ANALISIS JURIDICO Y MATERIAL DE LA EVIDENCIA DIGITAL EN LOS DELITOS INFORMATICOS JUDICIALIZADOS POR LA FISCALIA GENERAL DE LA NACION EN EL MUNICIPIO DE BUCARAMANGA EN EL PERIODO 2006-2010

PAULA ANDREA ALVAREZ DAVID

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLITICAS
BUCARAMANGA
2011

ANALISIS JURIDICO Y MATERIAL DE LA EVIDENCIA DIGITAL EN LOS DELITOS INFORMATICOS JUDICIALIZADOS POR LA FISCALIA GENERAL DE LA NACION EN EL MUNICIPIO DE BUCARAMANGA EN EL PERIODO 2006-2010

PAULA ANDREA ALVAREZ DAVID

TESIS

DIRECTOR
LUIS ALEJANDRO BECERRA
DOCENTE UNIVERSIDAD PONTIFICIA BOLIVARIANA
ABOGADO

CODIRECTOR
FERNANDO GARCIA BARAJAS
INGENIERO DE SISTEMAS

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLITICAS
BUCARAMANGA
2011

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga, Diciembre 09 de 2011

Este trabajo de grado está dedicado especialmente a mis padres quienes son la principal fuente enriquecedora de mi conocimiento, ellos con su esfuerzo lograron proporcionarme todos los medios necesarios para que me pudiera formar como una excelente profesional, llena de todas las capacidades para enfrentar la cotidianidad de la vida.

Gracias a la formación académica y personal que recibí en esta institución, puedo decir orgullosamente que soy una profesional que le aportara a la sociedad.

Agradezco de manera muy especial a mi director de tesis el doctor Luis Alejandro Becerra y al gran colaborador el doctor Luis Guillermo Rosso quienes fueron las personas que me guiaron durante todo el desarrollo de mi proyecto de grado, porque supieron trasmitirme de manera efectiva sus conocimientos tanto en el tema como en el proceder del proyecto, ellos lograron crear en mí una conciencia investigativa y una concepción del verdadero ser del profesional. Por otro lado agradezco al Doctor Fernando Barajas porque no solo me brindo toda tola información necesaria para complementar mi proyecto, sino que además fue el artífice de la idea de trabajar sobre la evidencia informática, para de este modo contribuir técnica y jurídicamente en el ámbito de los delitos informáticos.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: ANALISIS JURIDICO Y MATERIAL DE LA EVIDENCIA DIGITAL EN LOS DELITOS INFORMATICOS JUDICIALIZADOS POR LA FISCALIA GENERAL DE LA NACION EN EL MUNICIPIO DE BUCARAMANGA EN EL PERIODO 2006-2010

AUTOR(ES): PAULA ANDREA ALVAREZ DAVID

FACULTAD: Facultad de Derecho

DIRECTOR(A): LUIS ALEJANDRO BECERRA

RESUMEN

Esta propuesta de investigación servirá para poder identificar un marco general sobre la conceptualización básica necesaria relativa a los delitos informáticos, sus objetivos, importancia, sus principios, y la evidencia digital en lo que refiere a la necesidad de su existencia, su manejo jurídico y material, y la informática forense. Esto se hará en conjunto con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y aquellos que sin estar plasmados jurídicamente tiene incidencia en el manejo de evidencia digital durante la cadena de custodia y en el curso de un proceso penal. Se podrá conocer como ha sido la transformación de las tecnologías en herramientas para cometer ilícitos, los mecanismos y modalidades que utilizan los especialistas en la internet para vulnerar derechos protegidos constitucionalmente. De igual forma es importante saber el rol que tienen que desarrollar los investigadores judiciales para salvaguardar la prueba del delito informático y con ello conocer como existen en Latinoamérica diferentes legislaciones que han logrado enmarcar jurídicamente este tipo de procedimiento. Mediante el trabajo de campo conoceremos alternativas que permitirán mejorar el manejo de la administración de justicia en lo que refiere a delitos informáticos, habilitando y definiendo aspectos legales que contribuyan a la regulación y la tipificación del manejo de evidencia informática. Con ello podremos identificar cuáles son los retos legales o tecnológicos que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de pericia informática. Es primordial que se tenga claro porque de la pericia informática depende la eficacia de la prueba jurídicamente hablando y de esta la protección de derechos del sujeto pasivo de la comisión del delito.

PALABRAS CLAVES:

delitos informáticos informática forense ilícitos evidencia informática

V° B° DIRECTOR DE TRABAJO DE GRADO

GENERAL SUMMARY OF WORK OF GRADE

TITLE:	LEGAL ANALYSIS AND MATERIAL EVIDENCE DIGITAL COMPUTER CRIMES PROSECUTOR prosecuted BY GENERAL\'S OFFICE IN THE MUNICIPALITY OF BUCARAMANGA in 2006-2010
AUTHOR(S):	PAULA ANDREA ALVAREZ DAVID
FACULTY:	Facultad de Derecho
DIRECTOR:	LUIS ALEJANDRO BECERRA

ABSTRACT

This research proposal will serve to identify a general framework for conceptualizing necessary background on cybercrime, its objectives, importance, principles, and digital evidence as regards the necessity of its existence, its legal and material handling and computer forensics. This will be done in conjunction with existing regulations (laws) for the management of computer crime, by understanding the guidelines established in our law and those embodied legally without having an impact on the handling of digital evidence in the chain of custody and in the course of criminal proceedings. We will know as has been the transformation of technology tools to commit crimes, the mechanisms and modalities used by specialists on the Internet to violate constitutionally protected rights. Similarly it is important to know the role they have to develop judicial investigators to safeguard the evidence of computer crime and thus know how there are different laws in Latin America that have been legally framed this type of procedure. Through field work alternatives that will know better manage the administration of justice when it comes to cybercrime, enabling and defining legal issues that contribute to the regulation and criminalization of computer evidence handling. This can identify the legal and technological challenges that arise when managing a cyber crime before, during and after a process of computer expertise. It is essential to be clear because of computer expertise depends on the effectiveness of proof legally speaking, and thus the protection of rights of the taxpayer of the offense.

KEYWORDS:

illegal cybercrime computer forensics computer evidence

V° B° DIRECTOR OF GRADUATE WORK

INTRODUCCION

Esta propuesta de investigación servirá para poder identificar un marco general sobre la conceptualización básica necesaria relativa a los delitos informáticos, sus objetivos, importancia, sus principios, y la evidencia digital en lo que refiere a la necesidad de su existencia, su manejo jurídico y material, y la informática forense. Esto se hará en conjunto con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y aquellos que sin estar plasmados jurídicamente tiene incidencia en el manejo de evidencia digital durante la cadena de custodia y en el curso de un proceso penal.

Se podrá conocer como ha sido la transformación de las tecnologías en herramientas para cometer ilícitos, los mecanismos y modalidades que utilizan los especialistas en la internet para vulnerar derechos protegidos constitucionalmente.

De igual forma es importante saber el rol que tienen que desarrollar los investigadores judiciales para salvaguardar la prueba del delito informático y con ello conocer como existen en Latinoamérica diferentes legislaciones que han logrado enmarcar jurídicamente este tipo de procedimiento.

Mediante el trabajo de campo conoceremos alternativas que permitirán mejorar el manejo de la administración de justicia en lo que refiere a delitos informáticos, habilitando y definiendo aspectos legales que contribuyan a la regulación y la tipificación del manejo de evidencia informática. Con ello podremos identificar cuáles

son los retos legales o tecnológicos que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de pericia informática. Es primordial que se tenga claro porque de la pericia informática depende la eficacia de la prueba jurídicamente hablando y de esta la protección de derechos del sujeto pasivo de la comisión del delito.

La importancia de la evidencia digital recolectada, analizada y expuesta en un proceso penal va a tener a lo largo de la investigación mayor incidencia no solo por los actores que intervienen en la comisión del delito sino en todos los intervinientes y protectores de los derechos de la sociedad.

CONTENIDO

MARCO TEORICO

REFERENTE HISTORICO

La regulación Colombiana evidencia que la ley 527 de 1999 no fue la primera norma que trato lo concerniente a derecho y tecnología. Una labor de “arqueología jurídica” podría concluir que fue la ley 8 de 1970 la pionera en materia de autorizar en el articulo 7 al presidente de la república para, entre otras, adoptar medidas necesarias para generalizar el *uso del computador electrónico y los trámites administrativos relacionados con los impuestos nacionales y poner especial énfasis en el mejoramiento y organización de las oficinas de cobranzas y ejecuciones fiscales.*

Posterior a la ley 527, nuestro marco legal se vienen nutriendo de normas relacionadas con el mensaje de datos, firmas digitales, firmas electrónicas, entidades de certificación, tecnologías de información y comunicación, protección de datos personales, delitos informáticos, antecedentes disciplinarios y judiciales electrónicos, títulos valores electrónicos, teletrabajo, contratación electrónica, nombres de dominio, gobierno electrónico, factura electrónica, voto electrónico, y la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de Administración de justicia. Esto pone de presente no solo la inmersión masiva de lo “electrónico” en el sistema jurídico del país sino que cada día gran parte de los asuntos jurídicos cotidianos guardan relación con la amalgama derecho-tecnología.

La ley 527 de 1999 es producto de la labor de armonización que organismos internacionales han liderado con la finalidad de lograr a nivel mundial un consenso sobre fundamentos jurídicos mínimos para el desarrollo del comercio electrónico y el uso de los mensajes de datos como una nueva forma jurídica valida de manifestar la *voluntad* y como *medio de prueba.* la Organización de las Naciones Unidas (ONU), a través de la comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional (CNUDMI), publico en 1996 la ley modelo sobre el comercio electrónico, cuyos principales propósitos son los siguientes: 1). Ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan crear un marco jurídico en donde se admita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de comercio electrónico, y 2).conceder igualdad de trato tanto a los usuarios de mensajes consignados sobre un soporte informático como a los usuarios de la documentación consignada sobre el papel.

La precitada ley es una disposición cardinal en todo lo relacionado con el uso de los mensajes de datos como medio por el cual se manifiesta la voluntad y el soporte de documentos electrónicos. De allí surgieron equivalentes funcionales centrales para cualquier actividad y reglas atinentes a lo denominado evidencia digital o electrónica.

La ley 527 de 1999 constituye el marco jurídico integral y general que avala, salvo algunas excepciones, el uso de los mensajes de datos en todas las actividades de los sectores públicos y privados. Su importancia es indiscutible, sin perjuicio de que con anterioridad a ella existieran ya algunas normas sectoriales que trataban cuestiones

relacionadas con temas como la desmaterialización, la factura, la Administración de Justicia y los medios electrónicos entre otros.

Con la evolución de la ley penal colombiana fue posible tipificar conductas centrales de lo que se engloba bajo el término delitos informáticos. La ley 1273 de 2009 modifico el Código penal y estableció la protección de la información y de los datos como nuevo bien jurídico tutelado. Este plexo normativo tiene varias implicaciones:

En primer lugar, adiciona el artículo 58 para establecer como circunstancia de agravación el uso de medios informáticos, electrónicos o telemáticos en la realización de conductas punibles. Se trata de un reconocimiento a los efectos en masa, e ilimitados, que puede ocasionar el empleo de dichos medios en fines criminales. En segundo lugar, crea el titulo VII *bis,* denominado “De la protección de la información y de los datos”. Bajo dicho manto precisa y amplia el delito de acceso abusivo a un sistema informático, previsto en el artículo 195 de la ley 599 de 2000, el cual de manera explícita quedo derogado. En tercer lugar, retoma e incorpora una serie de términos en nuestra jerga jurídica, como “sistema informático”, “dato informático” y “sistemas de tratamiento de información”. Lamentablemente la ley no los define, lo cual podría generar problemas a la hora de sancionar, porque la tipificación no es precisa. Cabe recordar que en el artículo 10 del Código Penal exige que la conducta sea definida de manera inequívoca, expresa y clara, además de los elementos que se requiera de acuerdo a la naturaleza del tipo.

REFERENTE JURIDICO

Colombia ha implementado iniciativas que le permiten en diferentes espacios, establecer mecanismos que le puedan controlar los delitos relacionados con las tecnologías. En el campo jurídico, Colombia mantiene las siguientes leyes decretos y acuerdos, relacionados con la informática y la información.

AÑO	**LEY / DECRETO/ ACUERDO**	**ORDENANZA**
1985	Ley 57	Transparencia y Acceso a la Información Gubernamental
1999	Ley 527	Información en forma de mensaje de datos
2000	Decreto 1747	Entidades de Certificación, los Certificados y las Firmas Digitales
2000	Resolución 26930	Estándares para la autorización y funcionamiento de

		las entidades de certificación y sus auditores.
2001	Ley 679	Explotación, la Pornografía y el Turismo Sexual con Menores de Edad
2003	Decreto 2170	Certificación y Firmas Digitales
2004	Proyecto de Ley 154	Reglamento del Derecho a la Información
2006	Acuerdo PSAA06-3334	Reglamentación de medios electrónicos e informáticos en la justicia.
2009	Ley 1273	Ley de la protección de la información y de los datos

Nuestro país ha tenido un desarrollo particular con respecto a la investigación de delitos de índole informático, factores como el narcotráfico, lavado de activos, falsificación y terrorismo, han incentivado para que este país implemente unidades de investigación que le colabore al Estado en los procesos de indagación de actos ilícitos en los que se utilizan medios tecnológicos o que afectan sistemas de tecnología o de información.

La Ley 1273 aprobada en enero del 2009, crea un nuevo bien jurídico tutelado, el cual se denomina “protección de la información y de los datos”, en la sociedad colombiana, en se penalizan y sancionan los siguientes actos:

Atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos:

- ✓ Acceso abusivo a un sistema informático
- ✓ Obstaculización ilegítima de sistema informático o red de telecomunicaciones
- ✓ Interceptación de datos informáticos
- ✓ Daño informático

- ✓ Uso de software malicioso
- ✓ Violación de datos personales
- ✓ Suplantación de sitios web para capturar datos personales

Se puede observar que las sanciones establecidas para este tipo de conductas se orientan específicamente a preservar aspectos que se van ligados con la seguridad de la información en la que se trata de salvaguardar la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Colombia ha sido uno de los países que ha recibido ayuda por parte de los Estado Unidos para buscar la persecución efectiva de actos criminales, gracias a que su rama de investigación de naturaleza informática se originó a partir del año 1984 cuando los laboratorios del FBI y otras agencias que pertenecen a los Estados Unidos promovieron el desarrollo de programas para examinar evidencias computacionales, lo que ha cimentado las políticas anti-criminales en nuestra sociedad.

Existe un Grupo Investigativo de Delitos Informáticos (GRIDI) que investiga las conductas delictivas que se derivan del uso de la tecnología y las telecomunicaciones, éste organismo se sustenta con el apoyo de equipos de informática forense y personal profesional capacitado que atienden incidentes informáticos presentes durante una investigación judicial. Los grupos de investigación de delitos informáticos se encuentran

equipados con laboratorios de Cómputo Forense, en las ciudades de Bogotá, Medellín, Bucaramanga, Cali y Barranquilla, los cuales permiten un mejor el análisis de la información digital.

Los organismos oficiales han declarado que los delitos relacionados con la informática en Colombia han tenido un incremento significativo en el año 2007, ya que durante el transcurso del año 2006 se encausaron 433 procesos que corresponden a los delitos informáticos, las cifras oficiales brindadas por la DIJIN (Dirección Central de Policía Judicial), del mes de Enero a Septiembre del 2007, mencionan la denuncia de 630 casos, sin considerar aquellos que se llevan por la Fiscalía y el DAS (Departamento Administrativo de Seguridad), el trafico de bases de datos, fraude electrónico, falsificación o clonación de tarjetas, entre otros, han tenido un costo aproximado de 349 millones de pesos colombianos para las personas naturales y alrededor de 6.6 billones de pesos colombianos para las empresas.

El aumento de la delincuencia utilizando los sistemas de cómputo va en tendencia de aumento, por lo que se hace necesario analizar las herramientas necesarias en la legislación Colombiana para obtener el mejor procedimiento de manejo de evidencia en el delito informático y con ello las diferentes actividades especializadas que tiene que realizar los peritos forenses. En los capítulos siguientes podremos ver como no solo es imprescindible tener tipificadas todas las posibles conductas delictuales en la informática sino, como se protege efectivamente los derechos que la ley penal enmarca como fundamentales en todo proceso penal.

CAPITULO I

EL DELITO

Para poder comprender la temática del delito informático y específicamente la prueba o evidencia informática que de ello se deriva, tema que realmente nos compete, es de vital importancia hacer un retroceso o una reconstrucción de la llamada teoría del delito, ya que esta se convertirá en una herramienta necesaria que nos brindara una base sólida en lo que refiere al delito, desde la perspectiva del legislador y los doctrinantes.

"La teoría del delito se le llama a la parte de la ciencia del derecho penal que se ocupa de explicar que es delito en general, es decir, cuales son las características que debe tener cualquier delito, esto facilita la averiguación de la presencia o ausencia del delito en cada caso concreto" [1]. Este concepto es previo al Código penal puesto que le suministro al legislador un criterio político-criminal sobre lo que el mismo puede penar o dejar impune y con ello presupone la existencia de un derecho del Estado a penar. Con esto nació la necesidad de imponer sanciones, algunas veces un tanto drásticas, a aquellas conductas humanas que eran reprochables por la sociedad y que por ende contaminaban la vida armónica de los seres humanos.

