UNIVERSIDAD DE PAMPLONA

HERRAMIENTAS VIRTUALES Y LOS DELITOS INFORMÁTICOS EN LOS PROCESOS JUDICIALES EN SAN JOSÉ DE CÚCUTA

Rocío de Belén Contreras Manrique
Juvenal Valero Bencardino
José Vicente Carvajal Sandoval
Luz Marina Espinosa Bohórquez
Liliana Contreras Manrique

HERRAMIENTAS VIRTUALES Y LOS DELITOS INFORMÁTICOS EN LOS PROCESOS JUDICIALES EN SAN JOSÉ DE CÚCUTA

Herramientas virtuales y los delitos informáticos en los procesos judiciales en San José de Cúcuta/ Rocío de Belén Contreras Manrique, Juvenal Valero Bencardino, José Vicente Carvajal Sandoval, Luz Marina Espinosa Bohórquez, Liliana Contreras Manrique -- Pamplona: Universidad de Pamplona. 2025.

217 p; 17 cm x 24 cm
ISBN (Digital): 978-628-7656-61-1

Sede Principal Pamplona, Km 1 Vía Bucaramanga-
Ciudad Universitaria. Norte de Santander, Colombia.
www.unipamplona.edu.co
Teléfono: 6075685303

Herramientas virtuales y los delitos informáticos en los procesos judiciales en San José de Cúcuta

Rocío de Belén Contreras Manrique
Juvenal Valero Bencardino
José Vicente Carvajal Sandoval
Luz Marina Espinosa Bohórquez
Liliana Contreras Manrique

ISBN (digital): 978-628-7656-61-1
DOI: https://doi.org/10.24054/seu.114
Primera edición mayo de 2025
Colección Ciencias Sociales y Humanas

Rector: Ivaldo Torres Chávez Ph.D
Vicerrector de Investigaciones: Aldo Pardo García Ph.D

Corrección de estilo: Andrea del Pilar Durán Jaimes
Diseño y diagramación: Laura Angelica Buitrago Quintero

HERRAMIENTAS VIRTUALES Y LOS DELITOS INFORMÁTICOS EN LOS PROCESOS JUDICIALES EN SAN JOSÉ DE CÚCUTA

Rocío de Belén Contreras Manrique
Juvenal Valero Bencardino
José Vicente Carvajal Sandoval
Luz Marina Espinosa Bohórquez
Liliana Contreras Manrique

Formando nuevas generaciones con sello de excelencia comprometidos con la transformación social de las regiones y un país en paz

SELLO EDITORIAL
UNIVERSIDAD DE PAMPLONA

Vicerrectoría de INVESTIGACIONES UNIPAMPLONA

PRÓLOGO

El presente libro está orientado en el tema de investigación especial sobre las herramientas virtuales y los delitos informáticos en las actuaciones penales y del derecho de familia en el circuito judicial de Cúcuta, se procura ahora, condensar la categoría delictual haciendo énfasis en el peritaje informático como debate jurídico – probatorio y su implementación en los estrados judiciales; esto por medio de la interacción interdisciplinaria, al tratarse de diferentes ramas del Derecho. El derecho informático y la informática jurídica surgen a nivel internacional y nacional debido a las nuevas tecnologías emanadas de los medios electrónicos; partiendo su origen en la evidencia digital adquirida a través de la información que navega como comercio electrónico y a su vez de las telecomunicaciones presentes en el ciberespacio.

Se indagó en la jurisprudencia nacional, en la legislación vigente y en las decisiones judiciales del circuito judicial de Cúcuta con relación a las áreas del Derecho mencionadas, sobre la presentación, producción e incorporación de la prueba pericial e informática en los procesos penales y de familia, con miras de observar la celebración de audiencias de juicio oral, donde se ventile dentro del debate probatorio la prueba pericial regulada en la Ley 906 de 2004 o Código de Procedimiento Penal del nuevo sistema penal acusatorio, del mismo modo en la Ley 2213 de 2022, la cual implementó las nuevas tecnologías de la información y las comunicaciones en las actuaciones judiciales en todas las ramas del Derecho, en consecuencia a la pandemia COVID 19.

