quedado acreditados.

Asimismo, el juzgador estimó que se determinó la forma y modo de actuar del acusado, al intimidar a su víctima, entregándole un teléfono celular y posteriormente mediante llamadas telefónicas realizadas por personas desconocidas, lo amenazaban de muerte, sino entregaba la cantidad de 300 quetzales semanales para permitirle vender en el área de Villa Hermosa, Municipio de San Miguel Petapa, habiéndole impuesto al acusado una pena de ocho años de prisión.

De esta forma se considera que se le dio el valor probatorio correspondiente a la evidencia digital recolectada, como aparatos telefónicos y del contenido de este se arribó a la conclusión para emitir la condena correspondiente.

Caso concreto No. 3

El tercero de los casos sometidos al análisis para establecer la incidencia que tiene la prueba o evidencia digital, especialmente dentro del proceso penal guatemalteco, se refiere al expediente C-01074-20154-00604 del Tribunal Quinto de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente del Departamento de Guatemala, de fecha 24 de junio del año 2015, en proceso seguido contra dos personas de sexo masculino por el delito de extorsión, estableciéndose a través de las investigaciones practicadas por la agencia fiscal de extorsión del Ministerio Público que los acusados y aprehendidos el día 30 de noviembre del año 2014, llamaron a la víctima para exigirle la cantidad de 30 mil quetzales para no atentar o asesinar a alguno de su hijos o a su esposa, pues ya conocían donde vía y a qué horas salía y entraba a su casa, ante esto la víctima presentó la denuncia ante las autoridades correspondiente, de tal forma que fue asignado un investigador de la División de Acción Nacional Contra el Desarrollo Criminal de las Pandillas, para asesorar a la víctima, luego el agente asignando haciéndose pasar por la víctima, le respondió que únicamente contaba con la cantidad de 5 mil quetzales, a lo que el extorsionador estuvo de acuerdo con recibir e indicó que ese dinero tenía que entregarlo el día domingo 30 de noviembre del año 2014 a las nueve horas, frente a la Despensa Familiar ubicada en el área de aprehensión, indicando el extorsionador que el dinero lo quería dentro de una bolsa de nylon de color negro y que lo llegarían a recoger dos patojos, quienes le dirían que iba por el dinero de la extorsión, por lo que la víctima hizo entrega al agente investigador de 2 billetes de la denominación de cinco quetzales, los cuales se reprodujeron y se unificaron con recortes de papel periódico, simulando la cantidad demandada.

En ese contexto, el tribunal correspondiente emitió su valoración sobre la prueba material aportada por el ente acusador, de esta manera, se consideró para el efecto, un

celular de color negro con rojo marca Claro, una celular marca Samsung de color negro, así como el dinero y recortes de papel periódico empleado para simular el monto total del dinero.

En ese orden de ideas, los razonamientos que inducen a condenar a los acusados giran en torno a lo expuesto en el artículo 386 del Código Procesal Penal, de tal forma que el tribunal luego de valorar este tipo de evidencia digital y de los elementos contenidos en esta, condenó a 7 años de prisión inconmutables a los acusados. Ante esta serie de circunstancias se considera que en efecto se valoró ampliamente los elementos de convicción consistentes en evidencias de tipo digital, pues el tribunal se fundamentó en lo reflejado en mensajería y contenido telefónico.

Caso concreto No. 4

Sentencia de recurso de apelación especial por motivo de fondo 133-2018, de fecha cuatro de agosto de dos mil dieciocho, emitida por la Sala Regional Mixta de la Corte de Apelaciones de Jalapa-Jalapa

Dentro de este proceso se encuentra como acusada una persona de sexo femenino, por el delito de PRODUCCIÓN DE PORNOGRAFÍA DE PERSONAS MENORES DE EDAD.

Los hechos se dieron lugar el día veintinueve de marzo del año dos mil dieciséis, aproximadamente a las diecisiete horas con veintisiete minutos, en la residencia ubicada en la aldea El Chiltepe, del municipio de Jutiapa del departamento de Jutiapa, cuando la acusada con un teléfono celular le tomó fotografías desnuda a la menor [...] de nueve años de edad, la madre de la menor el día veintisiete de abril del dos mil dieciséis, en horas de la tarde ingresó a su cuarto de habitación de la residencia ubicada en la Ladea El Chiltepe, con el objeto de hacer limpieza derivado de que la acusada le pagaba que realizara este trabajo y dentro de un bote junto a la basura estaba una memoria micro SD marca A DATA, de color negro con capacidad de un GB memoria externa número de