El derecho penal se fue convirtiendo con el pasar del tiempo en una herramienta efectiva que el legislador empezó a utilizar para ponerle orden a la sociedad. El concepto de delito se define desde diferentes perspectivas, pero todas estas apuntan hacia un mismo horizonte, según Francesco Carneluti[2] "el delito es un producto de conflicto intersubjetivo de intereses, por esto el delito es un modo de ser de la sociedad, no del individuo", para Jackobs[3] "El delito es una comunicación defectuosa, una desautorización de la norma o falta de fidelidad a la misma. La norma es una

[1] ZAFFARRONI, Eugenio Raúl. Manual de derecho penal. México D.F: 4ed.1988.pag 333.
[2] CARNELUTTI, Francesco. El delito. Editorial Leyer. Bogotá D.C:2005. Pag8.
[3] JACKOBS, Gunther. Strafrechtt Allgeimeiner Teil, Berlin, 1983, pags. 34 y 36, citado por Velasquez.

expectativa social institucionalizada" para Carrara[4] es "una Infracción a la ley de un Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañosos" como estas, existen infinidad de definiciones que como se dijo anteriormente apuntan hacia un mismo fin, definir que es delito, el legislador buscando unanimidad de conceptos consagro en el Código penal los elementos estructurales del delito para que a partir de ellos se pueda concluir cuando se está en presencia de lo que la ley considera como delito.

El delito es una conducta del hombre que puede darse de forma positiva o negativa (activa u omisiva) sabemos por nuestro derecho penal que entre una infinita cantidad de conductas posibles de los seres humanos, solo algunas de estas son delitos. Para poder distinguir las conductas que son delito de las que no lo son, tenemos que acudir al Código penal, donde unos dispositivos legales describen las conductas prohibidas a las que se asocia una pena como consecuencia. Por lo tanto no habrá delito, cuando la conducta de un hombre no se adecue a alguno de esos dispositivos.

Técnicamente llamamos tipos a los elementos de la ley penal que sirven para individualizar la conducta que se prohíbe con relevancia penal. Cuando alguna de esas conductas humanas se adecue a lo preceptuado por el legislador, quiere decir que esa conducta es típica o que es lo mismo que decir que presenta la característica de tipicidad. De este modo hemos obtenido dos caracteres del delito: genérico uno (conducta) y especifico otro (tipicidad), es decir que la conducta típica es una especie del genero conducta.

No obstante, con la sola característica de tipicidad no se individualiza la especie delito, puesto que no toda conducta típica es delito, ya que existen dentro del derecho penal circunstancias en las que opera una justificación como exclusión del carácter delictivo de la conducta típica tales como la legítima defensa o el estado de necesidad y, en general, de supuestos de "legítimo ejercicio del derecho". "De esto resulta que a veces

[4] CARRARA, Francisco.

hay permiso para cometer conductas típicas, pero por el contrario cuando la conducta típica no está permitida o tiene causal de justificación delictiva diremos que, además de típica, será también contraria al orden jurídico funcionando como unidad armónica, porque de ninguno de sus preceptos surge un permiso para realizarla"[5]. A esta característica de contrariedad al orden jurídico, funcionando como conjunto armónico que se comprueba con ausencia de permisos la llamaremos antijurídica como segundo elemento para que se constituya el delito.

Pese a lo anterior si leemos el código penal podremos observar que hay supuestos de hecho de los que se deduce que no toda conducta típica y antijurídica es un delito, ya que menciona supuestos en que la conducta es claramente típica, por no existir un permiso para realizarla, y sin embargo no hay delito. En la doctrina este fenómeno tiene el nombre de *injusto penal* reconociendo que el injusto penal "no es un delito, sino que para serlo, ha de ser reprochable al autor en razón a que tuvo la posibilidad exigible de actuar de otra manera"[6],

De esta forma hemos podido construir el concepto del delito como una conducta típica, antijurídica y culpable. Estos tres conceptos o elementos característicos del delito son los que nos van a ayudar a detectar cuando se está en presencia de una conducta, que la ley penal podría sancionar, independientemente del manejo que de ello hagan los administradores de justicia. El significado que estos tres elementos tienen en la ley penal servirá para poder detectar cuando se está en presencia de un delito informático. El hecho de encontrarse tipificados en nuestra legislación penal significa que se están cumpliendo efectivamente los cometidos estatales en cuanto se siga velando por la protección de los bienes de las personas.

1.1.1 LA CONDUCTA

La conducta es un acto de voluntad de los seres humanos, que tiende a crear situaciones jurídicas en la sociedad. El legislador se ha visto en la necesidad de crear

[5] ZAFARRONI. Op. Cit., p. 335.
[6] http://www.elprisma.com/apuntes/derecho/escuelaspensamientopenal. Consultado el 24 Julio de de 2011.

un marco jurídico dentro del cual se encuentran reglas mínimas de comportamiento entre los seres humanos y con ellas las sanciones determinadas para las personas que infrinjan dichos mandatos. La garantía para la aplicación de dichas reglas de comportamiento tienen como base fundamental el principio de "*nullun crimen sine Legem"*[7] que le permite a la sociedad notar si existen arbitrariedades por parte de los administradores de justicia que, en algunos casos, aplican la ley de manera subjetiva y hacen justicia con su propia mano. "De rechazarse este principio, el delito podría ser cualquier cosa, abarcando la posibilidad de penalizar el pensamiento, la forma de ser, las características personales etc"[8].

De la conducta podemos decir que si bien es un comportamiento del hombre algunas veces natural y espontaneo otras veces no, tienen en común una finalidad un tanto previsible en algunos casos, en los cuales se hace necesario tener los medios para desarrollarla y con ello poder obtener un resultado. Ese resultado tiene como conducto un nexo de causalidad que es lo que lo entrelaza con la conducta. Muchos autores afirman que el nexo y el resultado no hacen parte de la acción (conducta) sino que la acompañan en forma inescindible, simplemente que estos tres elementos juntos alteran algo en el mundo exterior[9].

En el comportamiento humano, la conducta no se agota con el ejercicio activo del sujeto como se muestra anteriormente la acción, sino que también tiene un aspecto pasivo relevante, ya que el derecho penal, no contiene normas prohibitivas, sino que también, aunque en menor medida, normas imperativas que ordenan acciones cuya omisión puede producir resultados socialmente nocivos. Lo que el legislador castiga en estos eventos, es la no realización de la acción mandada. La *omisión* social y jurídicamente relevante referida siempre a una acción determinada, cuya no realización constituye ausencia. "De aquí se desprende que el sujeto autor de la omisión debe estar en

[7] NULLUM CRIMEN SINE LEGEM." Nadie será condenado a menos que su conducta constituya un crimen" http://www.definicionlegal.com/definicionde/Nullumcrimensinelege.htm. Consultado el 20 de Octubre de 2011.

[8] CLAUS, Roxin. Derecho penal general. La estructura de la teoría del delito. Editorial Civitas.2ed.España.2003.p .275.

[9] ZAFFARONI. Op. Cit., p. 338.

condiciones de realizar la acción, porque de no ser así existiría la posibilidad de que no pueda hablarse de dicha omisión. De todas las acciones posibles que un sujeto pueda realizar, al ordenamiento jurídico penal, solo le interesa aquella que espera que el sujeto haga (auxiliar, socorrer, impedir que se cometa un delito, etc.)"[10].

"Una elemental prueba sistemática de la validez del concepto de conducta, consiste en comprobar que la acción sirve de base a todas las formas que los tipos adoptan para individualizar sus prohibiciones, es decir, que siempre los tipos prohíben conductas respetando la estructura del ser de la conducta"[11].

De principales clasificaciones estructurales de los tipos penales se distingue tipos dolosos y culposos, activos u omisivos en donde la conducta del sujeto se califica dependiendo la finalidad, los medios para llevar a cabo la conducta o el hecho de no realizar un algo debido[12].

1.1.2 LA TIPICIDAD

La tipicidad se derivada de la conducta, por esto se hace necesario evaluar cual es la dimensión que tiene la adecuación de esa conducta en la ley penal.

"Ninguna hecho por antijurídico o culpable puede ser considerado como delito si este no corresponde a una descripción contenida en una norma penal, con ello el legislador hizo una clasificación y tipifico aquellos actos más intolerables y lesivos para los bienes jurídicos más importantes, para amenazarlos con una pena"[13]. Esto no quiere decir que en el ordenamiento jurídico se encuentren reglamentados hasta los mínimos detalles de las conductas humanas, simplemente que la diversidad de formas de aparición que adoptan los comportamientos delictivos impone la búsqueda de una imagen conceptual lo suficientemente abstracta para poder englobar en ella todos aquellos

[10] MUÑOZ CONDE, Francisco. Teoría general del delito. Bogotá D.C:2ed.2008. pag. 5.

[11] CLAUS. Op. Cit., p. 229.
[12] ZAFFARONI. Op. Cit., p. 338.
[13] MUÑOZ. . Op. Cit., p.10.

comportamientos que tengan características esenciales comunes. Esta figura puramente conceptual es el *Tipo*.

Dentro de la teoría de la tipicidad es imprescindible esclarecer algunos aspectos que se encuentran en la legislación colombiana, para utilizarlos como base en el entendimiento de la teoría del delito.

Encontramos *que El tipo* que es un instrumento legal, lógicamente necesario y de naturaleza predominante descriptiva, que tiene por función la individualización de las conductas humanas.[14] Se dice que es un instrumento legal, pues el tipo pertenece al texto legal donde se encuentran sus diferentes especies es, pues, un dispositivo plasmado en la ley. Dispositivo que en lo que nos compete y en materia penal se hace necesario para poder determinar la presencia de un delito realizado por medio informático, ya que los elementos que el legislador plasma como constitutivos de los mismos son los que antes de que se pueda iniciar un proceso penal, cuando se encuentre en la fase investigativa podrá arrojar información acerca de que se está en presencia del tipo penal.

Además se dice que es un predominantemente descriptivo, porque a la hora de consignar las conductas el legislador suele acudir a descripciones valiéndose de figuras lingüísticas apropiadas, o elementos descriptivos como “matar”, “falsificar”, “cosa”, “vehículo automotor”, etc, los cuales se perciben mediante los órganos de los sentidos normalmente, y en otras oportunidades utiliza expresiones que se remiten o sustentan en gran medida en juicios de valor de carácter jurídico, como sucede cuando usa expresiones como “matrimonio valido”, “arbitrariamente”, consideradas a veces como elementos de la antijuricidad “ajena”, “documento”, “empleado público”, “documento público”, u otras de contenido extra jurídico como sucede con las “imputaciones deshonrosas” o “persona honesta”,[15] todo esto con el fin de darle especificidad a la conducta.

[14] ZAFARRONI. Op. Cit., p.340.
[15] VASQUEZ, Fernando. Manual de derecho penal. Bogotá D.C: 2002. P. 206

El tipo penal busca individualizar las conductas humanas penalmente prohibidas o mandadas, porque él es el encargado de otorgar relevancia penal a los diversos comportamientos valorados de manera negativa por el legislador, se busca con esta jerga jurídica es la taxatividad de las conductas en la norma, lo que en ultimas le agrega el legislador son palabras que condicionan el actuar de las personas, enmarcando dichas conductas en un cuadro de requisitos que de cumplirse se estaría dando el primer requisito para concretar el Delito.

Lo que se realiza con los parámetro anteriores es el llamado *juicio de tipicidad* se trata, en otras palabras, de la operación mental llevada a cabo por el juez, mediante la cual se constata o se verifica la concordancia entre el comportamiento estudiado y el texto legal[16].

Se ha advertido que se trata de un concepto dinámico y funcional en la medida en que se presupone la existencia de una conducta ajustada al tipo, subsumible en el, o ligada a el por un nexo de dependencia temporal o personal[17]. En otras palabras, la tipicidad es la resultante afirmativa del juicio de tipicidad.

Ahora bien, si realizada esta última operación mental acontece que el producto de la misma es negativo, pues la acción examinada no encaja, no coincide con los caracteres imaginados por el legislador en el tipo concreto, incluso acudiendo a ciertos mecanismo que amplían el radio de acción de este los llamados amplificadores del tipo penal, se dirá que no hay adecuación típica, esto es, se tratara de un evento de *atipicidad.* Como puede verse los conceptos de tipicidad y atipicidad son correlativos y están uno en función del otro.

[16] Ibid., p. 210.
[17] CLAUS. Op. Cit., p. 283.

Funciones del tipo penal

Es lugar común por parte de la doctrina hablar de los cometidos, de las tareas o funciones, del tipo penal; no obstante, se habla de 3 principales funciones que son las que tienen inmersa la finalidad del derecho penal:

En primer lugar, el tipo cumple una función *garantizadora,* pues es la expresión del principio de legalidad del cual emanan garantías de índole subjetiva, procesal y de ejecución penal, la cual es pieza fundamental a la hora de imputarle una o varias conductas típicas al sujeto activo del tipo penal. En segundo lugar, se postula que el tipo tiene una función *fundamentadora* pues es el presupuesto de la ilicitud, ya que es debido que se dé la condición de contrariedad con el ordenamiento jurídico establecido para el momento de la realización del hecho. La última función que se le asigna es una función *sistematizadora* ya que con esta teoría no solo ha sido posible tender un puente de unión entre la parte general y especial del Código Penal, sino al mismo tiempo realizar un estudio sistemático de las diversas figuras delictivas a partir de sus características peculiares[18].

A continuación se examinara como hace presencia la tipicidad en las diferentes formas del tipo como lo propone el doctor Muñoz Conde[19]:

*El tipo en los hechos dolosos de comisión
*El tipo en los hechos culposos de comisión
*El tipo en las figuras de carácter especial
*El tipo en los hechos omisivos dolosos
*El tipo en los hechos omisivos culposos

Aspectos objetivos- el aspecto objetivo de estos tipos consiste en verificar su estructura, sus componentes descriptivos, con ellos los elementos de todo tipo que vendrían siendo la acción, el nexo de causalidad y el resultado en los tipos que así lo requieran.

[18] MUÑOZ. Op. cit., p. 12.
[19] Ibid., p. 12.

Por otro lado la aparición de los sujetos de la acción que vendrían siendo el sujeto activo y el sujeto pasivo, o el bien jurídico tutelado por la legislación penal.

Aspectos subjetivos- sus componentes fundamentales son el *dolo* y la *culpa,* estos dos elementos con el debido estudio pueden ser detectados fácilmente en las descripciones típicas. El dolo por su parte tiene dos componentes de suma importancia uno de ellos el elemento cognoscitivo, el cual comprende no solo el conocimiento de las circunstancias del hecho, sino la previsión del desarrollo del sucesivo mismo incluida la causalidad y el resultado. Por otro lado encontramos el elemento volitivo el cual no solo basta con el conocimiento previo de las exigencias necesarias de la descripción legal, es indispensable que el agente se dedique a realizar la conducta tipificada, por ello se exige un segundo momento en el dolo, denominado voluntario, un querer, como dice la ley.

La culpa se presenta como una actuación que produce un resultado lesivo que es realizada por parte del sujeto agente que, siendo un hecho previsible, violo el deber de cuidado de modo determinante para la producción de un daño[20]. En los hechos omisivos ya sean de tipo doloso o culposo la conducta del sujeto consiste en la no realización del deber que la ley le impone a las personas en debidas circunstancias, lo que produce la incursión en alguno de los tipos penales por ese hecho omisivo, teniendo en cuenta que existe dentro de nuestra legislación atenuantes que le permiten excluir su responsabilidad o disminuir una pena.

Dentro de los tipos especiales encontramos los llamados “preterintencionales” que se presentan cuando el agente dirige su voluntad de causación hacia determinado resultado, produciéndose uno más grave que el que estaba, por lo menos, en capacidad de prever como lo decía el más grande penalista de habla hispana Jiménez De Asúa “un resultado que excede de nuestra voluntad, que traspasa la intención que tuvimos al emprender nuestro acto”.

[20]CLAUS. Op. Cit., p. 290.

Pero como se dijo en un aparte anterior no solo es necesario que la conducta realizada por un sujeto sea contraria a ley, es necesario que se perjudique a otro sujeto, al cual se le lesionan derechos respaldados por las legislaciones y que efectivamente cause un deterioro grave e injustificado a su derecho o a su patrimonio. Esta descripción en derecho penal es llamada Antijuricidad, dicha figura jurídica viene a ser pieza fundamental para poder detectar la presencia de un delito informático, como lo explicábamos anteriormente no solo la conducta del sujeto agente basta para encausar dicha actividad como ilícita, sino que además de esto se necesita la lesión a un bien jurídico tutelado por el estado para poder condenar o imponer sanciones a la persona que la realice, en este caso la protección a la información y a los datos obtenida violando el derecho a la intimidad.

1.1.3 LA ANTIJURICIDAD

Por antijuricidad podemos entender aquella conducta típica que lesiona o pone en peligro, sin derecho alguno, el interés jurídicamente tutelado en el tipo penal.

La figura de la antijuricidad tiene diferentes funciones conceptuales: *la antijuricidad formal y materia*l. Von Liszt (1899) [21]partiendo de su concepción positiva sociológica que todavía hoy deja sentir su influjo, habla de la antijuricidad formal entendida como la contravención de la norma estatal, de un mandato o de una prohibición del orden jurídico, de una parte y, de la otra, de la antijuricidad material concebida como la acción socialmente dañosa, antisocial o asocial o mejor, como el *peligro* para los bienes jurídicos. Son necesarios al momento de estructurar el delito dentro del cual incurrió el sujeto agente, ya que es requisito *sine quanun* que esa acción no solo sea contraria a ley sino que efectivamente afecte el bien que puede representarse de diferentes formas en la vida cotidiana; en el delito de homicidio el bien jurídico seria “la vida”, en el “hurto” seria el bien mueble sacado de la esfera del titular del derecho de propiedad, en las

[21] VON LISZT, Franz. La teoría final del derecho penal. 1881. Pag 138. Citado por Muñoz Conde en la Teoría General del Delito.

“lesiones personales” la integridad física, y así sucesivamente se pueden encontrar de la estructura el tipo, el bien frente al cual el legislador le otorga una protección especial.