Por lo tanto, se realizó un breve análisis del documento CONPES 3854 de 2016 del Departamento Nacional de Planeación, siendo este pertinente ya que versa sobre la seguridad y entorno digital debido al creciente uso en las actividades económicas y sociales, asimismo de la Política Nacional de Seguridad Digital CONPES

3995 de 2020 del Departamento Nacional de Planeación, la cual tiene por objetivo desarrollar confianza digital y mejorar la seguridad digital, con la finalidad de convertir a Colombia en un país competente en este ámbito.

Las leyes que tipifican las conductas punibles que atentan o vulneran la información y los mensajes de datos, fungen como bases para la implementación de las nuevas tecnologías como herramienta auxiliar a la justicia a través de la prueba pericial informática, lo cual se explicará posteriormente al analizar la jurisprudencia de la Corte Constitucional relacionada a los delitos informáticos.

Conforme a lo anterior, consultadas sentencias relacionadas con los delitos informáticos y la aplicación de las nuevas tecnologías en el ámbito jurídico, es indispensable mencionar que estas se originaron con la Ley 1273 del 2009, posterior a esto, se pueden encontrar las primeras decisiones enfiladas en la protección de la información y los mensajes de datos, resaltándose la sentencia C-662 del 2000 de la Corte Suprema de Justicia, la cual menciona lo siguiente: "Los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley. (Corte Suprema de Justicia, Sentencia C-662/00, 2000, s/p)"

Por consiguiente, la corte se refiere a la seguridad de la información plasmada en un documento escrito, su validez y absoluta credibilidad en lo escritural; sin embargo, enuncia en su providencia, la protección de los datos cuando técnicamente sean producidos, elaborados o enviados por los medios electrónicos, constituyendo la base primaria de nuestro objetivo para llegar a los mecanismos de intervención de peritos informáticos en las pruebas forenses practicadas en el circuito judicial de Cúcuta con relación al área penal y de familia.

Respecto al surgimiento de los TICS, la Corte Constitucional analizó un tema con similar sentido jurídico en cuanto a los primeros orígenes de la informática, para llegar al tratamiento de la información y de los datos, esto se encuentra consagrado en la Ley 527 de 1999, “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”. Escrito relevante que se convertirá en una guía práctica y de consulta para los profesionales, estudiantes o cualquier ciudadano colombiano que esté interesado en conocer sobre las nuevas tecnologías, sus responsabilidades, deberes, derechos y libertades, puesto que aunque no es una normatividad actual, permite inferir que la informática ha estado presente en el Derecho desde tiempo atrás, y que la prueba pericial informática no es un tema nuevo para nuestro ordenamiento jurídico, pero sí de suma relevancia para ser investigado y brindar información a la comunidad, ya sea académica, estudiantil o social.

PREFACIO

El Derecho y la Ingeniería de Sistemas se unen para analizar la situación experimental de los peritos actuantes en los juicios penales y de derecho de familia desde la óptica del peritaje informático, como técnica probatoria que se ventila en los despachos judiciales. Las pruebas poseen siempre una fuente, una producción o práctica reglamentada en la ley y a su vez, conducen a la convicción del juez sobre la existencia de hechos, conductas o pretensiones para la recta y eficaz administración de justicia.

Los estudiosos del Derecho – en este caso penal y de familia – y los expertos en informática observan que en determinados litigios judiciales se requiere del auxilio a la justicia por parte del perito especializado en las TIC, de la cibernética, o virtualidad, de las redes sociales, del WhatsApp, firmas electrónicas, y en general de todo aquello que requiera a un profesional de la informática para llevar pruebas a un proceso judicial.

Desde hace décadas se da la utilización de la computadora, correos electrónicos, mensajes por teléfonos celulares, o de tabletas y similares, actualmente con la impartición de justicia a través de los medios virtuales como la celebración de audiencias por canales digitales, nos lleva a predicar que el mundo se moderniza y es necesaria la correcta capacitación de los peritos informáticos, para la búsqueda de la verdad o demostración de los hechos fácticos y jurídicos de la Fiscalía frente al imputado o acusado tratándose de un proceso penal, como también de las pretensiones de las partes en conflicto de derecho privado, puntualmente en el derecho de familia, ya que en numerosos eventos involucra personas cobijadas por vulnerabilidad como: niños, adolescentes y mujeres.