serie WM ocho GR cero uno guion GUACA guion NA, características obtenidas de los peritajes realizados, memoria que recogió la madre de la menor y se la llevó y se la dio a su otra hija y le preguntó qué era y ella le explicó que era una memoria de teléfono y prestó un teléfono y fue así como observaron las fotografías en el celular y efectivamente se observaron a la menor [...] mediante una serie de fotografías donde se apreció a la menor vestida y luego se iba quitando la ropa hasta que se quedó desnuda haciéndose cosas como tocándose la vagina, luego la madre de la menor le reclamó el hecho a la acusada, quien lo negó, luego se arrodilló y le pidió disculpas y perdón, pero la acusada meses anteriores también le había insistido a la madre de la menor que se dejara tomar fotos desnuda y que le pagaría la cantidad de cien quetzales a lo que ella se negó. Al extraer la información de la memoria micro relacionada, que proporcionó la madre de la menor, por medio del Análisis Técnico Informático Forense, de la Dirección de Investigaciones Criminalísticas, se observan varias fotografías de la menor [...] vestida luego desnuda tocándose la vagina en el cuarto que la acusada habita en la residencia ubicada en la dirección antes descrita y cerca se observa un espejo y se puede ver una persona de sexo femenino con las mismas características de la acusada con un teléfono celular en las manos y dentro del mismo informe donde se recuperaron las fotografías eliminadas se pueden apreciar más fotografías de la menor agraviada vestida normal.

El juez Unipersonal de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente del departamento de Jutiapa, declaró a la acusada responsable del delito de PRODUCCIÓN DE PORNOGRAFÍA DE PERSONAS MENORES DE EDAD, se le impone la pena de siete años de prisión inconmutables y la pena de multa de sesenta mil quetzales, otorgándole valor probatorio al informe pericial realizada por personal de la Dirección de Investigaciones Criminalísticas, donde se estableció la extracción de la información, fotografías de la menor víctima, de la memoria micro SD descrita en la relación de los hechos, evidencia digital extraída del indicio antes descrito.

Caso concreto No. 5

Sentencia de Casación por motivo de fondo 1143-2017, de fecha siete de febrero de dos mil diecinueve, Corte Suprema de Justicia.

Dentro de este proceso se encuentra como acusado una persona de sexo masculino, por los delitos de ESTAFA PROPIA EN FORMA CONTINUADA, MANIPULACIÓN DE INFORMACIÓN EN FORMA CONTINUADA y USO DE INFORMACIÓN EN FORMA CONTINUADA y como víctimas la entidad Banco Agromercantil de Guatemala, Sociedad Anónima y otras personas individuales.

Los hechos se dieron lugar cuando el acusado, los días veintitrés y veinticuatro de agosto de dos mil diez, en diferentes momentos, desde las cuentas de correos electrónicos: seguridad@agromercantil.com.gt y servicios@agromercantil.com.gt; utilizando registros informáticos envió correos electrónicos a personas particulares y cuentahabientes del Banco Agromercantil de Guatemala, Sociedad Anónima, con el objeto de engañarlos para hacerles creer que el Banco les requería, a través de un vínculo electrónico ("link"), que proporcionasen los datos de sus cuentas bancarias, nombre de usuario y contraseña de acceso a la banca virtual legítima del Banco relacionado, logrando así perjudicar a varios cuentahabientes en su patrimonio, pues realizó débitos de a diferentes cuentas monetarias. En consecuencia, el procesado defraudó el patrimonio de la entidad Banco Agromercantil de Guatemala, Sociedad Anónima por la cantidad de ochenta y cinco mil quetzales.

El Tribunal Primero de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente del municipio de Mixco, departamento de Guatemala, en sentencia del catorce de mayo de dos mil doce resolvió, dictar una sentencia de carácter condenatorio y lo declaró autor responsable de los delitos de ESTAFA PROPIA EN FORMA CONTINUADA, MANIPULACIÓN DE INFORMACIÓN EN FORMA CONTINUADA y USO DE INFORMACIÓN EN FORMA CONTINUADA imponiéndole las penas de: por el delito de estafa propia en forma continuada, cometido en contra del patrimonio de la

entidad Banco Agromercantil, Sociedad Anónima; tres años de prisión conmutable a razón de cien quetzales por cada día de prisión y multa de cinco mil quetzales, por el delito de manipulación de información en forma continuada, la pena de tres años de prisión conmutables a razón de cien quetzales por cada día de prisión y multa de tres mil quetzales y por el delito de uso de información en forma continuada, la pena de un año y seis meses de prisión conmutables a razón de cien quetzales por cada día de prisión.

El tribunal consideró, que el procesado participó activamente en los ilícitos que se le imputaron, pues se apersonó a las agencias bancarias respectivas y abrió cuentas bancarias a su nombre con el propósito deliberado de que los usuarios transfirieran dinero ajeno a estas, lo que consiguió mediante la utilización de la tecnología “Vianet”, “Fishing” y “Paynexus”; pues retiró cantidades de dinero que dichos usuarios le transfirieron en forma anómala. De igual manera con esas transferencias se realizaron pagos de varios servicios; también se le pudo ver, mediante grabaciones de las cámaras de las agencias bancarias, realizando transacciones diversas, por lo que el ánimo de lucro quedó debidamente acreditado en autos. Dichos extremos reflejaron la autoría directa del procesado en los hechos imputados.

Contra lo resuelto por el tribunal, el procesado interpuso recurso de apelación especial por motivos de forma y de fondo.