Aspectos negativos de la antijuricidad

Existe dentro de la antijuricidad aspectos negativos tipificados como causales de justificación de la conducta, por lo tanto quien realiza una conducta típica justificada no comete, en primer lugar un hecho punible, pues al no haber antijuricidad mal puede predicarse la existencia de culpabilidad. Dentro de las causales de justificación encontramos[22]:

*El estado de necesidad justificante
*La legítima defensa
*El ejercicio del cargo y de derechos de coacción; la autorización de la autoridad
*Riesgo permitido[23]

Todos los anteriores criterios tienen una estructura particular, que, de darse cabida a alguno estaría en presencia de una causal de justificación que produciría un eximente en la responsabilidad del sujeto. Si hablamos dentro del entorno del delito informático esta causal vendría a ser demostrada cuando se esté en presencia de un proceso penal, en donde el juez determinara si efectivamente existió un eximente de responsabilidad en la conducta realizada.

1.1.4 CULPABILIDAD

Para terminar la exposición de los componentes de la teoría del delito debe estudiarse el elemento de la *culpabilidad,* la doctrina actual se muestra más preocupada por darle a este estrato del hecho punible un contenido preciso, por ello se insiste en una

[22] CLAUS. Op. Cit., p.788.
[23] Ibid., p. 788.

clasificación que se fundamenta en las elaboraciones del positivismo sociológico de finales del siglo XIX, en virtud de la cual sebe distinguirse entre los aspectos *formal y material* de las diversas categorías delictuales. El concepto formal comprende todos aquellos presupuestos que, en un ordenamiento jurídico dado, son indispensables para formular al agente la imputación subjetiva, mientras que el material busca desentrañar el contenido, el porqué de esa imputación. No basta con decir que la culpabilidad es un juicio de reproche, sino que es indispensable indagar por los presupuestos del contenido de los cuales depende esa reprochabilidad[24].

Así las cosas, Zaffaroni[25] entiende por culpabilidad o responsabilidad plena, el juicio de exigibilidad en virtud del cual se le imputa al agente la realización de un injusto penal (desvalor de la acción y desvalor del resultado), pues, dadas las condiciones de orden personal y social imperantes en el medio donde actúa, se encontraba en posibilidad de dirigir su comportamiento acorde con los requerimientos del orden jurídico y no lo hizo, habiendo podido llevar a cabo. Se trata de hacer un juicio de carácter eminentemente normativo fundado en la exigibilidad, idea que preside toda la concepción de la culpabilidad y en virtud de la cual el agente debe responder por su comportamiento.

Aspectos negativos de la culpabilidad

Dentro de los presupuestos sobres los cuales descansa el juicio de culpabilidad se encuentran los contenidos en el artículo 31 del código penal[26] la capacidad de comprender la ilicitud del acto y de auto determinarse de acuerdo a esa comprensión, por lo cual, si falta cualquiera de ellos, o ambos al mismo tiempo, no se puede emitir en contra del agente ningún juicio de responsabilidad penal, en otras palabras: *es culpable quien tiene la posibilidad de comprender las exigencias normativas y de conducirse o motivarse de acuerdo con dichos dictados* .Esto significa a contrario sensu, que no es culpable o responsables quien, dadas las circunstancias de orden personal y social

[24] MUÑOZ. Op.cit., p. 16
[25] ZAFFARONI. Op. Cit., p.421.
[26] CODIGO PENAL COLOMBIANO. Editorial Leyer. Bogotá D.C:2010. P. 42.

concretas en las que realiza el injusto (conducta típica y antijurídica), se encuentra en imposibilidad de decidirse conforme a las exigencias de derecho.

Conforme a lo anterior, el aspecto negativo del juicio de exigibilidad de traduce en el análisis concreto de los eventos que inhiben al Estado, por intermedio del órgano jurisdiccional competente, para imputar a la persona responsabilidad penal. Por ello se estudia en primer lugar, el *error de prohibición,* que se presenta cuando el autor del injusto no ha tenido la posibilidad de comprender el carácter ilícito del mismo; en segundo lugar, los casos de *estado de necesidad,* en los cuales el autor no puede determinarse de acuerdo con las exigencias normativas; y en tercer lugar los eventos de *inimputabilidad* en los cuales, por obra y efecto de los fenómenos del trastorno mental o de inmadurez psicológica, la persona no puede comprender el carácter ilícito de su actuar y/o determinarse de acuerdo con dicha comprensión[27].

Lo común en estas tres situaciones, es que al agente no se le puede exigir un comportamiento distinto al que ha realizado y el ordenamiento penal, en desarrollo del canon universalmente reconocido según el cual a lo imposible nadie está obligado, se hace eco de ello dando cabida a la inculpabilidad. Esto siempre y cuando por parte del juez se haya hecho un examen exhaustivo de la conducta realizada por el agente ya que no solo basta alegar la inimputabilidad o los demás casos en los que se excluye ya responsabilidad, basta decir que es necesario probarlos.

1.2 DISPOSITIVOS AMPLIFICADORES DEL TIPO

1.2.1 COPARTICIPACIÓN

Si el tipo penal comprende la descripción de una conducta humana con todos los ingredientes que permiten darle a esa conducta el calificativo de consumada, y la experiencia, sin embargo nos enseña que no siempre el individuo logra realizar lo que

[27] VASQUEZ, Op.cit., p. 201.

se propone, que muchas veces se queda en la mitad del camino, y por otra parte también sucede que la acción humana tipificada en el código penal con sujeto activo singular, puede ser realizada por varias personas o con la ayuda o contribución de otras desbordando así el marco típico, en estas dos hipótesis se hace necesario unos mecanismos amplificadores del tipo, ya que, en estas dos hipótesis, este ordenamiento sería impotente para aplicar la sanción criminal, ya que no cabrían en ninguno de los tipos plasmados en ella.[28]

El tipo penal está escrito en términos de un autor único, en singular; "el que", "el funcionario público", pero la realidad jurídica es que en un delito pueden participar varios sujetos activos o plural como lo explicábamos anteriormente. Esto se denomina coparticipación, tal es el caso de algunos tipos con sujeto activo compuesto, en el que un solo sujeto no puede cometer el ilícito, como en la asonada, la rebelión, conspiración, el concierto para delinquir o en delitos donde pueden participar varios sujetos en la comisión del mismo, aunque también puede ser uno solo el que lo cometa. "La realidad fáctica nos muestra que cuando se comete un ilícito siempre participan varias personas"[29]. Ahora ya son pocas las modalidades delictivas cometidos por sujeto único, sobre todo en los delitos contra el patrimonio, en los delitos contra la vida que usualmente son el resultado de un delito previo contra el patrimonio, entratandose de delincuencia común, también participan varios sujetos.

La modalidad del delincuente que desarrolla su acción por sí y para sí, está desaparecida, ahora lo común es la conformación de bandas o grupos o por lo menos pares para delinquir, pues ello garantiza protección y seguridad para cada uno de los integrantes del grupo o banda y por demás la distribución funcional del trabajo delictivo, o por especialidades, garantiza eficacia en el desarrollo del ilícito y la obtención de un resultado querido.

[28] http://jbpenalgeneral.blogspot.com/2011/01/14-dispositivos-amplificadores-del-tipo.html. Consulto el 05 de Julio de 2011.
[29] ZAFARRONI. Op.cit., p. 432.

Los delincuentes se han especializado y formado empresas criminales donde la improvisación es un factor superado. La tecnología está siendo parte importante de su logística, la Internet, los sistemas, las más avanzadas técnicas, artefactos mecánicos y electrónicos y sofisticados procedimientos son utilizados con maléficos propósitos. Son los autores del ilícito los sujetos activos. Son los seres humanos que realizan la conducta punible, ellos despliegan la acción, el comportamiento, la conducta típica y suelen tomar parte criminosa distintos sujetos y por ello es importante diferenciar los grados de responsabilidad penal en base a las aportaciones que realice cada uno de ellos, de tal forma que habrá sujetos que recibirán la totalidad de la pena amenazada, otros que al realizar contribuciones secundarias estarán más alejados de los aspectos fundamentales del delito y, por tanto, podrían llegar a recibir una pena menor y, por ultimo sujetos cuya responsabilidad penal es totalmente inexistente[30].

1.2.1 LA TENTATIVA

No siempre el delito se agota en el resultado a veces va más allá, como en el caso de algunos delitos contra el patrimonio, donde luego del resultado viene el aseguramiento de lo hurtado[31]. En otros casos, el delito no va más allá de su inicio de ejecución o no termina su ejecución aunque avanza mucho en ella o simplemente aunque termine su ejecución, el resultado queda incompleto o no se logra. En estos casos el delito está incompleto y se le denomina en la doctrina internacional como delito tentado.

El tipo penal está estructurado de manera hipotética como un delito en el que el resultado es parte del tipo y por ello es que se aplica una pena. El delito acabado es la generalidad en el derecho penal especial, pero en la realidad fáctica, una acción puede ser iniciada y no concluida en el resultado querido y aun así, pone en inminente peligro

[30] http://www.robertexto.com/archivo/penal_uribe_amplif_tipo.htm. consultado el 20 de Octubre de 2011.
[31] CLAUS. Op. Cit., p. 788.

el bien jurídico tutelado[32]. El logro del resultado querido depende única y exclusivamente de la destreza del sujeto activo para planearlo, seguirlo en su ejecución y dominarlo hasta el resultado, lo anterior incluye la idoneidad de medios y el conocimiento necesario sobre las circunstancias de tiempo modo y lugar en que deba desatar el plan trazado, es el conocimiento y aprovechamiento de la oportunidad. Si una voluntad o circunstancia externa impide el desarrollo total de la acción o el logro del resultado, es o porque el sujeto activo no valoro correctamente la acción a realizar ni trabajo acertadamente sobre la valoración del riesgo propio y el colateral.

Un *iter crimini*[33]*s* debidamente concebido desde su origen y en todos sus detalles, aun en las situaciones más extremas, no debe fallar. Aunque la doctrina y la jurisprudencia se ha dedicado a darle categorías a la Tentativa, finalmente esto no es lo más importante, si un delito se inicia y no logra su resultado, poco importa si es mucha o poca la proximidad o inmediatez de los actos ejecutados a la realización del delito, el peligro del bien jurídico de todas maneras existe. La mera inducción no aceptada, o no cumplida, al igual que todo acto preparatorio que no vulnere ni ponga en peligro bien jurídico alguno, queda por fuera de la punibilidad. Es posible que la ley establezca tipos penales para punir ciertas conductas que se pueden realizar en los actos preparatorios de un delito en concreto, pero estos actos en sí, ya son delitos y nunca dejaran paso a que se configure una tentativa.

El derecho penal exige la confluencia de un doble desvalor: el de acción y el de resultado, los que por demás, deben aparecer estrechamente unidos[34]. Pero es posible que el delito no asuma una forma perfecta de ejecución y no alcance a causar el daño o lesionar el bien jurídico, entonces es necesario que el estado haya previsto esta posibilidad y mediante criterios político-criminales se resuelva por su ataque y control, tenemos entonces el desvalor de acción aunque no se haya causado efectivamente el del resultado pero sí hay inminencia potencial de que llegue a causarse.

[32] http://www.robertexto.com/archivo/penal_uribe_amplif_tipo.htm. consultado el 12 de Marzo de 2011.
[33] http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/seis.htm. Consultado el 12 de marzo de 2011.
[34] CLAUS. Op.cit., p. 788.

Como forma perfecta de ejecución, solo está la consumación. Son formas imperfectas aquellas en que el autor no llega a realizar "*perfectamente*" la conducta descrita en el supuesto de hecho típico, pese a intentarlo. Si la ejecución obedece a un plan perfecto, entonces la ejecución será perfecta y estaremos ante la *consumación* del delito.

Este asunto es importante en el tratamiento de los delitos de peligro, cuya consumación no exige siquiera la lesión del bien jurídico, por mucho que quizá sea este el interés ultimo del autor. El delito de incendio se causa (consuma) con la sola puesta en peligro del bien jurídico, sin importar si efectivamente el bien jurídico sufre un daño efectivo, pues en este caso ese último daño, el legislador no lo exige, en los delitos informáticos si es necesaria por el contrario la consumación del hecho, esto es, a manera de ejemplo haber realizado un hurto por medio informático en cuentas bancarias, no basta el supuesto que el sujeto agente haya intentado obtener los dineros sino que efectivamente los haya sacado de la cuenta, ya sea a manera de transferencia electrónica, o con otro medio informático utilizado para obtenerla.

La consumación entonces, no depende tanto del proyecto criminal del sujeto como de los términos en los que el legislador ha plasmado la conducta en el tipo. Cuando el sujeto no logra entonces perfeccionar el delito, y se queda en el intento, el legislador anticipa la consumación, invadiendo el terreno de lo antijurídico tradicionalmente reservado para las formas perfectas, e impone una pena por el solo intento de delito.

Estos dispositivos amplificadores del delito fueron creados por el legislador a razón de la necesidad que fue surgiendo con la atipicidad, y el hecho de penar ciertas conductas reprochables realizadas por una pluralidad de personas o por hechos que al no llegar a su consumación no eran penados por la ley, a pesar de que visiblemente ponían en peligro bienes o derechos de los ciudadanos.

En ese orden de ideas recopilamos lo que es en ultimas es el delito, construyendo a partir de su teoría la forma cómo nació a la vida jurídica y como se ve reflejado en una sociedad que día a día lo exterioriza de diferentes formas.

3.1 DELITO INFORMATICO

El delito informático es una forma de exteriorización de las infinidades de conductas que el legislador consagra en el código penal como delito. Las heterogéneas actuaciones perjudiciales de ciertos agentes, han hecho que en Colombia se vaya desarrollando esta rama del derecho penal. A diferencia de otros países como Estados Unidos, Australia, Francia, nuestro país no ha desarrollado a profundidad el tema. Este avance se ha dado por la necesidad de tener armas suficientemente eficaces para combatir los ataques y daños que por medio de los sistemas de cómputo se podían realizar a las personas o hasta la misma Nación.

En la actualidad encontramos diversas definiciones del concepto de delito informático, pero para hacer un acercamiento global de esta definición, podemos decir que es una conducta típica, antijurídica y culpable que realiza un sujeto agente utilizando técnicas informáticas para extraer o destruir información de personas naturales o jurídicas.

El delito informático se encuentra consagrado en la ley 1273 de 2009[35] la cual se incluyó dentro del código penal Colombiano, debido a las necesidades urgentes de reglamentar este tema materia de estudio. Sin dejar de lado la gran historia y la incidencia que ha tenido este tipo de conductas ya tipificadas en el mundo. Esta ley creo la protección de otro bien jurídico como lo es la información y los datos, de esta manera se podrán preservar íntegramente los sistemas que utilicen tecnologías de la información y de las comunicaciones, de igual forma tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se informen jurídicamente para evitar incurrir en alguno de estos tipos penales.

Fue necesario llegar hasta este punto debido a que nuestro análisis jurídico y material de la evidencia informática, está basado netamente en el delito informático, ahora la pregunta será la siguiente ¿Cuál es la importancia que tiene la prueba o la evidencia

[35] Ley 1273 de 2009. Ptroteccion de información y de datos.

que se deriva de esos delitos informáticos? Y además de esto ¿será necesario que dicha prueba proveniente de un ilícito tenga que cumplir con ciertos requisitos procesales y sustanciales para que pueda ser valorado dentro de un proceso penal? Con esto nos referimos a si puede o no ser aceptada por el administrador de justicia.

La respuesta seguramente será afirmativa, si hacemos un comparativo con los requisitos que exigen la mayoría de pruebas en cualquiera de las ramas del derecho. Podemos traer a colación una teoría que fue desarrollada por el catedrático italiano el señor Luigi Ferrajoli quien desarrollo la teoría general del garantismo penal, y que será nuestro punto departida para desarrollar los interrogantes anteriormente planteados. Ferrajoli[36] dice que una constitución puede ser avanzadísima por los principios y los derechos que sanciona y, sin embargo, no pasar de ser un pedazo de papel si carece de técnicas coercitivas, es decir, de *garantías* que permitan el control y la neutralización del poder y del derecho ilegitimo, es por esto que el trata de hacer un análisis detenido de cómo el Estado protege efectivamente los derechos de los ciudadanos, ya que argumenta que la garantía de los derechos vitales de cada persona son condición indispensable para una convivencia pacífica.

Por lo anterior surge la necesidad no solo de que sean respetados todos los derechos que se han otorgado a través del tiempo a los ciudadanos, sino de que exista un ordenamiento jurídico completo tanto en el ámbito sustancial como en el ámbito procesal, de no existir este tipo de normatividades se daría lugar a que existieran lagunas jurídicas que traería como consecuencia la violación de derechos fundamentales otorgados a los seres humanos, llámese en un proceso penal el sujeto activo o el sujeto pasivo de u hecho punible. Laguna que posiblemente tuvo lugar con el nacimiento de un nuevo capítulo de la historia jurídica como lo son los delitos informáticos.

En Colombia el manejo probatorio dentro del proceso penal tuvo como base el Código de Procedimiento Civil al tiempo que en materia penal también se iba desarrollando el

[36] FERRAJOLI, Luigi. Derecho y razón. Teoría del garantismo penal. Editorial Trotta.7ed.p. 852-893.

tema de pruebas. Con el nacimiento de una nueva forma de cometer ilícitos como son los delitos informáticos, se creó la necesidad de reglamentar el manejo probatorio de la evidencia que se recolecta de estos hechos, si bien es conocido se maneja través de pericias que realiza los investigadores judiciales, que tienen creados ciertos parámetros para el manejo de la prueba, jurídicamente no encuentran refugio en una norma legalmente establecida para demostrarle a los jueces de la republica que efectivamente el material probatorio recolectado hace parte de un procedimiento efectivo y que por ende garantiza la protección de derechos que posiblemente fueron violados como resultado de una conducta reprochable al sujeto que la realizo.

Por esto en el capítulo siguiente entraremos a analizar todos los elementos que constituyen el tema de la prueba, para de esta forma poder examinar la incidencia que tiene en el delito informático en cuanto a su manejo y eficacia.