La historia enseña que el Derecho ha ido evolucionando conforme a las necesidades de la ciudadanía, pero a su vez,

nos coloca de presente conductas que se encuentran tipificadas en el código penal y comportamientos humanos, que frente al debate propiciado en litigios penales y de familia se desvían de la legalidad, razón por la cual requieren de la ciencia o de la técnica para su demostración y esclarecimiento.

De manera específica en materia penal, los delitos informáticos son tipificados por la legislación y de la misma forma, se reglamenta el medio de conocimiento producido por los expertos en la ley procedimental. En derecho de familia de similar forma, se establece en el Código General del Proceso las exigencias para la presentación, producción y valoración de la prueba pericial. En la informática se tiene cada uno de estos medios y se consagra la técnica o protocolos que son necesarios para su revelación, empero, mediante el Derecho y la Ingeniería, se han de llevar legalmente ante un juez cuando hagan parte del peritaje informático.

En consecuencia, la capacitación de los peritos es de suma importancia en estos momentos de modernidad, de uso y de abuso de los medios informáticos, para coadyuvar el experto con la administración de justicia, llegando a una justicia material y eficaz, ya que sin los peritos especializados dentro de los procesos penales y de derecho de familia que se requieran, no podrá haber verdadera impartición de justicia por cuanto la verdad llegará a medias o de manera deficiente al juez fallador.

La presente ponencia hace referencia a la prueba pericial informática en los despachos judiciales de asuntos penales y de derecho de familia, en cuanto a la necesaria idoneidad de los abogados e ingenieros que podrían fungir como peritos en los debates probatorios que se presenten por delitos informáticos o por elementos probatorios o evidencias que se llegaren a descubrir y producir para la confrontación de la contraparte – Fiscalía – defensor, o en derecho privado, de la parte demandante vs la parte demandada, respectivamente.

Se hace indispensable, como se demostrará en este texto, la adquisición de conocimientos por los peritos que incursionan en

procesos o juicios orales en todas las áreas o competencias para la recta aplicación del derecho y la justicia, como finalidad constitucional regulada mediante la debida actuación procesal y probatoria. La adquisición la podrá obtener el abogado con el aprendizaje del derecho informático y de las enseñanzas técnicas de la ingeniería en este campo; asimismo, lo logrará el ingeniero – de sistemas – mediante conocimientos básicos del mencionado derecho. Conjugación o combinación de conocimientos necesarios para que cumpla el perito informático con todas las obligaciones legales y éticas sobre esta especialización del peritaje informático.

A continuación, los comportamientos tipificados como delitos informáticos, los temas sobre la protección de la información y de los datos, de los atentados informáticos, de la actividad en internet, telecomunicaciones, archivos electrónicos, documentos electrónicos, firma electrónica, entre otros, y su valoración, deberá ventilarse y demostrarse en los estrados de los jueces de familia; todos ellos son conocidos a través de la ingeniería de sistemas, que son los expertos o técnicos en esta materia. Los delitos y sus aspectos legales, sustanciales o procesales, son conocidos por los abogados especialistas en derecho penal, pero la mayoría desconoce de aquellas materias de la ciencia o técnicas de la informática, que dominan sus estudiosos.

Las apreciaciones que esbozaremos sobre el derecho informático y sobre el peritaje informático tienden asimismo, a formular la invitación formal a la comunidad académica a la celebración de la capacitación continua de excelentes profesionales que acudan ante los despachos judiciales mediante informes periciales sustentados en la ética, la ley y la ciencia, que asistan ante los estrados para presentar y soportar técnica o científicamente la opinión pericial informática – en derecho penal o derecho de familia – de acuerdo a las exigencias de los códigos de procedimiento penal y del Código General del Proceso, y la reglamentación expedida para los ingenieros en esta especialidad.