La Sala Primera de la Corte de Apelaciones del Ramo Penal, Narcoactividad y Delitos Contra el Ambiente, en sentencia de fecha uno de agosto de dos mil dieciséis, declaró improcedente el recurso de apelación especial por motivos de forma y de fondo interpuesto por el procesado.

Contra lo resuelto por la Sala el procesado interpone recurso de casación por motivos de forma y de fondo.

Habiendo sido declarado improcedente el motivo de forma, se realiza el estudio del motivo de fondo invocado.

Para el primer caso de fondo invocado por el recurrente, es pertinente iniciar citando el contenido del artículo 10 del Código Penal, el cual establece: "...Los hechos previstos en las figuras delictivas serán atribuidos al imputado, cuando fueren consecuencia de una acción u omisión normalmente idónea para producirlos, conforme a la naturaleza del respectivo delito y a las circunstancias concretas del caso o cuando la ley expresamente los establece como consecuencia de determinada conducta...". Continuando con el desarrollo argumentativo, esta Cámara determina que se configuró la relación de causalidad para el tipo penal de manipulación de información, toda vez que esta se configura cuando la acción normalmente idónea se dirija a utilizar registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica. Es así que, de los hechos acreditados se establece que el procesado utilizó registros informáticos de computación para alterar información supuestamente requerida por la institución bancaria agraviada, con el objeto de aparentemente verificar el origen lícito del dinero depositado en dichas cuentas, para dar un fingido cumplimiento de una obligación respecto al Estado, aprovechando esto para alterar el monto real del dinero existente en las cuentas de los clientes de la entidad agraviada, por cuanto que el procesado sustrajo dinero de estas, afectando su situación patrimonial vía electrónica.

La Cámara Penal considera que existe relación de causalidad para la figura penal de uso de información, por cuanto que dicha figura se encuadra cuando la persona procesada "...sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, banco de datos o archivos electrónicos...". Es en ese orden de ideas, se estima que quedó acreditado ante el tribunal de sentencia que el procesado no teniendo la autorización del Banco Agromercantil de Guatemala, Sociedad Anónima, utilizó sus registros informáticos e ingresó al banco de datos y archivos electrónicos de sus clientes, a través de una operación fraudulenta (phishing), esto para adquirir información confidencial (contraseña), porque el procesado se hizo pasar por el agraviado banco en una aparente comunicación oficial electrónica (correo electrónico)

para adquirir dicha información. Es en esa línea de pensamiento que, el procesado ingresó al sistema de banca virtual del banco agraviado, creando una página electrónica falsa análoga a la original, solicitando la contraseña de los usuarios, con el objeto de verificar el origen de los fondos a solicitud de la Intendencia de Verificación Especial (Estado), logrando el procesado acceder a dichas cuentas y hacer traslados de sumas dinerarias propiedad de clientes del Banco Agro mercantil hacía cuentas de depósitos previamente abiertas por el procesado en mención.

A la vista de las puntualizaciones anteriores, se declaró improsperable el primer caso de procedencia invocado por motivo de fondo.

Caso concreto No. 6

Sentencia de Casación por motivo de fondo 336-2017, de fecha ocho de agosto de dos mil diecisiete, Corte Suprema de Justicia.

Dentro de este proceso se encuentra como acusado una persona de sexo masculino, por los delitos de HURTO AGRAVADO y MANIPULACIÓN DE INFORMACIÓN y como víctimas la entidad Banco Citibank de Guatemala S.A.

Los hechos sucedieron el día tres de agosto del año dos mil nueve (03/08/2009), en el período comprendido de las ocho a las diecinueve horas, constituido en la agencia número 557 de Banco Citibank de Guatemala S.A., “AGENCIA KIOSCO SUVISA” ubicada en sexta avenida ruta tres y cuatro zona cuatro del Municipio de Guatemala del Departamento de Guatemala, locales ocho y nueve del Centro Comercial “Mister Bodeguitas Plaza”; en su calidad de EJECUTIVO DE ATENCIÓN AL CLIENTE, desempeñándose como cajero encargado de la Agencia Kiosco Suvisa, usted utilizó el programa de computación denominado COBIS, propiedad de la entidad Bancaria Banco Citibank de Guatemala S.A., utilizado para registrar las operaciones contables relacionadas con las operaciones contingentes diarias de la agencia número quinientos cincuenta y siete (557) “AGENCIA KIOSKO SUVISA” de dicha entidad bancaria, ubicada