CAPITULO II

TEORIA DE LA PRUEBA

La noción de prueba aparece unida a todas las actividades de tipo social, puede afirmarse que es una necesidad que surge desde que el hombre vive en sociedad. En todas las ciencias reconstructivas, la prueba tiene una importancia fundamental, pues permite conocer el pasado, pero en el campo del derecho es vital para saber quien tiene la razón.

En el mundo del proceso civil como penal, la prueba es fundamental, esta se encuentra destinada a producirle certeza al juez, por lo tanto el reconstruye los hechos tal cual como se supone que ocurrieron y los subsume en la norma general y abstracta prevista por el legislador, para de esta forma darle aplicabilidad y concordancia con el caso en particular. Es necesario hablar de prueba judicial, para establecer un comparativo con la evidencia informática que se obtiene en este tipo de delitos, en este caso, la prueba va a recibir un tratamiento totalmente diferente a las pruebas que usualmente se utilizan en los demás procesos.

2.1 Prueba judicial

La prueba judicial es el acto o conjunto de actos destinados a la verificación científica (fáctica y reconstructiva) de la veracidad de los juicios jurídicos formulados sobre la ocurrencia de un delito y de su responsable, tiene un fin el cual es el de generar en el juzgador un convencimiento mas allá de toda duda razonable, sobre los presupuestos facticos de su decisión, cuyos artífices son el ministerio público, las partes e intervinientes en un proceso penal[37].

Para tener una noción de prueba penal lo más ajustada posible, es indispensable tener en cuenta las diferencias específicas, que, precisamente caracterizan las pruebas

[37] FLORIANAN, Eugenio. De las pruebas penales. Bogotá: Editorial Temis.2002.p 44-45.

penales frente a las judiciales. Así en razón con sus elementos se destacan los siguientes de la clasificación que hace el profesor.[38] Gustavo Cuello Iriarte:

a) Su objeto esta constituido por los juicios jurídicos que, como resultado de la labor de investigación y en el cumplimiento de la función de acusar, formula la Fiscalía General de la Nación, al presentar la acusación ante el juez competente.

b) La actividad probatoria está a cargo de las partes e intervinientes (la Fiscalía General de la Nación, la defensa, la víctima y su abogado) y del ministerio publico. El juez es el director del proceso y por ende de la actividad probatoria, pero le está vedado decretar pruebas de oficio, en atención al sistema acusatorio con excepción de los jueces de control de garantías, "…empero, el juez de control de garantías, en aras de garantizar la eficacia de los derechos materia del control judicial, si puede decretar y practicar pruebas de oficio cuando lo considere indispensable"[39]. Dice la sentencia citada:

"a juicio de esta sala, la prohibición contenida en el art 361 del Código de Procedimiento penal no es absoluta, en tanto que los jueces de control de garantías si pueden decretar y practicar pruebas de oficio en casos en que considere necesario……".

c) Los medios de pruebas, que hacen parte de los *medios de conocimiento* son los establecidos en el Código de Procedimiento Penal (prueba testimonial, prueba pericial, prueba documental y prueba de inspección) o cualquier otro medio técnico o científico que no viole el ordenamiento jurídico.

[38] CUELLO IRIARTE, Gustavo.Derecho probatorio y pruebas penales. Editorial Legis.2008.p

[39] SENTENCIA C-396/2007 Corte constitucional, Magistrado Ponente: Marco Gerardo Monroy Cabra.

2.1.1 PRINCIPIOS DE LA PRUEBA APLICADOS A LOS DELITOS INFORMATICOS.

Por otro lado el profesor Jairo Parra Quijano[40], hace una enumeración interesante sobre los principios generales de la prueba que son los que les ayudan a los administradores de justicia a descubrir si verdaderamente el elemento material probatorio puede alcanzar la suficiente certeza para ser tenido en cuenta dentro de un proceso penal. En ellos encontramos:

1. **PRINCIPIO DE LA VERACIDAD**

   Si en el proceso debe reconstruirse o hacerse una vivencia de cómo ocurrieron los hechos, para sobre ellos edificar la sentencia, las pruebas deben estar exentas de malicia, o falsedad. Cuando los testigos comparecen, a un proceso, están obligados a decir la verdad, a no deformarla.

2. **PRINCIPIO DE LA LIBRE APRECIACION**

   La convicción del juez debe haberse formado libremente, teniendo en cuenta los hechos aportados al proceso por los medios probatorios y de acuerdo con las reglas de la sana critica, de ahí que cumplan todas las reglas establecidas en la ley, para que se pueda hablar de formación libre del convencimiento

3. **PRINCIPIO DE LA UNIDAD DE LA PRUEBA**

   Cuando se regla que el juez expondrá razonadamente el merito que le asigne a cada prueba, no cabe duda que se consagra el método analítico, el estudio individualizado de cada medio probatorio, las diferencias que se hacen y las reglas de la experiencia que se aplican. Este medio de prueba explicado en la

[40] PARRA QUIJANO, Jairo. Tratado de la prueba judicial. Tomo I. Bogotá, librería del profesional, 5ed, 1996. P35.

sentencia muestra al justiciable y a la sociedad la manera ponderada y cuidadosa como el funcionario estudia las pruebas. Permite de igual forma observar que medio de prueba fue mal evaluado, para poder utilizar los recursos. La valoración conjunta viene después del estudio individualizado de cada medio o elemento probatorio.

"En materia penal el encartado tiene virtual y realmente a su favor la presunción de inocencia y ella obliga, en todo momento que se haga la valoración de la prueba a un estudio analítico de cada medio en particular y, una vez hecho, se razone sobre la influencia que cada una ejerce en la conclusión a que se ha llegado".[41]

4. PRINCIPIO DE IGUALDAD

La oportunidad para conocer la investigación penal que se ha iniciado, debe ser inmediata, para los sujetos procesales. Si no se hace esa comunicación en el tiempo indicado se rompe la igualdad, y como sostiene Jaime Bernal Cuellar y Eduardo Montealegre[42]: "mientras (el Estado) que ejerce la plenitud de su poder investigativo, el imputado no participa en la aducción de medios probatorios que posteriormente se pueden usar en su contra".

Este principio tiende a lograr un equilibrio en el proceso, las partes tienen que tener igualdad de oportunidades para pedir y obtener que se les practiquen

[41] CUELLO IRIARTE. Op.,.cit.p36.
[42] BERNAL Cuellar Jaime y Montealegre Eduardo. El proceso penal. Universidad Externado de colombia,1995,pag44

pruebas y para contradecir las del contrario, pero y sobre todo un conocimiento de los hechos, que interesan en general a la investigación.

5. PRINCIPIO DE LA PUBLICIDAD

La prueba puede y debe ser conocida por cualquier persona ya que, proyectada en el proceso, tiene un carácter social, hace posible el juzgamiento de la persona en una forma adecuada y segura. Es posible, cumpliendo este principio, que terceras personas puedan reconstruir los hechos.

6. PRINCIPIO DE LA FORMALIDAD Y LEGITIMIDAD DE LA PRUEBA

La prueba debe ser aprehendida, para el proceso en forma valida, requiere el cumplimiento de formalidades de tiempo, modo y lugar y, además, su inmaculacion, exenta de vicios como error, fuerza o dolo.

En materia penal a diferencia que en el ámbito civil la prueba pese a que puede provenir de una autoridad competente como es la policía judicial, puede que no tenga valor probatorio alguno sino cumple con las exigencias establecidas en materia penal, como lo es cuando empieza la etapa de instrucción solo este cuerpo policial puede actuar si tiene orden expresa del fiscal, de no ser así esta prueba seria nula de pleno derecho y no se podría tener en cuenta en un proceso.

Es en este principio donde vale la pena anotar que dentro de las investigaciones que se adelantan en los delitos informáticos, la policía judicial llámese cualquier autoridad que sea competente para determinado caso, tiene que seguir los

lineamientos existentes si los hay, de forma estricta, puesto que ellos son en primera instancia quienes tienen contacto directo con la prueba, por lo tanto, no pueden dejar de ninguna manera que la evidencia recolectada pueda ser viciada.

7. PRINCIPIO DE LA LIBERTTAD DE LOS MEDIOS DE PRUEBA

En materia penal se ha afirmado que los medios de prueba deben estar taxativamente enumerados, por ello se ha dicho que las normas sobre las pruebas penales son normas de garantía, por lo cual toda su disciplina debería ser considerada como instrumento de defensa para el imputado. El medio de prueba, no es solamente un asunto procesal, sino también es una oportunidad de tutelar los derechos individuales constitucionalmente garantizados, frente al peligro de sus posibles violaciones.

8. PRINCIPIO DE LA SEPARACION DEL INVESTIGADOR Y DEL JUZGADOR

En penal el Estado que es el más interesado en saber que fue lo que realmente ocurrió, no lo sabe y por ello tiene una doble misión: averiguar dónde está la información e informarse.

En Colombia de conformidad con el artículo 250 de la Constitución Política de Colombia[43] el fiscal que investiga, en un momento dado se transforma en juez y valora la prueba para dictar o no medida de aseguramiento, esta doble función del fiscal, que dicho sin ambigüedades significa buscar y entender información y además valorarla, en ella se cometen muchos errores, estas mixturas no son buenas y se atenta contra el derecho a la contradicción, ya que se suponen pruebas y se le hace nido a subjetividades del funcionario. Es por eso que esa separación de poderes tiene que estar bien estructurada en la ley, para que no

[43] Constitución Política de Colombia. ed Legis. Bogotá; 2007. P.132.

haya lugar a ninguna violación de derechos fundamentales por el hecho de haber una mezcla de roles.

9. PRINCIPIO DE LICITUD DE LA PRUEBA

La prueba ilícita es la que se obtiene violando los derechos fundamentales de las personas. La violación se puede haber causado para lograr la fuente de la prueba o el medio probatorio. A diferencia de la prueba ilegal, que es aquella que se obtuvo con violación del procedimiento penal establecido.

La licitud en materia informática, viene conexa a las diferentes actividades que realiza la policía judicial, no basta con que efectivamente se recolecte la prueba dentro de un lugar o en elementos informáticos en los cual se tenga orden judicial para inspeccionar, la actividad de búsqueda y recolección es mucho más técnica que recoger un pedazo de tela o acordonar un lugar, para obtener algún indicio que sirva de prueba.

Cumpliendo con la función social encomendada por el legislador, estos principios forman parte estructural el acto probatorio. Esto se convertirá en una de las herramientas para el uso adecuado de los medios de prueba existentes en Colombia.

Los principios anteriormente expuestos son y serán la base de todo proceso, no solo el positivismo jurídico es la herramienta más útil para impartir justicia, se ha confirmado que el ajuste a la norma solo hace parte de un análisis necesario para aplicar la ley, por otro lado las leyes naturales de las cuales se derivan los principios son las que claramente nos podrán proporcionar la verdad de los hechos.

2.1.2 ELEMENTOS DEL ACTO PROBATORIO

Existen elementos en el acto probatorio que determinan que personas están facultadas para aportar pruebas en un proceso o hacer efectivo su derecho de contradicción, así como el tema objeto de debate y que por ello hace necesario el surgimiento de la

prueba. Además de esto también a ayudan a encajar la conducta típica, antijurídica y culpable en la ley penal. Estos elementos son[44]:

SUJETO. En el acto probatorio suelen distinguirse varios sujetos de acuerdo con el papel que cumplan:

- El sujeto proponente: Es el sujeto que está facultado para pedir pruebas, esto es las partes
- El sujeto destinatario: se refiere al sujeto al cual está dirigida la prueba, esto es al juez quien es el encargado de verificar su grado de credibilidad y establecer si obtiene con ella certeza de los hechos.
- El sujeto contradictor: atañe a quien le corresponde controvertir la prueba y recae en la opositora de quien la propuso.

OBJETO. Se entiende por objeto de la prueba todo lo que es susceptible de probarse y demostrarse en el proceso jurisdiccional.

ACTIVIDAD. Puede concebirse como el conjunto de actuaciones realizadas para incorporar al proceso los hechos objeto de prueba. De acuerdo al medio probatorio que pueda utilizarse suele clasificarse en libre o legal.[45]

- Libre: es cuando el correspondiente ordenamiento enuncia algunos medios probatorios, pero permite el empleo de otros distintos de acuerdo con la evolución que se registre en ese campo.
- Legal: tiene ocurrencia cuando la disposición limita los medios probatorios a los que ella expresa o taxativamente indica.
- fuentes de la prueba en materia penal.

[44] CAMACHO, Azula. Manual de derecho procesal. Bogotá D.C: editorial Temis. P.14.
[45] Ibíd., p. 15.

2.2 FUENTES DE LA PRUEBA EN MATERIA PENAL

El ordenamiento ha introducido una denominación especial para las fuentes de la prueba, la cual es la de los elementos materiales probatorios, que se utiliza en muchas de sus disposiciones, precisamente en el artículo 275 del Código de Procedimiento Penal, hace una enunciación no taxativa de los mismos.

ART 275.-Elementos materiales probatorios y evidencia física

Para efectos de este código se entienden por elementos materiales probatorios y evidencia física los siguientes:

a. Huellas, rastros, manchas, residuos vestigiosos y similares, dejados por la ejecución de la actividad delictiva.

b. Armas, instrumentos, objetos y cualquier otro medio utilizado para la ejecución de la actividad delictiva.

c. Dinero, bienes y otros efectos provenientes de la ejecución de la actividad delictiva

d. Los materiales descubiertos, recogidos y asegurados en el desarrollo de la diligencia investigativa de registro y allanamiento, inspección corporal y registro personal.

e. Los documentos hallados en diligencia investigativa de inspección o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados allí.

f. Los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámara de vigilancia, en recinto cerrado o en espacio público.

g. El mensaje de datos, como el intercambio electrónico de datos, Internet, correo electrónico, telegrama, telex, telefax o similar regulados por la ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.

h. Los demás elementos descubiertos por el Fiscal General o por conducto de servidores de la policía judicial o el perito del instituto nacional de medicina legal o de laboratorios aceptados oficialmente.

Bajo el estricto rigor de la academia debe aceptarse que las expresiones elemento material probatorio y evidencia física son términos distintos. La relación de ellos es que uno y otro son utilizados por el fiscal en la etapa de la investigación y se constituyen en el soporte de la acusación, mientras que el juez trabaja con la prueba.

En el fallo del 19 de Noviembre de 2006, magistrado ponente: Sigifredo Espinosa Pérez puntualizo:[46]

" los elementos materiales probatorios y las evidencias físicas recaudadas en las etapas del proceso indagación e investigación, si bien sirven de soporte para imponer medidas de aseguramiento o medidas cautelares, o para restringir derechos fundamentales, no tiene efecto por sí mismos en el juzgamiento, es decir, no sirve para fundamentar una sentencia, pues esta, ha de estar soportada en las pruebas aducidas durante el juicio oral, de acuerdo con el principio de inmediación inserto en el artículo 379 de código de procedimiento penal que señala; el juez deberá tener como prueba únicamente las que hayan sido practicadas y controvertidas en su presencia"

[46] SENTENCIA 19 de Noviembre de 2006, magistrado ponente: Sigifredo Espinosa Pérez.

Los actos materiales probatorios obtenidos de la investigación, tienen la potencialidad de convertirse en prueba si son presentados ante el juez de conocimiento en el curso del juicio oral.[47] Como sucede en los delitos informáticos, los elementos recolectados como computadores, USB, teléfonos celulares en una escena donde posiblemente se cometió un delito de esta clase, son posiblemente elementos para potencialmente convertirse en pruebas, no por ello todo lo recolectado es objeto materia de prueba en un proceso, necesita además de ello la contradicción y la verificación.

2.2.1 NECESIDAD DE LA PRUEBA

Hablamos de necesidad de la prueba porque es pieza imprescindible en cualquier proceso penal para poder determinar, si se debe imputar a un sujeto una conducta típica, antijurídica y culpable. Esto parte del principio de presunción de inocencia del cual gozan todos los sujetos que están inmersos en un proceso penal, en los delitos informáticos que es el tema que nos atañe, y precisamente la eficacia del manejo probatorio de la evidencia que provenga del delito informático, la labor del Estado por conducto de su ente destinado a la investigación de este tipo de delitos, es mucho más ardua, ellos necesitan hacer un estudio minucioso de cada prueba allegada o aquellas que ellos mismos sustraen de la escena donde se cometió el delito.

En todos los países se ha vuelto indispensable adaptar las leyes vigentes a las nuevas concepciones técnicas y tecnológicas, con el fin de dar respuestas a las necesidades derivadas de la práctica jurídica y a las exigencias propias del mundo globalizado, en los asuntos comerciales, civiles, entre otros. Lo anterior tiene como objetivo principal que cada uno de los ordenamientos jurídicos posea la capacidad de regular cambios de sus sistemas económicos, sociales, permitiendo, con ello, que el propio derecho no se vuelva arcaico e ineficaz.

[47] CUELLO IRIARTE, Gustavo. Derecho probatorio y pruebas penales. Editorial Legis.2008.P

Es claro que tanto la internet como los medios electrónicos se han convertido en los instrumentos más rápidos para realizar negocios a nivel nacional e internacional, por cuanto a través de ellos se pueden perfeccionar y concretar transacciones en cuestión de segundos, transacciones que traen consigo efectos e implicaciones jurídicas. Las pruebas electrónicas de dichas transacciones, susceptibles de ser aportadas a un proceso determinado, pueden verse afectadas por una valoración deficiente por parte del juez. Esto cuando no existen criterios o requisitos jurídicos que guíen la actividad valorativa de la evidencia digital a nivel nacional e internacional, dejando tal acción al libre albedrío de la razón y de la sana critica. Estos dos criterios, si bien son útiles y suficientes en determinados casos, en el campo de la informática y, más específicamente, en lo referente a la evidencia digital, dada su especialidad, requieren una valoración más clara y detallada que cualquier otro medio probatorio.