La impartición de justicia es parte de los derechos humanos y derechos fundamentales como garantía del debido proceso y de la prerrogativa material y técnica. Colombia registró en la carta política de 1991, un gran número de derechos y garantías que posee toda persona residente o de paso por nuestro país, dejando en claro que se deben cumplir estos en todos los ámbitos relacionados con la vida humana, especialmente en las nuevas tecnologías, siendo estas uno de los factores que propician el avance y evolución de la sociedad, asegurándose su efectivo respeto, garantía y eficiencia.

Los nuevos textos constitucionales garantizan estos derechos fundamentales que están acordes con las declaraciones de derechos humanos, los derechos del hombre, los tratados internacionales suscritos por Colombia y que hacen parte del bloque de constitucionalidad que poseen supremacía – de acuerdo con el artículo 93 de la constitución: “Los Tratados y Convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción, prevalecen sobre el régimen interno” (República de Colombia, 1991, art.93), es decir, los instrumentos como el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana de Derechos Humanos, Convención de Viena sobre relaciones diplomáticas, las Reglas Mínimas de las Naciones Unidas para la administración de justicia o “Reglas de Mallorca”, entre otros, conducen al respeto de las garantías sustanciales en cuanto al debido proceso, donde encontramos todo lo relacionado con las pruebas y la necesaria vinculación con la informática o las TIC.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS Y FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I

DEL ORDENAMIENTO JURÍDICO

CAPÍTULO I
DEL ORDENAMIENTO JURÍDICO

El derecho penal según, los autores Calvete-León & Garcés-Vásquez (2019). Expresaron el desarrollo histórico; a través de los paradigmas del Derecho, que se han transformado desde el siglo XIX hasta la actualidad. Es relevantes, el paradigma del Derecho en Colombia: la constitucionalización del derecho penal, nuevo Derecho, 15(24), 37-54. es un ordenamiento de normas, que orienta a los individuos o a la sociedad para actuar e interactuar y a su vez respetarlas, cumplirlas que vienen el poder público del Estado, así, la aplicación, las evidencias y las pruebas legalmente que integran el juicio oral, siendo soporte y apoyo para el juez o magistrado los elementos conceptuales a través de herramientas técnicas, en detectar la calidad de delito en el comportamiento, si ocasionó un perjuicio real al bien jurídico tutelado por el legislador y si se ejecutó u ocasionó con dolo, culpa.

Sobre este particular, el paradigma jurisprudencial propuesto por Ferrajoli (2014) resalta el desarrollo de la norma a través de la cultura y las prácticas cotidianas. De tal manera, busca una justicia basada en el acatamiento de los mandatos divinos, reflejando la experiencia histórica del derecho, desde las prácticas cotidianas hasta la época de las codificaciones y la custodia de la información. Es importante reconocer que el derecho constituye un patrimonio de normas sociales, categorías, principios y precedentes judiciales transmitidos por la cultura y la práctica jurisprudencial y doctrinal (Ferrajoli, 2014).

A continuación, el paradigma legalista o páleo-positivista, es reconocido por el estado moderno, como mecanismo para restringir el poder absoluto a través de las leyes, estableciendo una estructura del actuar en el poder como término frente a la libertad de los ciudadanos (Ferrajoli, 2014). Concluyendo

el único criterio de existencia de las normas en su fuente de creación y no hay una correlación entre las normas jurídicas y las normas morales.

Avanzando en el tema, el paradigma constitucional, son normas jerárquicas superior del ordenamiento jurídico, dando transcendencia al origen y validez de otras normas.

Ferrajoli (2012) expuso un paradigma constitucional garantista, entre ellos, lo formal como constitutivo del derecho. Incluye los contenidos de las normas jurídicas, con directrices expuestas de los derechos humanos y un paradigma constitucional principialista. En el segundo orden, paradigma constitucional neoconstitucionalismo por Ferrajoli (2012); sin embargo, su teórica es de una corriente iusnaturalista; permitiendo el Derecho como contenido natural de las personas y las concepciones del derecho moderno. Conforme a ello, Alexy (2017) propuso, en la solución de los conflictos entre principios a través de la ponderación en el análisis argumentativo e interpretativo, en la solución de los conflictos.