en la dirección antes descrita y registró de forma ilegal la transferencia simulada número CIENTO CUARENTA Y UNO (141) por la cantidad de TRESCIENTOS NOVENTA MIL QUETZALES (Q.390,000.00), denominada ENVÍO DE EFECTIVO EN AGENCIA, operación que quedó registrada en el sistema COBIS, REPORTE DE CAUSAS TRANSACCIONES DE CAJA ATX, con el usuario jl36099 en la cuenta contable 101.MON.010101, con destino a la entidad WACKENHUT DE VALORES S.A., por medio del transportadores de valores PROTECCIÓN DE VALORES S.A., habiéndose establecido en la presente investigación que dicha transferencia es totalmente falsa e inexistente, toda vez que las entidades antes relacionadas, indicaron no haber recibido dicho efectivo, información que fue confirmada por el Licenciado Roberto Gularte, Gerente de Operaciones de la entidad Protección de Valores S.A., (PROVAL) y en acta administrativa número 022-2009 faccionada en la entidad Wackenhut de Valores S. A, por Margarita Noriega, Gerente de Operaciones y José Luis López, Jefe de Auditoría de la referida entidad, donde se establece que en el período del treinta de julio al siete de agosto del año dos mil nueve (30/07/2009 al 07/08/2009), la AGENCIA SUVISA ZONA 4, SE ENCONTRABA CERRADA; se establece por medio del oficio de fecha cuatro de mayo del año dos mil diez (04/05/2010), firmado por Claudia Morales, Directora de Operaciones de la entidad Bancaria Banco Citibank de Guatemala S.A., que el usuario jl36099 con el cual se opera el sistema contable de Banco Citibank de Guatemala S.A., la simulación de dicha transferencia le corresponde al procesado, OPERACIÓN REGISTRADA EN EL SISTEMA CONTABLE DENOMINADO “COBIS” de la entidad bancaria Banco Citibank de Guatemala S.A., con el objeto de ocultar el hurto de efectivo de las cajas registradoras y la caja fuerte de la agencia número quinientos cincuenta y siete (557), “AGENCIA KIOSKO SUVISA” de la entidad Bancaria Banco Citibank De Guatemala S.A., realizado por el acisado por la cantidad de TRESCIENTOS NOVENTA Y NUEVE MIL QUINIENTOS DIECISIETE QUETZALES CON OCHENTA Y SEIS CENTAVOS (Q.399,517.86), acción ilícita que se prueba especialmente con el informe número BCB-AI-105-2009 firmada por [...], Directora de la Unidad de Control de Banco Citibank de Guatemala S.A. y las declaraciones testimoniales tanto de la señora [...] Directora de Control de la entidad Bancaria Banco Citibank de Guatemala S.A., como de

[...], Gerente de Auditoría Regulatoria de la entidad Bancaria antes relacionada, así como con la PERICIA CONTABLE, identificada como DICTAMEN 01-2010 de fecha diecisiete de mayo del año dos mil diez (17/05/2010), firmada por el CONTADOR PÚBLICO Y AUDITOR DEL MINISTERIO PÚBLICO, con funciones en la UNIDAD DE DELITOS RELACIONADOS CON BANCOS, ASEGURADORAS Y DEMÁS INSTITUCIONES FINANCIERAS DE LA FISCALÍA DE SECCIÓN CONTRA EL CRIMEN ORGANIZADO, donde se determina que usted manipuló el sistema informático de la entidad bancaria Banco Citibank De Guatemala S.A., con el ánimo de ocultar el hurto de TRESCIENTOS NOVENTA Y NUEVE MIL QUINIENTOS DIECISIETE QUETZALES CON OCHENTA Y SEIS CENTAVOS (Q.399,517.86). Por lo que su conducta, típica y antijurídica encuadra en los tipos penales de HURTO AGRAVADO y MANIPULACIÓN DE INFORMACIÓN

El Tribunal Octavo de Sentencia Penal, Narcoactividad y Delitos Contra el Ambiente, constituido en juez Unipersonal, dictó sentencia el diecinueve de noviembre de dos mil catorce, en la que condenó al acusado por los delitos de hurto agravado y manipulación de información.

Para arribar a la anterior decisión concluyó lo siguiente: "… Para el juzgador resulta suficientemente probado, que los actos propios del delito, fueron desarrollados en forma personal por el acusado, debido a que la ejecución de los delitos requería la utilización de la confianza que le depositó el banco al procesado y que aprovechando al acceso del dinero que se le había confiado se apoderó de este sin la autorización de su propietario y dicha conducta la oculta utilizando el sistema informático con el cual realiza una falsa transacción la cual no cuenta con el respaldo documental necesario para establecer que efectivamente existió, con lo cual se concluye que se hizo solo con la finalidad de ocultar el hecho de haber tomado la cantidad de dinero antes referida para su apropiación por lo que el procesado es responsable penalmente por haber participado en forma directa y personal en los delitos por lo cual tiene la calidad de autor…"

El procesado el procesado interpuso recurso de apelación especial por motivo de fondo, en el que señaló como único submotivo de fondo la interpretación indebida de los artículos 246 y 247 concatenados al artículo 10, todos del Código Penal.