Ahora bien, es necesario comprender el principio de la equivalencia funcional el cual tiene como finalidad adaptar y darle la misma fuerza probatoria de los documentos consignados en papel a los contenidos en formato de mensajes de datos, firmas electrónicas y demás conceptos tecnológicos. Lo que se pretende es cumplir con los mandatos estipulados por la ley, al incorporarle los requisitos de forma a los documentos electrónicos, como son *fiabilidad, inalterabilidad* y *rastreabilidad.* Es decir, "el principio en mención establece que un mensaje de datos que cumpla con la función de declaración o representación tendrá los mismos efectos jurídicos propios de los medios de prueba tradicionales"[48].

En conclusión, los documentos electrónicos o mensajes de datos están en la capacidad de brindar equivalentes grados de seguridad como los documentos consignados en un papel y en muchos casos, un mayor nivel de confiabilidad y rapidez. Para poder predicar un grado de seguridad confiable se deberá cumplir con los requisitos técnicos y

[48] CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá: Universidad de los Andes, 2010. 348p.

jurídicos plasmados en la ley, cuestión que se hace palpable en el derecho Colombiano con la llegada del principio de equivalencia funcional, pero no se encuentra de forma completa, puesto que en el ordenamiento jurídico no encontramos taxativamente una norma q indique cuales son los requisitos que tiene que reunir la prueba informática que busca ser aportada en un proceso penal y que de cumplir con estos pueda ser valorada efectivamente por el juez.

En preciso decir que la ley 527 de 1999[49] surge como una norma interpretativa de la regulación actual, por cuanto los equivalentes funcionales que son esgrimidos en ella permiten una interpretación actualizada y acorde con las necesidades de la realidad tecnológica, adaptando las normatividades ya vigentes al mundo contemporáneo. Así las cosas, el mensaje de datos definido por la ley 527 como "la información generada, enviada, recibida, almacenada o comunicada por los medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el EDI, la Internet, el correo electrónico, el telegrama, el telex, o el telefax". Los requisitos de forma exigidos para las diversas actuaciones quedarán suplidos para la información consignada en mensaje de datos de la siguiente forma:

1. **Equivalencia funcional del escrito*:*** a pesar de que el escrito cumple un sinnúmero de funciones, la ley 527 considero que la más relevante es la de permitir el acceso de la información almacenada en el mensaje de datos con posterioridad a su creación. Lo anterior se deriva del artículo 6 de la ley en cuestión, el cual consagra:

   "cuando cualquier norma requiera que la información conste por escrito, ese requisito quedara satisfecho con un mensaje de datos, si la información que este contiene es accesible para su posterior consulta. Lo dispuesto en este articulo se aplicara tanto si el requisito establecido en cualquier norma constituye una

[49] Ley 527 de 1999. Ley de mensaje de datos

obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito"

2. **Equivalente funcional de la firma:** las funciones generales de la firma son las de identificar a alguien y vincular a esa persona con el contenido del documento. La legislación comercial define la firma como "…la expresión del nombre del suscriptor o de alguno de los elementos que la integren o de un signo o símbolo empleado como medio de identificación personal".[50] El equivalente de la firma manuscrita es la firma electrónica o la firma digital, aunque no son iguales, las dos son jurídicamente validas.

3. **Equivalente funcional del original*:*** a diferencia de los demás equivalentes, la función de este sufre una gran modificación, por cuanto el acceso a la información consignada en formato de mensaje de datos necesariamente implica realizar una copia de la información consignada en ella. Por tal motivo, el original se suple en los mensajes de datos siempre y cuando exista una garantía confiable de que la información almacenada se ha conservado íntegramente desde el momento de su creación de forma final. El artículo 8 de la ley 527 es el encargado de regular la materia en los siguientes términos:

Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedara satisfecho con un mensaje de datos, si: **a)** Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se genero por primera vez en su forma definitiva, como mensaje de datos o en alguna forma; **b)** debe requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

[50] CÓDIGO DE COMERCIO. Ed. Legis. Bogotá; 2007. art 826. p. 131.

Esto es lo que efectivamente los investigadores judiciales tienen que realizar al momento de la recolección de información, ellos lo que usualmente hacen es guardar la información bajo un código que está conformado por letra y números que permite contrastar si efectivamente la evidencia que se recolecto es la misma que fue utilizada por el autor presunto del delito informático.

Los equivalentes funcionales de escrito y firma se armonizan con las realidad gracias al principio de neutralidad tecnológica consagrado en los artículos 6 y 7 de la ley 527, los cuales establecen que no será necesario el uso de una tecnología específica para lograr el equivalente de cada uno de ellos, por cuanto estos quedan satisfechos con el cumplimiento de las funciones establecidas para cada caso en concreto, cuestión que servirá para que un mensaje de datos se entienda firmado o conste por escrito.[51]

Todo el análisis anterior nos permite ver la problemática de la prueba electrónica en Colombia y, en especial, la valoración de esta. Ello teniendo en cuenta que la prueba electrónica es otro tipo de prueba físicamente concebida, que encuentra su soporte en un medio magnético, sin perjuicio de que por regla general sea considerada como una prueba documental.[52]. Así es como la valoración de la prueba electrónica, además de contener y cumplir las normas consagradas en los artículos 174 y siguientes del Código de Procedimiento Civil, deberá reunir los requisitos establecidos por la ley 527 de 1999. Los requisitos de admisibilidad de la evidencia digital se encuentran desarrollados en el artículo 10 de la mencionada ley, que estipula:

"Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VII del Titulo XIII, Sección Tercera, Libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negara eficacia, validez o fuerza obligatoria y probatoria

[51] Revista de Derecho, Comunicaciones y Nuevas Tecnologías. 5 ed. p.88.

[52] LA PRUEBA EN EL SISTEMA PENAL ACUSATORIO, cap. 7. Disponible en: http:// www.fiu.co/fiu/dp/cdinteractivo/manuales/y/formatos/modulopruebas.pdf. Consultado el 3 de Mayo de 2011.

a todo tipo de información en un mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".

A partir del precepto anterior, el juez no podrá negarle fuerza probatoria ni admisibilidad a los mensajes de datos por el simple hecho de serlo. Esto por cuanto se presentaría una ilegalidad por parte de este al contrariar los mandatos establecidos en la ley. Así como en materia civil la prueba debe ser valorada desde la sana critica y razonabilidad del juez, para el caso de la prueba electrónica este también deberá cumplir con la normatividad estipulada en la ley 527 de 1999. Es decir que sumado con esos dos conceptos, el juez deberá "estudiar y valorar la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje y en la forma en que se identifique a su iniciador y cualquier otro factor pertinente".[53]

En Colombia se cuenta con dos alternativas jurídicas de valoración de la prueba electrónica en los delitos informáticos que, a pesar de ser idóneas y eficaces para esclarecer los hechos de un caso, cuentan con problemas de tiempo, costos, especialidad y uso de tecnología especial para la identificación y valoración de este tipo de prueba, problemas que pueden llegar a obstruir la eficiencia en la resolución del litigio.

En primer lugar, los hechos pueden ser valorados a través de un *peritazgo* decretado por el juez, el cual no es obligatorio y si susceptible de ser objetado por cualquiera de las partes en materia civil, pero en materia penal esa evidencia que se recolecta se envía a los funcionarios encargados del estudio de este tipo de pruebas para que las analicen y posterior a esto presenten sus dictámenes ante el estrado judicial. La segunda alternativa que tiene el juez recae en la valoración de las pruebas electrónicas como meros *indicios*, por cuanto el mensaje de datos que determina la existencia de un hecho dentro del proceso podría no llegar a cumplir con los requisitos mínimos de

[53] ley 527 de 1999. Op., cit. art 11.

seguridad jurídica, cuestión que puede no proporcionarle al juez la confianza sobre la autenticidad de la información almacenada en un documento electrónico.

Esto trae como consecuencia el restarle fuerza probatoria a la evidencia aportada en el formato de mensaje de datos, sin tener en cuenta que esta es una prueba apta para darle certeza al juez sobre los hechos del caso en particular y que en dado caso puede servir como plena prueba al ser admitida de esta forma en un proceso, esto ahorraría la necesidad de acudir a los auxiliares de la justicia.

2.2.2 DE LA PROBLEMÁTICA DEL DELITO INFORMATICO

El reconocimiento del desarrollo, conformación y superposición del delito informático en torno a una amplia gama de disciplinas y la facultad para determinar el grado real de los denominados delitos informáticos y la amenaza que estos implican para la sociedad, generan grandes dificultades. Tales dificultades se centran en torno a dos cuestiones fundamentales: en primer lugar, que no existe una definición del delito informático universalmente aceptada; en segundo lugar, que el nivel de detección de dichos crímenes, al igual que los métodos establecidos para determinar los daños monetarios resultantes de estos, son considerados inadecuados.

La falta de un acuerdo en torno a la definición de delitos informáticos solo puede entorpecer el juzgamiento de dichos crímenes, pues en muchos casos los jueces se han inclinado por entender los delitos informáticos como una forma novedosa de cometer fechorías tradicionales. En consecuencia muchos de estos delitos “son procesados como crímenes tradicionales, por el hecho de no verificar que los requisitos que cumplen ciertas conductas delictivas se encuadran en un delito considerado como informático”.[54]

[54] United State sentencing Comission [acceso el 12 de junio de 2008] disponible en: http//www.ussc.gov/publicat/cmptfrd.pdf. Consultado el 03 de Mayo de 2011.

A pesar de la posición asumida por el ordenamiento jurídico colombiano frente al valor probatorio y la admisibilidad de las nuevas tecnologías y sus productos en los procesos judiciales, la presentación de evidencia digital ante los jueces implica grandes dificultades. No es suficiente descifrar el lenguaje técnico a los términos de un abogado, como se traduciría una lengua extranjera al español, pues las complejidades de este tipo de casos frecuentemente sobrepasan los conocimientos y la experiencia de los funcionarios judiciales. Incluso algunos elementos de la evidencia digital pueden parecer intangibles para los funcionarios digitales, dada su naturaleza "virtual" o sus confusas similitudes con otros elementos de evidencia." Esto podría ilustrarse en la realidad a través de un caso en el que tuviese que explicarse a un juez las diferencias entre la fecha del último acceso y la de la última modificación de un archivo en el sistema de archivos NT System (NTFS) en un sistema informático".[55]

A diferencia del documento escrito, las pruebas contenidas en un ordenador deben ser allegadas a un proceso judicial junto a una interpretación exacta, que claramente identifique su importancia en el contexto donde fueron encontradas. Por ejemplo, el disco duro de una computadora comprende datos binarios e ignora tipos de datos más complejos, que pueden estar codificados como simples códigos binarios, códigos binarios decimales, o datos hexadecimales. Es por esto que la interpretación de la evidencia digital debe estar en manos de personal calificado, con fines de poder ser presentada en forma accesible para su posterior examen por un tribunal. No obstante, la simplificación excesiva puede resultar peligrosa, en la medida en que puede implicar una interpretación muy abierta de la evidencia.

Es por esto que nace la necesidad de comenzar a capacitar personal especializado en la materia, puesto que no se puede decir que un juez rápida y efectivamente entenderá

[55](Kennedy, I.,"investigating digital crime", en R.Bryant, investigating digital crime, England, Wiley, 2008, p. 52). Consultado el 03 de mayo de 2011.

la terminología informática en aras de descubrir la verdad y entender el conducto que realizo la evidencia digital.

Los factores de incidencia en una investigación de la informática forenses son ilustrados de manera general en la siguiente figura:

Para que una investigación pueda coadyuvar a un correcto juzgamiento de las conductas delincuenciales a través de sistemas tecnológicos, informáticos o telemáticos, es menester según el profesor Cano[56] que el sistema de justicia penal este orientado hacia una aplicación de la ley basada en estudios previos, principalmente en aéreas de conocimiento: informática básica, evidencia digital y delitos informáticos.

Todas las conductas realizadas con medios de computo apuntan hacia un mismo lado, el cual es restringir el ingreso a un medio electrónico, destruir evidencia, o cometer por medio de ellos otro tipo de delitos, esto se trae a colación para poder dar respuesta a el interrogante planteado en el capítulo I, la respuesta es NO, efectivamente en nuestra legislación existe normatividad respecto de que ciertas conductas que están

[56] CANO MARTINEZ. Op., cit. 348 p.

enmarcadas como delito informático, los medios y los sujetos que intervienen en ella, no existe un procedimiento establecido para que los investigadores encargados de la evidencia informática, puedan demostrar efectivamente que la manipulación de la prueba fue solo como requisito de análisis probatorio, pero difícilmente pueden respaldarse en alguna normatividad para demostrar que la prueba goza de todas las garantías para que sobre ella se pueda ejercer el principio de contradicción.

Analizada la prueba, en materia penal, podemos decir que esta cumple con los requisitos de forma, que determina en qué casos se está en presencia de posible evidencia o material probatorio, pero adicional a esto necesitamos saber cómo se comporta el delito informático en la sociedad, con esto me refiero a cuáles son las modalidades delictivas que pueden utilizar los sujetos por medio de la tecnología para cometer ilícitos. Una vez encontramos cuáles son los modos operandi podremos construir parámetros para contrarrestar esta manipulación de tecnología, y de este modo entender por qué es importante no solo el procedimiento para la eficacia de la prueba, sino la importancia que llegan a tener las garantías que se encuentran inmersas en un proceso penal.

CAPITULO III

ASPECTOS CRIMINALISTICOS DE LA INFORMATICA

Las practicas en computación forense han venido avanzando y armonizándose de tal forma que los profesionales de esta disciplina consiguen cada vez resultados más confiables y tecnologías más efectivas, sin embargo, la misma dinámica de las vulnerabilidades tecnológicas y la inseguridad informática propia de los sistemas computacionales hace que día a día los esfuerzos de homogenización de dichas prácticas reciban mensajes nuevos, que exijan repensar nuevamente la manera de cómo se adelantan las investigaciones y los análisis. Por lo tanto las mejores acciones adelantadas con herramientas forenses siempre estarán expuestas a nuevos desafíos y pruebas, permitiendo nuevos desarrollos y estrategias para enfrentar la inseguridad de la información y los exigentes requisitos legales, alrededor de la evidencia digital, que se demandan al participar en un proceso judicial y por consiguiente la evidencia que de ellas se pueda recolectar.

La computación antiforense plantea una reflexión en el "lado oscuro" de las investigaciones forenses. Una realidad la cual nos invita a ver "lo que nosotros no vemos", a quitarnos la venda de nuestra propia experiencia, para observar cómo, cuanto conocemos puede ser vulnerado, distorsionado, escondido o destruido, sin que muchas veces nos percatemos de los hechos. Esto no solo lleva a cuestionar al investigador sobre su propia practica y las herramientas que utiliza para ello, sino a saber que dependiendo del manejo que se le dé a esa evidencia que sea hallada dentro de un ilícito, esta podría convertirse en la prueba más valiosa dentro de un proceso judicial, por lo tanto es una cadena de labores entrelazadas, que van desde el investigador hasta los órganos judiciales quienes son en ultimas las personas frente a las cuales va a ser llevada esa evidencia para que le propongan un valor probatorio[57].

[57] http://www.alfa-redi.org/rdi-articulo.shtml?x=9608. Consultado el 13 de Febrero de 2011.

Dentro del primer aspecto la criminalística informática, encontramos las *estrategias antiforenses* que dentro de su infinidad de definiciones encontramos una que se asemeja más a la realidad como lo describe Harris, R., 2006;[58] son métodos usados para prevenir la aplicación de la ciencia por parte de las agencias de policía, como apoyo a las leyes penales y civiles en un sistema de administración de justicia, o es cualquier intento para limitar la cantidad y la calidad de la evidencia forense. La finalidad de cualquier definición encontrada es la de poder entorpecer la actividad de los investigadores judiciales, colocándoles una tarea mucho más ardua de encontrar cualquier rastro o evidencia que pueda ser hallado en la escena del crimen. Estas estrategias tienen, entre otros objetivos los siguientes según Garfinkel, S., 2007[59]:

- Limitar la detección de un evento que haya ocurrido
- Distorsionar la información residente en el sitio
- Incrementar el tiempo requerido para la investigación
- Generar dudas en el informe forense o en el testimonio que se presente
- Engañar y limitar la operación de las herramientas forenses informáticas
- Diseñar y ejecutar un ataque contra el investigador forense que realice la pericia
- Eliminar los rastros que pudiesen haber quedado luego de los hechos investigados

Considerando los objetivos planteados es necesario conocer detalladamente el procedimiento que se utiliza en la informática forense para que los investigadores puedan desvirtuarlos uno a uno.

Según los investigadores dichas estrategias tienen una materialización a través de métodos evasivos como lo son: *la destrucción de evidencia, la eliminación de la fuente de evidencia, el ocultamiento de evidencia y la falsificación de evidencia.* La Destrucción de evidencia lo que busca es modificar el objeto que contiene la evidencia

[58] HARRIS, R. Arriving at anti-forensics consensus: examining how to define and control the anti-forensics problem. Digital investigation. P. 44-49. Citado por Jeimy Cano.pag.340.
[59] GARFINKEL, S. When the virtual is harder than real. Security challenges machine based computing environments. Depertment of computer science Stanford University. Citado por Jeimy Cano.p 341.

digital requerida, de tal forma que no sea posible conseguirla de manera confiable o real. Cuando se habla de eliminar la fuente de la evidencia, significa neutralizar el sistema o la técnica utilizada por el sistema para dejar los rastros, al controlar esa técnica o proceso no existirá evidencia y, por tanto, no habrá trazas que seguir en una investigación.

Si el atacante no ha podido materializar los dos métodos anteriores puede optar por esconder la evidencia o falsificarla. En la primera, la evidencia se dispersa en el medio que la contiene, se oculta en el o en el sistema en donde se encuentre, limitando los hallazgos del investigador en su proceso. En la segunda, crea o invalida la evidencia residente en el sistema para limitar las conclusiones o el análisis que adelante el investigador[60].