Argumentó que en la sentencia de primera instancia existió una evidente interpretación indebida de los artículos 246 y 247 del Código Penal, pues en los hechos que el Tribunal estimó como acreditados y en el material probatorio al que se le dio valor probatorio, se desprendió que el acusado no era penalmente responsable a título de autor del delito de hurto agravado por el que se le condenó, pues no se demostró fáctica y probatoriamente en el juicio que el procesado se haya apoderado de dicho dinero, así como tampoco se probó que el procesado haya desplazado o tenido control sobre la cantidad dineraria que se le imputó, por lo que su conducta no encuadraba en el delito de hurto agravado al no concurrir los verbos rectores necesarios para su encuadramiento, los cuales eran el apoderamiento, desplazamiento y control de la cantidad aducida; además, refirió que derivado de que no se acreditó el actuar del procesado encuadrado en el delito de hurto agravado, su conducta solo encuadraba en el delito de manipulación de información, pues las acciones desarrolladas se concretaron exclusivamente en manipular la información, propias del delito de manipulación de información, por lo que existió interpretación indebida del delito de hurto agravado, al tipificarlo sin concurrir sus verbos rectores necesarios.

La Sala Segunda de la Corte de Apelaciones del ramo Penal, Narcoactividad y Delitos contra el Ambiente, en sentencia de trece de febrero de dos mil diecisiete, no acogió el recurso de apelación especial por motivo de fondo interpuesto por el procesado.

Para el efecto consideró lo siguiente: "… De los hechos acreditados, se extrae que las acciones realizadas por el acusado, son idóneas para producir el resultado que encuadra en el delito de Hurto Agravado, toda vez que se acreditó que el acusado sin la debida autorización del propietario y con abuso de confianza tomó la cantidad de TRESCIENTOS NOVENTA Y NUEVE MIL QUINIENTOS QUETZALES CON OCHENTA Y SEIS CENTAVOS (Q.399,517.86), a Banco Citibank de Guatemala S.A., propietario de dicho dinero, tal como se regula y determina en los artículos 10, 246 y 247 del Código Penal. Además, es necesario acotar en el análisis que el motivo de fondo, se dirige al vicio de valoración jurídica de los hechos, no discutiendo el error en la fijación de los

sucesos, ello significa que los hechos acreditados por el Tribunal de Sentencia se mantienen firmes para la apelación especial, únicamente, corresponde hacer un análisis sobre su real significado jurídico de estos [...] En atención a los argumentos anteriormente expuestos, el recurso de apelación especial por motivo de fondo interpuesto resulta improsperable".

El procesado interpone recurso de casación por motivo de forma e invocó como caso de procedencia el numeral 6) del artículo 440 del Código Procesal Penal, por inobservancia del artículo 11 Bis del Código Procesal Penal en relación con los artículos 389 numeral 4) de la misma norma y 12 de la Constitución Política de la República de Guatemala.

La Cámara estableció que la Sala impugnada no realizó el examen debido y, por ende, dejó en estado de indefensión al apelante, pues le impidió conocer las razones claras, completas y legítimas de porqué resolvió de la manera en que lo hizo, violentando el artículo 11 Bis del Código Procesal Penal y el artículo 12 constitucional.

Por lo anterior, la Sala no cumplió con la obligación de fundamentar su decisión, de conformidad con lo establecido en el artículo 11 Bis del Código Procesal Penal y, como consecuencia, debe declararse procedente el recurso de casación y ordenarse el reenvío de las actuaciones a la Sala impugnada para que, en observancia de los vicios señalados por esta Cámara, emita una nueva resolución sin estos.

Derivado de los elementos expuestos con anterioridad, es importante señalar que la evidencia digital tiene un amplio valor probatorio en los delitos de manipulación de información, uso de información; como delitos informáticos propiamente dichos, en donde se afecta a la información como bien jurídico; pero también la evidencia digital es de suma importancia cuando los sistemas informáticos y tecnologías de la información y de las comunicaciones son utilizados como medios para cometer otros delitos como la extorsión, secuestros, estafas, homicidios, asesinatos, producción de pornografía infantil, hurtos, solo por mencionar algunos de ellos, en virtud que del adecuado

tratamiento de estas, se concluye que pueden contribuir determinantemente a brindarle una solución efectiva y oportuna al proceso penal correspondiente, aunado a que influye notablemente en el criterio de los juzgadores, quienes valoran positivamente el contenido de este tipo de pruebas.

El Estado de Guatemala carece de los medios económicos, tecnológicos, culturales y jurídicos para poder enfrentar la criminalidad informática que cada día avanza a una velocidad impresionante, esto debido a que no existe una política de Estado que se encargue de esta problemática, aun la iniciativa privada no ha invertido lo suficiente para poder evitar los ataques informáticos a sus sistemas y dentro de las mismas instituciones de públicas o privadas existen personas con alto grado de conocimiento en esta materia que realizan conductas que están fuera de la ley.

Otra característica de esta forma de delincuencia es que, para cometer un delito de carácter informático, no es necesario estar físicamente presente en el lugar para su comisión; a nivel mundial se ha conocido de ataques a los sistemas informáticos de entidades públicas y privadas, personas que físicamente se encuentran en otros países del mundo. Con la introducción de la Internet y en la actualidad la aparición de las denominadas redes sociales el ámbito geográfico para que se cometan estos ilícitos penales se expande, más si no se cuenta con las herramientas, instituciones, tecnologías y leyes adecuadas; la delincuencia informática podrá seguir cometiendo sus ilícitos sin que se pueda dar una respuesta efectiva, en cuanto a la investigación.

Uno de los principales problemas que dificulta poder realizar una eficiente investigación de los delitos informáticos es el tratamiento de la evidencia, la denominada evidencia digital, que resulta ser lo más importante para poder combatir la delincuencia informática. La recolección, manejo, almacenamiento y análisis de este tipo de evidencia tiene sus particularidades y características que hacen que su tratamiento sea diferente a cualquier otro elemento probatorio, en Guatemala no hay una institución especializada en el tratamiento de esta evidencia, siendo el Ministerio Público el encargado de capacitar al personal de la Unidad de Recolección de Evidencias en el adecuado manejo

de esta, utilizando las técnicas que garanticen el manteniendo de las características y propiedades de la evidencia digital.

Debe recordarse que el crimen organizado se caracteriza por la utilización de diversas formas para apoderarse del patrimonio de personas jurídicas e individuales, básicamente para financiar sus operaciones ilícitas, de tal forma que en plena era de la información digital, utilizan medios informáticos sofisticados que no solo afectan el patrimonio, sino también a un bien jurídico, por mucho, más importante, como la información que puede canalizarse a través de mecanismos tecnológicos o informáticos, circunstancia que paulatinamente se ha ido incrementando, debido entre otros aspectos a la ausencia especifica o concreta de tipos penales dentro de la legislación guatemalteca.

Por toda esta gama argumentativa, cobra notoriedad, la importancia de efectuar y desarrollar manuales o protocolos para garantizar una identificación, documentación y recolección eficientes de la evidencia digital dentro de los diversos escenarios criminales en los que es susceptible de localizar.

4.6. Propuesta de guía procedimental para la recolección efectiva de la evidencia digital en Guatemala

Debido a la importancia que tiene la evidencia digital dentro del proceso penal guatemalteco, es más que consistente efectuar el desglose de una propuesta breve de los pasos a seguir para identificar y recolectar el indicio o evidencia dentro de cualquier escenario en el cual es susceptible de documentar y recolectar, para el efecto se considera prudente seguir los siguientes pasos:

No.	Actividad	Responsable
1	Identificar el indicio electrónico a recolectar (teléfono, laptop, desktop, cámaras digitales, dispositivos extraíbles y otros), que se encuentre debidamente apagado.	Técnico embalador del Ministerio Público
2	Documentar a través de foto y video, las características esenciales del objeto a fin de que quede individualizado (serie, lote, inventario, etc.)	Técnico fotógrafo y embalador.
3	Resguardar el dispositivo en bolsas Faraday (para evitar el manejo a distancia por terceros)	Técnico embalador
4	Efectuar la descripción del indicio, con todas sus características que lo hacen único	Técnico embalador
5	Efectuar el embalaje y cadena de custodia	Técnico embalador
6	Verificar datos del embalaje y cadena de custodia	Técnico embalador
7	Trasladar hacia unidad de Asistencia Técnica del Ministerio Público o Laboratorio de Informática Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF).	Técnico embalador.

Fuente: Elaboración propia. Investigación año 2018.

De acuerdo con estos preceptos, es de suma utilidad atender estos lineamientos, con el fin de garantizar el manejo integral de la evidencia digital, en cualquier escenario criminal, en los cuales sean susceptibles de localizar.

Conclusiones

En el proceso penal guatemalteco existe un marco legal mínimo que regula la admisión de la evidencia digital en un proceso penal, los criterios para que esta sea valorada y la forma en que debe ser conservada esta evidencia, a través del Decreto Número 47-2008, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónica; sin embargo, esta ley no es de carácter propiamente penal o procesal penal, por lo que se hace necesario desarrollar procedimientos, tomando como base esta norma que sirva para elaborar manuales para el adecuado manejo de la evidencia digital. Es necesario aprobar normas que establezcan las formas en que la evidencia digital debe ser diligenciada durante la investigación antes y durante un debate oral y público, con el objeto de garantizar la legalidad e idoneidad de esta y que se cumplan con el requisito de contradicción, para que la evidencia sea fiscalizada por los diferentes sujetos procesales durante su diligenciamiento.

En Guatemala, los actuales tipos penales regulados en la legislación se limitan a proteger el patrimonio de las personas; sin embargo, a nivel internacional se ha establecido que estas conductas ponen en peligro bienes jurídicos como la información, las comunicaciones, la intimidad, la indemnidad sexual de las personas, entre otros, por lo que es necesario se analicen las iniciativas de ley que actualmente se encuentran en discusión en el Congreso de la República, con el objeto de dar la seguridad jurídica a los ciudadanos. El Estado de Guatemala no ha ratificado el Convenio sobre la ciberdelincuencia de la Unión Europea, Budapest, instrumento internacional importante para actualizar la legislación nacional en materia de delitos informáticos y lograr la cooperación en esta materia para la investigación y persecución de los sujetos activos y las estructuras criminales transnacionales que se dedican a cometer estos delitos.