Completando la propuesta de Harris, Garfinkel habla sobre la materialización de las técnicas antiforenses, detalla algunas técnicas tradicionales utilizadas como lo son *la sobrescritura de datos y metadatos,* así como la utilización de técnicas *criptográficas* y *esteganograficas.* La sobrescritura de datos y metadatos según el autor está asociada con la modificación física de la información residente en los medios de almacenamiento y sus sistemas de archivo. Esto es una manera de dejar inconsistente una posible recuperación de información o una forma de construir entradas falsas en las tablas de asignación de archivos que generan la aparición de archivos inexistentes.

Las técnicas criptográficas son un desafío para los investigadores forenses, ya que identificar evidencia digital cifrada establece una barrera para continuar con los hallazgos y genera discontinuidad en los rastros requeridos para armar la cadena de eventos. Cuando se da esta situación en una investigación en donde se presume que existió un delito informático lo único que produce es un entorpecimiento automáticamente la acción judicial y por ende el proceso penal, convirtiéndolo en tedioso y extenso.

[60] CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá: Universidad de los Andes, 2010. P.340.

La criptografía actualmente ataca la efectividad de las herramientas forenses y los resultados asociados con los análisis realizados por estas. De igual forma la esteganografia, entendida como el "arte de esconder la información, no solo opera sobre imágenes, sino sobre sistemas de archivos o tráfico de red, amplia el espectro de análisis y cuidados que el investigador debe tener cuando de aplicar sus procedimientos se trata"[61].

Todo lo anterior son las diversas formas que tienen los actores de un delito para tratar de entorpecer la justicia, es necesario haberlo determinado, puesto que una vez establecido en qué momento se materializa las técnicas antiforenses, el investigador puede empezar a actuar y con ello saber que elementos utilizar para poder descubrir al menos rastros de la comisión del delito. Una de las etapas más importantes de la investigación es la cadena de custodia que según el artículo 254 del Código de Procedimiento penal tiene como finalidad "…demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicara teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envió; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrara el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos…." Esta cadena de actuaciones tiene mayor incidencia en la investigación, por decirlo de esta forma es el punto de partida de una investigación exitosa que, al momento en el que el perito tenga contacto con dicha evidencia y seguir las determinaciones legales, podrá encontrar completa seguridad en que el elemento material probatorio o evidencia física guarda las mismas características que cuando fue recolectado.

3.1 MANEJO DE EVIDENCIA INFORMATICA EN EL DERECHO COMPARADO

Con las bases establecidas anteriormente sobre la situación de cómo posiblemente se pueden cometer ilícitos a través de sistemas de computo, podemos entrar a analizar un

[61] CANO MARTINEZ, Op., Cit. P. 337.

sistema jurídico penal de un país latinoamericano que pese a tener una legislación diferente a la nuestra, ha podido crear un manual del procedimiento que tienen que poner en práctica los investigadores judiciales en referencia al manejo de evidencia probatorio en el delito informático. Las modalidades de delitos pueden tener denominaciones diferentes en cada país, pero los mecanismos utilizados para la comisión del delitos son las mismas, en lo que puede existir una similitud, es en el manejo de evidencia, la cual pese a que los administradores de justicia tiene leyes diferentes, su finalidad es impartir justicia y encontrar la verdad, la cual podrá otorgar una prueba que goce de toda la validez requerida para llevar un proceso judicial a feliz término.

Ecuador ha sido uno de los principales países latinoamericanos en tener grandes avances en la materia, esto ha sido posible gracias a un gran equipo de personas que han podido construir un manual de manejo de evidencia informática en cabeza del doctor Santiago Acurio Del Pino, quien es el coordinador del departamento informático del ministerio fiscal distrital de pichincha (Ecuador), quien se ha encargado de materializar todas las ideas de crear lineamientos para los investigadores judiciales, quienes al ceñirse a esto, están creando un bloque de igualdad y seguridad jurídica para la comunidad.

Para el doctor Acurio *"la prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material. Aparecen en un inicio como presuntos responsables las personas que efectivamente así lo arroje la prueba, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento. El objetivo de la Informática forense es el de recobrar los registros y*

mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal"[62].

El Doctor Acurio en un llamativo manual y muy práctico por cierto, comienza por plantear principios básicos de la actuación judicial, entre ellos se encuentra como primera medida el hecho que los investigadores deben planear y coordinar sus acciones antes de tener contacto con la escena del crimen, no se puede de ninguna manera cambiar o alterar la información que se va almacenando a través de los hallazgos, en casos excepcionales puede una persona competente tener acceso a la información encontrada, estas personas llamadas peritos especializados van a colaborar con el procedimiento forense y posterior a ello, deberán rendir informe detallado de sus actuaciones, propone además que los investigadores deben llevar un orden en el registro de acciones realizadas, así como de las observaciones pertinentes que tengan frente a la comisión del delito, por último plantea que el fiscal designado estará encargado de dar cumplimiento a la ley.

El peritaje que realiza la persona especializada tiene que gozar con los principios de objetividad, autenticidad, legalidad, idoneidad, inalterabilidad y documentación, todos estos principios se encuentran consagrados en nuestra legislación colombiana y por no abordar todas las demás legislaciones, se podría decir que un gran número de ellas se encuentran en concordancia, no solo en lo que refiere a la prueba pericial sino a las finalidades que tiene la cadena de custodia ya sea en el delito informático o en los demás delitos consagrados en la ley penal.

El reconocimiento de la evidencia digital como siguiente paso es de vital importancia, ya que es importante clarificar los conceptos y describir la terminología adecuada que señale el rol que tiene un sistema informático dentro del *iter criminis*[63] o camino del

[62] MANUAL DE EVIDENCIA INFORMATICA. Acurio. http://www.slideshare.net/cxocommunity/manual-de. p.7. Consultado el 05 de febrero de 2011.

[63] "Es el conjunto de actos para llegar al delito" http://jorgemachicado.blogspot.com/2009/03/concepto-del-iter-criminis-o-fases-de.html. Consultado el 05 de Febrero de 2011.

delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener en el caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara donde debe ser ubicada y como debe ser usada la evidencia.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación. Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos, si de delito informático hablamos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

Una vez encontrados los hallazgos o los objetos materia de prueba, en el manual del doctor Acurio señala que se debe proseguir con la incautación de los elementos, situación esta que ocurre de igual forma en Colombia cuando la policía judicial emprende la cadena de custodia de acuerdo a lo consagrado en el artículo 254 del Código de Procedimiento Penal, y con dicha incautación todas la demás actuaciones previstas en los artículos siguientes del código.

Lo que se plantea a continuación son procedimientos que realizan los investigadores en Ecuador por supuesto siguiendo los lineamientos penales de su legislación.

3.1.1 EN LA ESCENA DEL DELITO

Los Investigadores que llegan primero a una escena del crimen y tienen ciertas responsabilidades como lo son:

- **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque.

- **INICIE LAS MEDIDAS DE SEGURIDAD**: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal. Esto según los creadores del *manual de manejo de evidencia informática* es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.

- **FACILITE LOS PRIMEROS AUXILIOS**: Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

- **ASEGURE FÍSICAMENTE LA ESCENA**: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su

posible alteración. Situación que se puede dar en cualquier clase de delitos penales.

- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS**: Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias como anteriormente lo mencionamos, se debe guardar y etiquetar cada una de ellas lo que en Colombia se conoce como Rotulación. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.

- **ENTREGAR LA ESCENA DEL DELITO**: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema correspondiente. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA**: Es indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas

referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del delito, esto en Colombia es llamado programa metodológico del cual están encargados los investigadores y el fiscal del caso ya que dentro de este programa, los investigadores están en la obligación de presentar 3 tipos de informes entre ellos; informe de campo, ejecutivo y de laboratorio, este ultimo exteriorizado una vez se realicen todos los experimentos necesarios sobre la prueba.

3.1.2 RECONSTRUCCION DEL DELITO

La reconstrucción del delito permite al investigador forense comprender todos los hechos relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del delito permiten al investigador realizar tres formas de reconstrucción a saber[64]:

Reconstrucción Relacional, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos.

Reconstrucción Funcional, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados

Reconstrucción Temporal, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

Este tipo de actividad aparte de ser realizada por expertos es indispensable que ellos utilicen la lógica o las posibles alternativas que por instinto se pueden deducir de la escena del delito, porque es este instinto el que puede dar una solución a una serie de interrogantes que se susciten en el trascurso de la investigación. Como ocurre en muchas ocasiones los elementos materiales probatorios que se encuentran en el lugar donde se cometió el delito son muy pocos, dificultando la actividad Estatal, y es la

[64] Ibid.,p.9.

astucia del personal especializado la que entraría a jugar un papel importante en la solución de una problemática existente.

3.1.3 ¿QUE HACER AL ENCONTRAR UN DISPOSITIVO INFORMATICO O ELECTRONICO?

A partir de esta pregunta, encontraremos una serie de procedimientos que no solo la policía judicial tendría que realizar, sino que cualquier persona del común podría aplicar en caso de que no se encuentre el personal especializado para salvaguardar una prueba. Este protocolo es el que se utiliza en Ecuador para los investigadores judiciales y se ha demostrado que ha sido efectivo a la hora de dotar la evidencia electrónica de plena validez.

Como medida primaria se dice que no se puede tomar objetos sin guantes de hule, ya que podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

Entre otras medidas se encuentran[65]:

- Asegurar el lugar.
- Asegurar los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños
- Si no está encendido, no encender *(para evitar el inicio de cualquier tipo de programa de autoprotección).*

[65] Ibid.,p.10.

- Verificar si es posible acceder a el sistema operativo con el fin de iniciar la secuencia de apagado y evitar pérdida de información.

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

- Si está encendido, no apagar inmediatamente para evitar la pérdida de información.

- si es posible, llamar un técnico.

CUANDO NO HAY TECNICO

Se recomienda:

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

- Si está encendido, no lo apagar inmediatamente.

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

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

- Si el aparato está conectado a una red, anotar los números de conexión, los conocidos números IP.

- Fotografíe la pantalla, las conexiones y cables.

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

- Coloque etiquetas en los cables para facilitar reconexión posteriormente.

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

- Si hay un disco, una disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retíralo, protegerlo y guardarlo en un contenedor de papel.

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

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

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

- Desconectar la fuente de poder.

- Quitar las baterías y almacenarlas de forma separada el equipo (si funciona a base de baterías o es una computadora portátil).

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

- Al llevar aparatos, anotar todo número de identificación, manteniendo siempre la cadena de custodia.

- Llevar todo cable, accesorio, conexión.

- Llevar, si es posible, manuales, documentación, anotaciones.

- Es necesario tener en cuenta que es posible que existan otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto hay que desconectar el cable de poder de todo hardware de Red (Router, modem).

3.1.4 REGLA DEL ENCENDIDO Y DEL APAGADO

1. Si el aparato está encendido "ON", no lo apague "OFF".

- Si apaga "OFF" puede iniciarse el bloqueo del aparato

- Transcribir toda la información de la pantalla del aparato y de ser posible tomar una fotografía

- Vigilar la batería del aparato, el transporte del mismo puede hacer que se descargue (Tener a mano un cargador)

- Sellar todas las entradas y salidas

- Sellar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria

- Sellar los tornillos para evitar que se puedan retirar o reemplazar piezas internas.

- Buscar y asegurar el conector eléctrico

- Colocar en una bolsa especial para aislar emisiones electromagnéticas, si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa

- Revisar los dispositivos de almacenamiento removibles (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles)

2. Si el aparato está apagado "OFF", dejarlo apagado "OFF".

- Prenderlo puede alterar evidencia al igual que en las computadoras

- Antes del análisis del aparato conseguir un técnico capacitado en el mismo

- Si no existe un técnico usar otro teléfono

- Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado

3.1.5 BUENAS PRÁCTICAS EN LA NECESIDAD DE RECOLECTAR EVIDENCIA INFORMATICA

Entre las sugerencias de los expertos en materia informática forense dentro de lo recomendado por el doctor Acurio y su grupo de expertos, encontramos:

- Recolectar las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.

- Documentar todos los pasos al revisar y recolectar los dispositivos de almacenamiento

- Alejar a los dispositivos de almacenamiento de cualquier magneto, radio trasmisores y otros dispositivos potencialmente dañinos.

Esto en el derecho comparado es algunas de las prácticas que los peritos o investigadores forenses utilizan para darle el mejor manejo probatorio a la evidencia digital recolectada en la escena del delito. Estos lineamientos no se encuentran plasmados en la legislación colombiana, lo que se hace es seguir una costumbre de procedimientos que se han agrupado para manejar la prueba informática, en Ecuador como en otros países del mundo este manejo probatorio ya se está aplicando y se ha podido probar que tiene una efectividad por encima del 70%, motivo aun mas para que Colombia pueda establecer sus propias pautas de manejo de evidencia informática.

Estos parámetros posiblemente se utilizan en nuestro país, ya que en el estudio de la materia de delitos informáticos en lo que refiere al manejo de evidencia informática, se pudo encontrar que existen grupos de investigación que expresamente se han encargado de recopilar este tipo de información, encontrándolo a nivel nacional mas no municipal como se ha hecho en la universidad de los Andes. Lo que se busca extraer

de esta información encontrada, es poder encontrar una materialización de esos mismos lineamientos procesales o al menos una garantía jurídica para los sujetos que intervienen en un proceso penal, buscando siempre descubrir la identidad se los sujetos agentes del delito informático que puede proporcionar una prueba, siendo extremistas, y poniendo como ejemplo una situación en la que sea la única prueba que exista en contra de un posible autor de un delito y que sin los requisitos esenciales del manejo probatorio, un juez de la republica podría inadmitirla y con esto se inaplicaría el principio de la recta impartición de justicia.

Puedo traer a colación un caso de la vida real, lo sucedido con Jerónimo Uribe el hijo menor del ex presidente Álvaro Uribe Vélez, a el cual le llegaron amenazas de muerte por medio de una de las redes sociales más conocidas como es Facebook, presuntamente el responsable de la creación del grupo en la red social era Nicolás Castro un estudiante de bellas artes en la ciudad de Bogotá. El estudiante fue detenido y se le imputo el delito de instigación para delinquir, el fue dejado en libertad por vencimiento de términos ya que se cumplieron 180 días si resolver la situación de imputado.

El abogado del imputado manifestaba que no existían pruebas que lo incriminaran, razón por la cual no se podía dejar detenido a su defendido. La Fiscalía no pudo demostrar ante el juez de control de garantías que efectivamente el señor Nicolás era quien publico dichas amenazas ya que la prueba que fue recolectada en el lugar de habitación de este joven, apuntaba que la dirección IP pertenecía al computador del señor Castro, además de esto la evidencia no fue manejada con el procedimiento efectivo para que esta tuviera eficacia probatoria no solo porque inaplicaron la cadena de custodia, sino porque dentro del procedimiento que realizaron los investigadores judiciales no pudieron demostrar la mismisidad del elemento recolectado "Al parecer, la

orden de captura y los elementos incautados, previo a la detención no surtieron los trámites legales requeridos por la Ley para legitimar la actuación judicial"[66]

Esto siendo uno de los casos más sonados en el ámbito público, pero que a fin de cuentas no tuvo ninguna trascendencia, como en otros casos los cuales se han dejado impunes por no tener fuerza probatoria la evidencia informática.

Argentina y Chile han sido países que han venido desarrollando técnicas similares a las que presenta el profesor Acurio para el manejo de evidencia informática, debido a los grandes índices de criminalidad que han aumentado desde el año 2000 hasta la fecha. En Argentina por ejemplo la justicia, conformó un equipo de peritos expertos en delitos informáticos, los mismos que asisten a las cámaras y juzgados del país, en los casos en los que se encuentran computadoras u otro tipo de dispositivos informáticos involucrados en delitos, sin embargo, también se da la figura de otro tipo de peritos entre los que se encuentran los peritos oficiales, de oficio y de parte, que pasan por un proceso de acreditación establecido de acuerdo a la jurisdicción para encargarse especialmente del manejo de la prueba informática. El estado por tanto está viendo la necesidad de darle un status al manejo de evidencia informática, puesto que por medio de las investigaciones han llegado a la conclusión de no poderle restar importancia a esta prueba técnica.

3.1.6 GUIAS MUNDIALES EXISTENTES PARA EL MANEJO DE EVIDENCIA DIGITAL

Para la recolección de evidencias se dispone de marcos de trabajo de distribución libre que han sido desarrollados tomando en cuenta las mejores prácticas. A continuación la siguiente tabla muestra algunas de las guías de reconocimiento mundial, para la recolección y manejo de evidencias en computación:

[66] http://www.elespectador.com/noticias/judicial/articulo195183-denuncian-ilegalidad-captura-de-nicolas-castro. Consulado el 06 de Febrero de 2011.

GUIA	PATROCINADOR	DISTRIBUCION
RFC 3227 - Guía para recolectar y archivar evidencia	Network Working Group http://www.ietf.org	Libre
Guía IOCE - Guía de mejores prácticas en el examen forense de tecnología digital	International Organization on Computer Evidence http://www.ioce.org	Libre
Guía DoJ1 - Investigación en la escena del crimen electrónico	U.S. Department of Justice http://www.usdoj.gov	Libre
Guía DoJ2 - Examen forense de evidencia digital	U.S. Department of Justice http://www.usdoj.gov	Libre
Guía Hong Kong Computación forense – Parte 2 – Mejores Practicas	SWGDE - Scientific Working Group on Digital Evidence http://www.swgde.org/	Libre

En el siguiente capítulo a través del trabajo de campo podremos hacer una comparación más exacta de lo que sucede en Colombia específicamente lo que podemos ver reflejado en Bucaramanga y con ello analizar las falencias que presenta nuestro sistema penal en lo que refiere al manejo de la prueba técnica o evidencia informática.

IV. TRABAJO DE CAMPO

A partir del trabajo de campo que se realizó podemos construir unos parámetros que van de la mano con las finalidades que el legislador propuso en la ley penal, las cuales podrán ser directrices para los investigadores judiciales y para los administradores de justicia a la hora de darle vida jurídica a la evidencia digital proveniente de la comisión de un delito informático.

4.1 ESTADISTICAS Y RECOLECCION DE DATOS

Lo primero que hicimos en esta investigación fue recolectar toda la información existente y de libre acceso que reposaba en la Fiscalía General de la Nación en el Municipio de Bucaramanga sobre los delitos informáticos que se han judicializado entre el año 2008 a 2010.

En la dependencia que se encarga de manejar los delitos informáticos, se encontró que desde el año 2006 al 2008 no se manejaba una base de datos sistematizada lo que impidió una estadística de los delitos informáticos a los cuales se les ha dado tramite durante ese lapso de tiempo.

La información a la cual pudimos tener acceso fue a los delitos informáticos manejados desde el año 2008 bajo la ley 906, algunos de estos delitos no son informáticos o no se encuentran dentro de la ley 1273 de 2009, pero esta entidad por medio de su Cuerpo Técnico de Investigación los ha atendido por que fueron realizados o cometidos a través de un medio informático.

Muchos de los casos relacionados a continuación se encuentran aun en investigación sobre todo los relacionados con hurtos informáticos debido a su complejidad:

CASOS POR TIPO DE DELITO	NUMERO DE CASOS
INJURIA Y CALUMNIA	136
ESTAFA	15
ACCESO ABUSIVO A UN SISTEMA INFORMATICO	22
HURTO POR MEDIO INFORMATICO Y SEMEJANTES	125
AMENAZAS	5
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	32
OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO O RED DE TELECOMUNICACION	6

PORNOGRAFIA CON MENORES	5
FALSEDAD EN DOCUMENTO PRIVADO	3
FALSEDAD PERSONAL	4
TOTAL	**353**

4.2 HABLANDO CON LOS INVESTIGADORES

Estos delitos pese a que no se encuentran descritos en la ley 1273 de 2009, también son cometidos por medios informáticos. Los investigadores durante el trabajo de campo nos manifestaban que la injuria y la calumnia son de los delitos más denunciados, aluden que se debía a que a nivel informático las redes sociales si bien eran herramientas útiles de comunicación, también eran medios ideales para amenazar la vida y honra de las personas, ya que por estos medios la vida personal se hace pública.

Después de haber encontrado estas cifras delictuales, en medio de charlas con los investigadores judiciales ellos relataron que si bien es cierto hay conductas que se han denunciado en la Fiscalía sobre actuaciones que revierten todas las características de los delitos tipificados en la ley 1273 de 2009, los administradores de justicia han variado la calificación de la conducta y la han tipificado en otro tipo de delitos, esto debido al

poco conocimiento que se tienen sobre las particularidades de los llamados delitos informáticos.

Es por esta razón existió la dificultad de encontrar sentencias que hayan calificado conductas punibles como delitos informáticos, la cultura sobre ellos es muy poca, pese a que los investigadores en audiencia pública han mostrado por que pertenecen a esa categoría de delitos.

4.3 CADENA DE CUSTODIA

El siguiente paso a analizar es el llamado cadena de custodia, según el Doctor Fernando Barajas Coordinador de la sección de delitos informáticos del CTI en Bucaramanga, esta medida es de vital importancia en la investigación penal porque de ello es donde dicha prueba podrá obtener la validez jurídica requerida por el juez.

La cadena de custodia comprende el conjunto de una serie de etapas que deben garantizar, con plena certeza, que las muestras y objetos por analizar y que posteriormente serán expuestos como elementos de prueba en las diferentes etapas del proceso, son los mismos que se recolectaron en el lugar de los hechos. Es a partir de estas etapas donde la prueba o evidencia digital se vuelve de vital importancia y de importante cuidado.

Es por ello que cada etapa debe ser manejada con el cuidado debido y con la profesionalidad que obliga el caso, una prueba que se halle en el lugar de los hechos y que los investigadores no cumplan con los parámetro establecidos por la norma para la custodia de la misma, no podrá gozar de validez alguna en un proceso penal, con ello la imposibilidad de atribuir una conducta típica, antijurídica y culpable que se haya realizado en contra de un inocente.

4.4 VALIDEZ JURÍDICA DE LA EVIDENCIA EN EL AMBITO COLOMBIANO

Para que la evidencia digital pueda alcanzar validez jurídica dentro de un proceso se hace necesario en primera instancia que exista una relación entre el delito y su autor, como bien se ha mencionado a dicha evidencia dentro de la legislación colombiana se le ha otorgado la misma fuerza probatoria que la de un documento. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son[67]:

- Autenticidad: satisfacer a los administradores de justicia en que: los contenidos de la evidencia no han sido modificados, la información proviene de la fuente identificada, y la información externa es precisa

- Precisión: debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en un proceso judicial. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos entendibles, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.

- Suficiencia: debe por sí misma y en sus propios términos mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

4.4.1 Requerimientos legales de la Evidencia Digital en Colombia

La Ley 527 de 1999 fue la base para poder darle fuerza probatoria a la evidencia informática en Colombia, a partir de ella y con la necesidad de reglamentar la materia se fueron construyendo normatividades que permitieron a la justicia crear

[67] Evidencia digital en el contexto colombiano. http://www.acis.org.co. Consultado el 11 de Febrero de 2011.

medianamente bases sólidas en lo que refiere a delitos cometidos por medios informáticos y con ello la aplicación de sanciones que adviertan a la sociedad sobre el uso indebido de la informática.

Los dos artículos dieron cabida a la validez jurídica del mensaje de datos y con ello su desarrollo normativo fue:

Ley 527. ART. 10. Admisibilidad y fuerza probatoria de los mensajes de datos. “Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original”.

Ley 527. ART. 11. Criterio para valorar probatoriamente un mensaje de datos. “Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente”.

Es decir, para que en Colombia un mensaje de datos tenga valor probatorio debe asegurarse: la confiabilidad en la forma en la que se generó; la confiabilidad en la forma en la que se conservó; y, la confiabilidad en la forma en la que se identifica al autor.

Además, la Corte Constitucional en la Sentencia No. C-662 de Junio 8 de 2000[68] consideró: "El proyecto de ley establece que los mensajes de datos se deben considerar como medios de prueba, equiparando los mensajes de datos a los otros medios de prueba originalmente escritos en papel. Al hacer referencia a la definición de documentos del Código de Procedimiento Civil, le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración algunos criterios como: confiabilidad, integridad de la información e identificación del autor".

4.5 PROCEDIMIENTO FORENSE PARA EL MANEJO DE INVESTIGACIONES

En la ciudad de Bucaramanga como en todo el territorio nacional el tema de delitos informáticos manejados por la Fiscalía General de la Nación ha tenido especial tratamiento pues su finalidad es garantizar a la sociedad la recta impartición de justicia. Esta búsqueda no ha venido sola, existen personas especializadas en la materia que se han dedicado a encontrar las falencias y fortalezas de las instituciones del Estado que tienen a su cargo la investigación y los procedimientos que tengan relación con los delitos cometidos por medios informáticos, con esto me refiero al doctor Jeimy Cano, el doctor Daniel Torres, y la doctora Sandra Rueda, quienes en la actualidad son docentes de la Universidad de los Andes y que se han dedicado a estudiar el tema desde la informática pura.

Dentro de sus múltiples estudios en la informática forense han publicado un artículo en donde claramente se recopila todas las actuaciones que deben realizar los investigadores judiciales independientemente de la dependencia a que pertenezcan (CTI, FISCALIA, SIGIN, etc) No es posible definir un procedimiento único para adelantar un análisis en Informática forense. Pero, si es posible definir una aproximación

[68] Sentencia Corte Constitucional en la Sentencia No. C-662 de Junio 8 de 2000. MP: Fabio Morón Díaz.

metodológica que permita el manejo adecuado de la evidencia digital, minimice la posibilidad de cometer errores en su manejo y que en alguna medida garantice la admisibilidad de la misma en situaciones jurídicas. Dicha aproximación incluye cinco etapas: planeación, recolección, aseguramiento, análisis y presentación de la Evidencia Digital.

4.5.1 Planeación

Teniendo en cuenta que todos los pasos anteriormente nombrados son metodológicos, se necesitó la verificación de los mismos durante el trabajo de campo que se realizó con el doctor Fernando Barajas, en el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, corroborando que efectivamente la recopilación que realizaron los docentes de la Universidad de los Andes apuntan a las actividades que realizan los cuerpos de investigación, dejando la salvedad por parte del doctor Barajas que si bien es cierto los pasos medianamente se cumplen no existe en su corporación una normatividad legal que exija su cumplimiento.

"Se espera que en esta etapa se detecte el incidente, el investigador se familiarice con dicho incidente y con el entorno en el que ocurrió y determine el proceso para la recolección de evidencia. El primer paso consiste en determinar los presuntos actores involucrados, (máquinas y/o usuarios), identificar el problema aparente e indagar qué tanto contacto tuvieron los usuarios con el sistema involucrado en el delito, para darse una idea de la contaminación de la escena"[69].

El doctor Jeimy segundo paso durante la planeación de la investigación exterioriza que "el investigador se debe familiarizar con el entorno informático y con el acontecimiento en cuestión. Para ello se sugiere el desarrollo de entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático, se busca determinar: Qué tipo de sistemas informáticos se usan, qué tipo de registros generan, si

[69]Evidencia digital en el contexto colombiano. Op,.Cit.pag3.

se cuenta con políticas de seguridad o no y quiénes son responsables del funcionamiento de los equipos y los servicios de la organización, etc"[70].

El investigador debe describir con detalle la escena, incluyendo nombres de usuarios y roles, ubicación física de usuarios, equipos, puntos de red, etc. Si es posible, se debe registrar información gráfica del lugar (fotos y videos), ya que muchas veces en ellos se encontrarán detalles que posteriormente pueden ser de utilidad en de la investigación, y que también pueden convertirse en evidencia digital: serán documentos todas aquellas formas de expresión producto del desarrollo de las técnicas de la comunicación y la informática, incluyendo, por ejemplo: videos y fotografías.

4.5.2 Recolección

Durante esta etapa los investigadores deben tener presente los requisitos exigidos por la ley 527 para que puedan garantizar que la prueba posiblemente pueda producir efectos jurídicos, de igual forma la evidencia recolectada debe ser la más relevante en la escena del crimen, de forma objetiva el investigador utilizando todo su olfato profesional determinara que elementos pueden o no llevarse a un análisis posterior, "habrá de tenerse en cuenta la confiabilidad en la forma en la que se haya generado, archivado o comunicado la información".[71]

Como muchas veces no es posible presentar los sistemas involucrados en una audiencia o tenerlos durante la investigación, se recomienda tomar una copia idéntica - Bit a Bit- de su contenido. Copia que representará al sistema en cuestión y que además será sobre la que se trabaje. Este tipo de copia es realizada por medio de herramientas que permiten copiar el contenido visible del dispositivo de almacenamiento, y el contenido invisible, es decir, la información de las áreas del disco que no están siendo

[70] Ibid,.pag3.
[71] CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá: Universidad de los Andes, 2010. 348p.

utilizadas, esto incluye los sectores que se encuentran disponibles para escritura, los que no están siendo utilizados por ninguna partición y el espacio sobrante cuando la información que se escribe en un bloque es menor que el tamaño de este[72].

El segundo enfoque toma medidas pasivas que, aunque no corrigen los problemas inmediatamente, permiten analizar el estado del sistema. Además, esto permite utilizar otras herramientas, tales como sniffers y honeypots, para recolectar nuevas pruebas que permitan o bien identificar al autor del delito o tener más evidencia. Es importante mencionar, que no se espera que toda la información que se examine y/o recolecte deba ser admisible como evidencia. Mucha de esta información será utilizada para, a través de ella, descubrir evidencia admisible[73].

El investigador como anteriormente se dijo es quien decide que tanta cantidad de información se debe recolectar, como sabemos dentro de la fiscalía antes de iniciar cualquier investigación el fiscal encargado del caso realiza un plan de trabajo llamado Programa Metodológico que junto a sus colaboradores cumplirán durante el desarrollo del caso, con esto cada movimiento que den tiene que ir ligado con los planteamiento inicialmente expuestos así como con la normatividad existente, puesto que se deja plasmado que, en donde y como se investigara.

Independientemente del camino tomado para realizar el proceso de recolección, la evidencia siempre debe ser recolectada de lo más a lo menos volátil.

Existen características de las herramientas de recolección forenses mínimas que deben cumplir las herramientas forenses para que la evidencia recolectada y/o analizada por ellas sea confiable son las siguientes[74]:

[72] Evidencia digital en el contexto colombiano. Op,. Cit. Pag4.
[73] Ibid,.pag5.
[74] Ibid,.pag5.

- Manejar diferentes niveles de abstracción: dado que el formato de la información en su nivel más bajo es difícil de leer, la herramienta debe interpretar la información y ofrecer acceso en diferentes niveles.

- Deben tener la capacidad de extraer una imagen bit a bit de la información. Todo byte debe ser copiado de la fuente, desde el comienzo hasta el final de ella sin importar si hay fragmentos en blanco.

- Deben tener un manejo robusto de errores de lectura. Si el proceso de copia falla al leer un sector de la media fuente, se debe marcar en el medio destino un sector del mismo tamaño y en la misma ubicación que identifique el sector que no pudo leerse, adicionalmente estas fallas deben ser documentadas.

- La aplicación no debe cambiar de ninguna manera el medio original.

- La aplicación debe tener la habilidad de realizar pruebas y análisis de una manera científica. Estos resultados deben poder ser reproducibles y verificables por una tercera persona.

Teniendo en cuenta estas consideraciones acerca de las herramientas, el investigador debe estar en capacidad de:

- Examinar el estado general del sistema: la memoria RAM de un computador, la lista de procesos en ejecución y el estado de la red.

- Realizar duplicados forenses.

- Desarrollar scripts y aplicaciones para automatizar la recolección.

Queda a criterio del investigador determinar si es correcto apagar y/o reiniciar el sistema relacionado con el delito que se investiga, ya que, al hacer esto se perderá información que puede ser valiosa en el momento de correlacionar la evidencia recolectada (el contenido de la memoria, qué archivos están abiertos, el estado de las conexiones de red, los procesos que se están ejecutando, los usuarios que están dentro del sistema), por esta razón recomiendan los expertos, mientras sea posible, generar una imagen del estado del sistema previa a que este sea apagado.

4.5.3 Preservación y aseguramiento de la evidencia digital

En esta etapa se busca garantizar uno más de los requisitos de admisibilidad fijados por la Ley 527 de la Legislación Colombiana: Para valorar la fuerza probatoria de la información digital habrá de tenerse en cuenta la confiabilidad en la forma en la que se haya conservado la integridad de la información y la forma en la que se identifique a su iniciador[75].

Para verificar la mismicidad de la evidencia recolectada se hace necesario que expertos en materia informática creen códigos que protejan la información, de esta forma buscaran la inalterabilidad de la prueba, este procedimiento difícilmente es utilizado por personas del común pese a que existen programas simuladores abiertos al comercio que indican cómo se puede verificar que un dato o un sistema de cómputo entero que guarda las mismas características iniciales de recolección. Colombia cuenta con entidades que expiden certificados de firma digital que pueden ser útiles para este tipo de procesos, sirviendo de esta forma no solo a la Fiscalía como estén acusador, sino a la defensa para que pueda probar su inocencia.

[75] Evidencia digital en el contexto colombiano. Op,. Cit. Pag4.

4.6 EL ANÁLISIS DE LA EVIDENCIA DIGITAL

La clave de una buena investigación está basada en lo que el investigador perciba del entorno donde se encuentra, al tener el primer contacto con la escena del delito se hace necesario que por intuición recree los todos posibles hechos, como segunda medida se hace necesario que la persona encargada de la manipulación de la evidencia sea conocedora del tema informático y que además de saber sobre el funcionamiento, límites y vulnerabilidad de la información que posiblemente pueda recolectar.

Para adelantar las tareas de análisis se sugiere realizar dos copias de seguridad (Backups) de los medios originales y trabajar sobre tales copias. Así, si se comete un error que altere la información en una de las copias, se pueda minimizar el impacto en la investigación realizando de nuevo un duplicado a partir de la otra copia y no se perderá la validez e integridad de la evidencia[76].

La tarea de recuperación y reconstrucción de la evidencia digital, requiere que se busque eficientemente sobre el contenido de diferentes medios de almacenamiento, con el fin de identificar evidencia relevante. Además, el investigador siempre debe suponer que puede existir información no visible dentro del medio, pero teniendo en cuenta que este no es siempre el caso y que es parte de su labor determinar la realidad en cuanto a este aspecto.

Un gran obstáculo que se puede presentar durante la investigación, es encontrarse con información cifrada, en donde se estaría utilizando la técnica criptográfica, como en el capitulo anterior se explico, en muchos casos sólo será posible tener acceso a ella si se dispone de la contraseña o llave que permite visualizarla. Una vez se ha recuperado o se ha encontrado información que podría ser relevante, es necesario realizar un

[76] Evidencia digital en el contexto colombiano. Op,. Cit. Pag8.

proceso de filtrado que permita extraer la información directamente relacionada con el incidente.

Se debe realizar un procedimiento de limpieza que por un lado conserve la integridad de la información recolectada y que por otro represente en su totalidad el escenario analizado.

Una vez se han descartado los datos que no tienen ninguna relevancia con la investigación, se debe iniciar el proceso de clasificación, comparación e individualización de la evidencia. La clasificación de la evidencia digital, es el proceso por el cual se buscan características que pueden ser utilizadas para describirla en términos generales y distinguirla de especímenes similares. La clasificación de la evidencia digital es útil al reconstruir un delito porque puede proveer detalles adicionales, es decir, cuando se combinan estos detalles pueden guiar al investigador hacia evidencia adicional, e inclusive hacia el mismo sospechoso del hecho en cuestión.