En la actualidad, no se cuenta con procedimientos o protocolos para el manejo, documentación y embalaje de la evidencia digital en una escena del crimen, por parte de la Unidad de Recolección de Evidencias del Ministerio Público, que es la unidad

encargada para el procesamiento de una escena de crimen y se utilizan los procedimientos normales para cualquier tipo de evidencia o indicio que se localice en una escena, lo que pone en peligro las propiedades propias de este tipo de evidencia lo que tiene como resultado que esta no pueda ser valoraba para poder establecer la culpabilidad de una persona dentro de proceso penal; por lo que resulta necesario y de carácter urgente, que se elabore un instrumento que contengan los procedimientos mínimos para el adecuado manejo de la evidencia digital

Referencias

Altmark, D. R. (1987. p. 64). *Informática y derecho.* Buenos Aires, Argentina.

Alvarado, R. y. (2016, p. 76). *Cibercrimen.* Guatemala: IUS.

Baón, R. R. (1996). *Visión general de la informática en el nuevo Código Penal.* Madrid, España. (s.e.)

Barrios, O. O. (2006). *Derecho e informática. Aspectos fundamentales.* Guatemala, Guatemala: Mayté.

Barrios, O. O. (2011, p. 2.). *El delito.* Guatemala, Guatemala. (s.e.).

Berducido Mendoza, H. E. (2004, p. 32). *Historia del proceso penal.* Guatemala, Guatemala. (s.e)

Binder, A. (1993, p. 19). *El Derecho Procesal Penal.* Guatemala, Guatemala. (s.e).

Bosch, C. F. (1997. p. 18). *Elementos fundamentales del derecho.* Ramírez. (s.e).

Cafferata, N. J. (1998). *La prueba en el proceso penal.* Buenos Aires, Argentina: Depalma.

Calderón, M. R. (2013). *Modulo de autoformación. La prueba en materia penal.* Guatemala, Guatemal: Instituto de la Defensa Pública Penal. (s.e).

Calderón, R. C. *El impacto de la era digital en el derecho.* Obtenido de http://www.vlex.com/redi/

Camacho, L. L. (1987). *El delito informático.* Madrid, España.

Chávez, G. A. (2012). *Policía Cibernética: Vigilancia preventiva, permanente y reactiva a los ilícitos informáticos.* Guatemala. (s.e).

Chouraqui, A. (1974). *L'informatique au service du droit.* París, Francia. (s.e).

Davara, R. M. (1996). *De las autopistas de la información a la sociedad virtual.* Pamplona, España: Aranzadi.

De la Rocha, H. (1997). *Presunciones e indicios en juico penal.* Buenos Aires, Argentina: Ediar.

De Pina Vara, R. (1983). *Diccionario de Derecho.* México D.F. : Porrúa S.A. .

Del Pino, S. A. (2007, p. 10). *Delitos informaticos, generalidades. .* Quito, Ecuador. (s.e).

Dellepiane, A. (2005). *Nueva teoría de la prueba.* Madrid, España.: Temis Ltda.

Desimoni, L. M. (1993). *La prueba indiciaria.* Madrid España: Centro de Estudios Judiciales. (s.e).

Florian, E. (1995). *De las pruebas penales.* (s.l.i), (s.e.)

Gamboa, J. (2010, p. 3). *Panorama del derecho informático en América Latina y el Caribe.* Santiago, Chile. (s.e).

Herrera, Á. C. (2010). *Hacia una correcta Hermeneutica Penal: Delitos informáticos Vs. delitos electrónicos.* Cuenca, Ecuador. (s.e).

Huerta, M. M. (2011). *Los delitos informáticos.* Buenos Aires, Argentina: Jurídica Cono Sur.

IDPP. *Historia del Instituto de la Defensa Pública Penal.* (Obtenido de http://www.idpp.gob.gt/: http://www.idpp.gob.gt/institucion/historia.aspx

Informatico, *Mundo informatico*. Obtenido de https://sites.google.com/site/mundoinformatico0/home/virus/1--cronologia

Jescheck, H. H. (1981, p. 350). *Tratado de derecho penal. Parte general.* Barcelona, España: Bosch.

Langer, M. (2011, p. 4). *Revolución en el Proceso Penal Latinoamericano: Difusión de ideas legales desde la periferia.* Santiago de Chile, Chile: CEJA - JSCA.

López Delgado, M. (2007). *Análisis forense digital.* Madrid, España. (s.e).

López, C. M. (2006, p. 45). *La violación al principio constitucional de presunción de inocencia pro parte de la Policía Nacional Civil durante la captura de imputados por hechos ilícitos.* Guatemala. (s.e).

Magdalena, O. W. Obtenido de https://scielo.conicyt.cl/: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-33992014000200001

Malatesta, F. (2002). *Lógica de las preubas en materia criminal.* Bogotá, Colombia: Temis S. A. .

Manzini, V. (1954, p. 20). *Tratado de Derecho Procesal penal.* Buenos Aires, Argentina: Jurídicas Europa-América.

Marín Vásquez, R. A. (2004). Sistema acusatorio y prueba. *Revista de temas procesales*, 44.

Melini, L. E. (2006, p. 45). *La violación de los principios de sencillez, celeridad y oralidad en los medios de impugnación del proceso penal guatemalteco.* Guatemala. (s.e).

Mittermaier, C. J. (1877). *La prueba en materia criminal.* Madrid, España: Imprenta de la Revista de Legislación.

Molina, S. J. (2003, p. 105). *Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial.* México D.F. (s.e).

Montaño, Á. A. (2008). *La problematica jurídica en la regulación de los delitos informáticos.* México D.F. (s.e).

Monterroso, C. J. (2003, p. 15). *Investigación criminal: Estudio comparativo y propuesta d eun modelo de policía de investigación en Guatemala.* Guatemala, Guatemala. (s.e).

Nación, S. C. (2011, p. 3). Valoración de la prueba circunstancia. *Revista Semanario Judicial de la Federación*.

Orozco Barrios, N. U. (2007). *Reparación del delito como una posible forma de sustituir las penas o de ser computada para atenuarlas dentro del proceso penal guatemalteco.* Guatemala, Guatemala. (s.e).

Ortíz Nishihara, M. H. *http://blog.pucp.edu.pe.* Obtenido de http://blog.pucp.edu.pe/blog/nuevoprocesopenal/2013/11/15/los-antecedentesmas-antiguos-de-la-prueba/

Ossorio, M. (2001). *Diccionario de Ciencias Jurídicas, Políticas y Sociales.* Buenos Aires, Argentina: Heliasta S.R.L.

Ovalle, F. J. (2016, p. 336). *Teoría general del proceso.* México D.F.: Oxford.

Plascencia, V. R. (2004, p. 1). *Teoría del delito.* México D.F.: Universidad Nacional Autónoma de México.

Portillo, M. W. (2012, p. 23). *El conflicto que existe entre la libertad de información y la vida privada de las personas en la República de Guatemala.* Guatemala. (s.e).

previa.uclm.es. *Introducción al derecho informático.* Obtenido de https://previa.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf

Quirós, H. Obtenido de s.calameo.com: https://es.calameo.com/read/005303851384fab394128

RAE. (2015). *Diccionario de la Real Academia Española.* Madrid, España: Civitas.

Ramón, I. (2001). *Informática y derecho.* Buenos Aires, Argentina. (s.e).

REDU. Obtenido de http://redusacunoc.tripod.com/: http://redusacunoc.tripod.com/PROCESAL_PENAL.html

Resa, N. C. (2005). *Crimen Organizado Transnacional.* Buenos Aires, Argentina: Astrea.

Reyes, A. (2007, p. 34). *Investigación del cibercrimen.* Buenos Aires, Argentina. (s.e).

Riestra, E. (1995, p. 118). *Informática jurídica aplicada a la enseñanza del derecho.* México D.F.: UNAM.

Rivero, A. (1986). Informática y derecho: La informática jurídica en España. *Informática y derecho monográfico*. (s.e).

Santos, C. O. (2007, p. 38). *La inconstitucionalidad en la celebración del debate cuando los jueces hacen interrogatorio a los procesados, en el Tribunal de Sentencia del Municipio de Santa Lucía Cotzumalguapa Departamento de Escuintla.* Guatemala. (s.e).

SEGOB. (2006). *Temas de derecho informático.* México D.F. (s.e).

Sosa, A. Obtenido de http://zefepalagot.blogspot.com/: http://zefepalagot.blogspot.com/2009/06/

Suñe, E. (1986). Introducción a la informática jurídica y al derecho de la informática. *Informática y derecho monográfico*. (s.e).

Téllez Valdés, J. (2008, p. 147). *Derecho Informático.* México D.F.: McGraw Hill.

Téllez, I. A. (2007, p. 45). *La investigación antropológica.* Alicante, España: Club Universitario.

Tellez, V. J. (1999). *Los delitos informáticos.* Buenos Aires, Argentina: Temis.

Tellez, V. J. (2004). *Derecho informático.* México D.F.: McGraw Hill.

Turtón Ávila, W. H. (2011, p. 68). *Necesidad de incluir un medio de impugnación en la audiencia de ofrecimiento de prueba en el proceso penal guatemalteco.* Guatemala, Guatemala. (s.e).

Vásquez Rossi, J. A. (2001, p. 76). *El Derecho Procesal Penal. Conceptos generales.* Buenos Aires, Argentina: Rubinzal-Culzoni.

Vásquez, M. E. (2006, p. 45). *Violación a los principios de inocencia y debido proceso de los adolescentes en conflicto con la Ley Penal al ser juzgados y condenados por un mismo juez.* Guatemala. (s.e).

Velez Mariconde, A. (2006). *Derecho Procesal Penal.* Córdoba, Argentina: Marcos Lerner Editora Córdoba.

Vivant, M. (1986). *Derecho de la informatica.* París, Francia: Lamy.

WIPO. Obtenido de https://www.wipo.int/: https://www.wipo.int/edocs/pubdocs/es/intproperty/450/wipo_pub_450.pdf