La evidencia digital puede ser clasificada, comparada e individualizada de diferentes maneras, las cuales deben ser utilizadas a criterio del investigador basado en la evidencia que se haya recolectado hasta el momento[77]:

Contenido: Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.

Función: El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente

[77] Ibid,.pag 8.

transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser individualizado por la localización remota a la que transfiere la información.

Características: Los nombres de inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital.

.

Para finalizar, es necesario reconstruir el escenario en el que ocurrieron los hechos a partir de la correlación de los diferentes elementos recolectados como evidencia. Es importante tener en cuenta, en lo posible, información diferente de la evidencia digital al reconstruir la escena.

Una de las características de los delitos informáticos es que la escena del crimen puede estar distribuida en diferentes sistemas con diferentes horarios, que por supuesto, pueden estar localizados físicamente en jurisdicciones diferentes, lo que en muchos casos dificulta y/o termina prematuramente una investigación ya que no es posible tener acceso a evidencia que podría ser clave para conocer el cuándo, cómo, dónde y por qué del incidente.

Para los investigadores, éste es uno de los mayores obstáculos que se presentan al realizar una investigación, adicionalmente, muchos de los delitos de alta tecnología, a pesar de ser cometidos desde sistemas locales, se realizan desde “Cafés Internet”, en los cuales, debido a la falta de regulación, el alto grado de anonimato y la alta actividad que presentan estos sistemas hacen que la evidencia digital que se encuentra en éstos tenga un tiempo de vida muy corto y por consiguiente la investigación solo pueda llegar hasta ese punto[78].

[78] Evidencia digital en el contexto colombiano. Op,. Cit. Pag8.

4.7 PRESENTACIÓN DE LA EVIDENCIA DIGITAL

En el desarrollo de este capítulo hemos podido determinar cuál es el manejo que a través de la informática se le da a la evidencia digital, sin embargo, es necesario convertirla en algo que pueda ser revisado e interpretado en un proceso judicial. Existe en la materia grandes interrogantes acerca de cómo a través de la neutralidad se le puede otorgar validez y eficacia a la evidencia informática, el doctor Cano especialista en la materia especifica que en la mayoría de los casos puede ser apropiado ofrecer 2 posibilidades.

Una de esas posibilidades es llamada de *bajo nivel* en la que se muestra la información tal como es sin ningún tipo de anotación y modificación. Y otra posibilidad es llamada *editada*, en la que se encuentra solo la información relevante y se explica que se hizo con ella y por qué. Con este enfoque, es posible realizar una inspección cruzada en la que la copia de bajo nivel es la encargada de sustentar técnicamente los argumentos presentados en la parte editada y comentada.

"Además es recomendable clasificar la evidencia para su presentación ante los administradores de justicia, identificando si los datos"[79]:

- Verifican los datos y teorías existentes (Evidencia que inculpa).
- Contradicen los datos y teorías existentes (Evidencia que exculpa).
- Muestran signos de manipulaciones para esconder otros datos.

Actualmente la legislación colombiana, no ofrece pautas generales en los códigos de procedimientos sobre cómo debe ser presentada la evidencia recolectada de un sistema de cómputo, lo cual es una de las razones que dificultan condenar las conductas relacionadas con delitos informáticos y/o relacionados con la informática,

[79] Evidencia digital en el contexto colombiano.Op,.cit.pag8.

adicionalmente, el desconocimiento de los aspectos técnicos básicos y del lenguaje utilizado en este tipo de casos por parte de los funcionarios judiciales, dificulta aún más la penalización de estos hechos.

Es por ello se hace necesario suplir todos los vacíos existentes en la legislación penal, puesto que lo único que hace es proporcionar más inseguridad jurídica en los administradores de justicia y con ello enseñarle a la sociedad que la impunibilidad va quedando en el pasado, de igual forma en necesario otorgarle a los investigadores judiciales todas las herramientas jurídicas para que la prueba o evidencia digital hable por si sola en un proceso y que las labores que ellos realizan no sean en vano.

Esto es una tarea conjunta de investigadores, fiscales y jueces de la republica, en donde todos tendrán que tener una formación en derecho informático debido a la necesidad de castigar delitos cometidos por este medio como efectivamente lo propone el legislador, no solo buscando la aplicación de una pena, sino procurando otorgar la adecuada calificación jurídica al delito, de lo contrario se perdería con la funcionabilidad de las sanciones penales.

En lo que refiere al proceso penal que actualmente se encuentra estructurado en Colombia, todavía presenta falencias que no permiten salvaguardar los derechos del individuo. El derecho se ha convertido en un instrumento de transgresiones de garantías constitucionales, por ello la finalidad de esta investigación es sentar un precedente acerca de la importancia que tiene la evidencia digital en los delitos informáticos apartándonos un poco de las demás ramas del derecho, como se pudo ver en el transcurso de la investigación se encontraron bases cimentadas creadas por el legislador pero incompletas en su aplicación.

En el derecho penal a diferencia de las demás ramas del derecho, requiere un estudio minucioso a la hora de darle aplicabilidad a las sanciones consideradas como reprochables en la sociedad, aquí lo que se juega es con la libertad del individuo que va

más haya de obtener el pago de una indemnización, deuda, el reconocimiento de un derecho etc, estamos hablando de el hecho de coartarle a alguien un conjunto de derechos que se desprenden de la *Libertad,* es por ello que en lo que refiere a delitos informáticos el manejo y análisis de la prueba en esencial y principal, con un buen estudio del caso y de la prueba fácilmente se podrán cumplir con los cometido estatales, dejando como anteriormente se recalcó la punibilidad en segundo grado.

CONCLUSIONES

Cuando se habla de delitos informáticos se parte de la base de la elevación a bien jurídico tutelado el derecho a la información, referida al dato informático, o si se quiere al bien jurídico a salvaguardar es la seguridad de la información, teniendo en cuenta que a través de su ataque se pueden vulnerar bienes como la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del Estado, por ello la importancia de protegerlo como lo tutela el derecho penal por su propio valor y por el peligro potencial que encierra.

La propuesta de buenas técnicas para la admisión y valoración de la prueba electrónica, y la incursión de ellas en el sistema jurídico colombiano, tiene como principal ventaja el simple hecho de tener el juez una herramienta legal que le proporcionara seguridad, confiabilidad y certeza a la hora de admitir y valorar la evidencia digital, dejando a un lado los criterios subjetivos de la justicia.

Algunos países han optado por estandarizar los procesos de búsqueda y recolección de evidencia digital como una forma de evitar la improvisación y de guiar a sus funcionarios en procura de poder defender la idoneidad de sus procedimientos en un proceso judicial. Si se certifica el estricto cumplimiento de un estándar se evitaría exponer el fruto de una ardua investigación a las argucias típicas esgrimidas en contra de las pruebas electrónicas. Dichas argucias de valen de la volatilidad y facilidad de alteración de la evidencia digital para poner en duda la verdadera certeza sobre un determinado hecho.

La evidencia digital debe ser cuidadosamente recopilada y manejada, para posteriormente pueda cumplir con los requisitos de admisibilidad en un proceso judicial.

Independiente de una legislación particular, es esencial garantizar la confiabilidad e integridad de la evidencia la cual tiene que cumplir con los parámetros establecidos en la cadena de custodia. Para consumar este propósito es indispensable contar con equipos de atención a incidentes de este tipo, que deberán seguir un procedimiento previamente definido, el cual deberá ser estándar para todos los miembros de un equipo en especial.

Una limitante para el sistema jurídico colombiano consiste en que, a pesar de contar en la actualidad con múltiples normatividades que regulan el nuevo campo de la informática entre los particulares y la actividad estatal, no existe aún conciencia ni cultura sobre la materia.

Los ataques a los sistemas informáticos en nuestro país van creciendo a medida del tiempo es por ello que es de vital importancia que haya una base jurídica para todos los procedimientos que realiza la policía judicial en aras de salvaguardar los derechos posiblemente vulnerados.

La cadena de custodia es la fase fundamental en la investigación penal por tratarse del momento en que se tiene el primer contacto con la prueba y donde existe el deber por parte del investigador judicial de realizar la mejor labor ya que a través de ella podrán descifrar la veracidad de los hechos nacientes del delito.

En el Municipio de Bucaramanga el hurto, la injuria y la calumnia realizados por medio informático, son los delitos que más se cometen diariamente y a los cuales la tecnología les ha otorgado un mecanismo más fácil para cometerlos.

La ley 527 de 1999 que reglamenta la admisibilidad y fuerza probatoria de los mensajes de datos, fue la promotora que hoy en Colombia se puede hablar de que existe otro medio probatorio que se obtiene por medio de la informática.

Para la presentación de la evidencia informática ante un juez de la república, ya sea por parte del abogado defensor o por perito informático, se hace necesario que se dé a entender al administrador de justicia que la evidencia informática esta revertida del principio de mismicidad. Principio que solo se puede obtener mediante el buen manejo de la cadena de custodia.

El procedimiento que se desarrollo en el capítulo IV está comprobado que otorga toda la validez jurídica y material que requiere la prueba o evidencia informática en un proceso penal.

GLOSARIO

- **DELITO** es una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

- **DELITO INFORMATICO** son operaciones ilícitas realizadas por medio de PCs o del Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

- **EVIDENCIA DIGITAL** es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas y especiales, que en determinado caso pueden establecer relación entre un delito y su autor

- **SISTEMAS DE ARCHIVOS NT SYSTEM** se trata de estándares diseñados por cada desarrollador de sistemas operativos, los cuáles indican la forma en que van a ser almacenados los archivos en los dispositivos de almacenamiento masivo (unidades SSD, discos duros, discos ópticos, memorias USB, etc.), así como también la forma en que va a iniciar el sistema operativo (proceso de arranque).

- **PERITAZGO** es el dictamen que se encomienda a una persona que es llamada perito que se encuentra capacitada para realizar este tipo de actividades, para que en materia de su competencia, presente dicho dictamen ante las autoridades judiciales o administrativas, de acuerdo a lo que el logro analizar.

- **MENSAJE DE DATOS** se entenderá como la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax

- **EDI (ELECTRONIC DATA INTERCHANGE)** el intercambio electrónico de datos es la transmisión estructurada de datos entre organizaciones por medios electrónicos. Se usa para transferir documentos electrónicos o datos de negocios de un sistema computacional a otro. El intercambio electrónico de datos puede realizarse en distintos formatos

- **DOCUMENTOS ELECTRONICOS** es la representación idónea capaz de reproducir una cierta manifestación de voluntad, materializada a través de las tecnología de las información, sobre soportes magnéticos, ópticos o similares, que se expresan a través de mensajes digitalizados que requieren de maquinas para ser percibidos y comprendidos por el hombre

- **COMPUTACIÓN FORENSE** es aquel estudio que permite adelantar las revisiones requeridas en medios tecnológicos, para valorar lo que sucedió en los sistemas de computo, y de manera científica explicar lo que pudo ocurrir, siempre basado y hechos y evidencia verificable

- **TECNICAS ANTIFORENSES** son actividades que realizan los intrusos de la Internet para evitar que un forense cualificado pueda llevar su investigación al éxito, con ello logran destruir evidencia o alterar dichos sistemas, para convertir en tediosa la labor de la investigador.

- **TÉCNICAS CRIPTOGRÁFICAS** es una disciplina bien sea aplicada al arte o a la ciencia, que altera las representaciones linguisticas de un mensaje y se utiliza

como medio de protección de información. se utiliza para cifrar o codificar información de manera que sea ininteligible para un probable intruso

- **TECNICAS ESTEGANOGRAFICAS** es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible a través de portador, para que pueda pasar desapercibida

- **CADENA DE CUSTODIA** es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal.

- **IEA (** Información electrónicamente almacenada) es cualquier forma de registro de información y cualquier tipo de escritos, dibujos, gráficos, listados, fotografías, grabaciones de sonido y otra data de compilación de datos, que pueda ser almacenada en cualquier medio que permita obtener la información directamente o, de ser necesarios, con la ayuda de un perito informático

- **SOFWARE** es el equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

- **EQUIPO INFORMATICO** corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

BIBLIOGRAFIA

ACURIO DEL PINO, Santiago. Manual de manejo de evidencias digitales y entornos informáticos informática. Ecuador. 2009.

BERNAL CUELLAR, Jaime Y MONTEALEGRE, Eduardo. El proceso penal. Universidad Externado de Colombia. Bogotá: 1995. 44p.

CAMACHO, Azula. Manual de derecho procesal. Bogotá D.C: editorial Temis.

CANO MARTINEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia. Bogotá: Universidad de los Andes, 2010. 348p.

CARNELUTTI, Francesco. El delito. Editorial Leyer. Bogotá D.C:2005. ISBN 9586906892.pag 8.

CLAUS, Roxin. Derecho penal general. La estructura de la teoría del delito. Editorial Civitas.2ed.España.2003.ISBN 8447009602.

CÓDIGO DE COMERCIO. ed Legis. Bogotá; 2007. Art 826. p. 131.

CODIGO PENAL COLOMBIANO. Editorial Leyer. Bogotá D.C:2010. ISBN 978-958-711-602-1.

CODIGO DE PROCEDIMIENTO PENAL. Editorial Leyer. Bogotá D.C:2010. ISBN 978-958-711-602-1.

CONSTITUCIÓN POLÍTICA DE COLOMBIA. ed Legis. Bogotá; 2007. P.132. ISBN 978-958-653-565-6.

CORTE CONSTITUCIONAL. Sentencia C-662 de junio 8 de 2000, M.P: Magistrado Fabio Morón Díaz.

CORTE SUPREMA DE JUSTICIA. Sala de casación penal. Fallo del 19 de Noviembre de 2006, M.P: Sigifredo Espinosa Pérez.

CUELLO IRIARTE, Gustavo. Derecho probatorio y pruebas penales. Editorial Legis.2008. 728p.ISBN 9586537048.

DEVIS HECHANDIA, Hernando. Teoría general de la prueba judicial. tomo I. editorial Temis, 2002. ISBN 9583503894.

FERRAJOLI, Luigi. Derecho y razón. Teoría del garantismo penal. Editorial Trotta.7ed. ISBN 848164495.

FLORIANAN, Eugenio. De las pruebas penales. Bogotá: Editorial Temis.2002.ISBN 9583503851

GARFINKEL, S. When the virtual is harder than real. Security challenges machine based computing environments. Department of computer science Stanford University. Citado por Jeimy Cano.p 341.

Harris, R. Arriving at anti-forensics consensus: examining how to define and control the anti-forensics problem. Digital investigation.p. 44-49. Citado por Jeimy Cano.p.340.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Normas Colombianas para la presentación de

Trabajos de investigación. Segunda actualización. Santafé de Bogotá D.C: ICONTEC, 1996. 126p. NTC 1307.

JACKOBS, Gunther. Strafrechtt Allgeimeiner Teil, Berlin, 1983, pags. 34 y 36, citado por Velasquez.

JAUCHEN, Eduardo. Tratado de la prueba en materia penal. Argentina: 2004.Rubinzal editores. ISBN 9507273700.

KENNEDY, “investigating digital crime”, en R.Bryant, investigating digital crime, England, Wiley, 2008, p.52.

LEY 1273 DE 2009.Proteccion de la información y de los datos.

MARQUEZ ESCOBAR, Carlos Pablo. El delito informático. La información y la comunicación en la esfera penal. Bogotá D.C: editorial Leyer. ISBN 9586903907.

MUÑOZ CONDE, Francisco. Teoría general del delito. Bogotá D.C:2ed.2008. ISBN 9789583502064.

PARRA QUIJANO, Jairo. Tratado de la prueba judicial. Tomo I. Bogotá, librería del profesional, 5ed, 1996. ISBN 9582501.

Revista de Derecho, Comunicaciones y Nuevas Tecnologías. 5 ed. p.88.

ROXIN, Claus. Derecho Penal parte general. 2 ed. Civitas. Bogotá.

SENTENCIA C-396/2007 Corte constitucional, Magistrado Ponente: Marco Gerardo Monroy Cabra.

SENTENCIA del 19 de Noviembre de 2006, magistrado ponente: Sigifredo Espinosa Perez.

VASQUEZ, Fernando. Manual de derecho penal. Bogotá D.C: 2002. ISBN 9583503665.

VON LISZT, Franz. La teoría final del derecho penal. 1881.

ZAFFARONI, Eugenio Raúl. Manual de derecho penal. México D.F: 4ed.1988.ISBN 9684011296.

CTI. Cuerpo técnico de Investigación de la Fiscalía General de La nación. Colombia.

http://www.elprisma.com/apuntes/derecho/escuelaspensamientopenal. Consultado el 24 Julio de 2011

http://jbpenalgeneral.blogspot.com/2011/01/14-dispositivos-amplificadores-del-tipo.html. Consultado el 05 de julio de 2011.

http://www.robertexto.com/archivo/penal_uribe_amplif_tipo.htm. Consultado el 20 de Octubre de 2011.

http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/seis.htm

LA PRUEBA EN EL SISTEMA PENAL ACUSATORIO, cap. 7. Disponible En:http://www.fiu.co/fiu/dp/cdinteractivo/manuales/y/formatos/modulopruebas.pdf. Consultado el 3 de Mayo de 2011.

United State sentencing Comission[acceso el 12 de junio de 2008] disponible en: http//www.ussc.gov/publicat/cmptfrd.pdf.

Kennedy, I., “investigating digital crime”, En R.Bryant, investigating digital crime, England, Wiley, 2008, p. 52.

http://www.slideshare.net/cxocommunity/manual-de, Consultado el 05 de Febrero de 2011.

http://jorgemachicado.blogspot.com/2009/03/concepto-del-iter-criminis-o-fases-de.html. Consultado el 05 de Febrero de 2011.

http://www.elespectador.com/noticias/judicial/articulo195183-denuncian-ilegalidad-captura-de-nicolas-castro. Consulado el 06 de Febrero de 2011.

http://www.alfa-redi.org/rdi-articulo.shtml?x=9608. Consultado el 13 de Febrero de 2011.