Como se mencionó antes, el ordenamiento jurídico colombiano, se hace necesario exponer la sentencia T-406 de 1992, se trazan los lineamientos del estado social de derecho colombiano.

Con la sentencia T-406, la Corte Constitucional (1992) planteó como fin del estado el cumplimiento de los principios y de los valores y el límite de las acciones del estado y directriz de interpretación, en los principios y los derechos fundamentales.

Por esta razón, los valores representan el catálogo axiológico se deriva el objetivo y la finalidad de las normas del ordenamiento jurídico pueden tener consagración explícita o no; lo importante es que sobre ellos se construya el fundamento y la finalidad de la organización política (Corte Constitucional, T 406, 1992). Entre los derechos fundamentales y principios, es coherente y a su vez interactúan con la conectividad entre las normas jurídicas de carácter jerárquica superior (Alexy, 2017).

Los clásicos derechos fundamentales reducen parcialmente el sistema jurídico: la relación entre el Estado y el ciudadano. Por el contrario, los derechos fundamentales, o principios, provienen de causas y efectos en el ordenamiento jurídico con una eficacia expansiva a todos los ámbitos jurídicos, siendo los derechos fundamentales de principal jerarquía dentro del ordenamiento jurídico (Cruz-Palmera, 2021).

La dogmática es un tratado o estudio de los dogmas, conduce objetivamente a la aplicación de las normas y a la interpretación correcta de ellas, interpretación normativa y valorativa de principios.

En el artículo 38 del Código Penal se establece que “las conductas preterintencionales o culposas sólo son punibles en los casos expresamente señalados por la ley” (Barreto, 1999). Por lo tanto, cuando no existe referencia específica a una conducta culposa o preterintencional, se concluye que estas deben evaluarse como dolosas, ya que no se establece otra modalidad de conducta.

1.1 Hechos basados en delitos informáticos

En los aspectos históricos se registró en épocas no muy lejanas se inició la referencia a las conductas delictivas cometidas por medio de tecnología computarizada; en el artículo intitulado “Criminalidad mediante computadoras” publicado en la revista Nuevo Foro Penal número 30 de 1985 (editorial Temis), indica el profesor Tiedemann (1985):

> El desarrollo de la técnica constituye un factor novedoso dentro del polifacético conjunto de factores de la criminalidad económica - social de una colectividad. Así mismo, la introducción y difusión de máquinas en la industria, el comercio y la administración pública, pero sobre todo en el sector de los bancos y seguros, implica, además de una nacionalización y de un progreso, la posibilidad y el medio para la comisión de nuevos hechos punibles. (Tiedemann, 1985, p.1)

Analizando las primeras conductas delictivas, observaron que el citado profesor alemán de la Universidad de Friburgo de Brisgovia, alude a la sistemática de sus modalidades, factores, frecuencia, conocimiento por parte de las autoridades, perjuicios y tipos de autores, considerando la necesidad de la reforma de las disposiciones vigentes de la época (1985), para luego tratar el tema de abuso de "cajeros automáticos". La palabra criminalidad utilizada como comportamientos antijurídicos o socialmente perjudiciales realizados merced de un equipo automático de procesamiento de datos, que abarca el problema de la amenaza a la esfera privada del ciudadano:

> Mediante la acumulación, archivo, asociación y divulgación de datos a través de computadoras; de hecho, hasta el momento en Alemania Federal solo se han conocido pocos casos de violación de derechos personalísimos debido al aprovechamiento abusivo de datos conservados en una computadora. De cualquier forma, el legislador alemán, en la "Ley Federal de Protección de Datos", reforzó la regulación con normas penales poco precisas. Y, por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el uso abusivo de datos procesados automáticamente. (Tiedemann, 1985, p.2)

En consideración trascendental de esta historia académica del profesor alemán, los casos ocurridos como modalidades delictivas, refiriendo a investigaciones efectuadas desde hace diez años por el instituto de criminología y derecho penal económico de la universidad de Friburgo; alude a la automatización de los procesos contables, y al descuido en los aspectos de seguridad de las computadoras, pues el medio bancario ofrece innumerables posibilidades de esta delincuencia y los riesgos se incrementarían si se concretase el proyecto de introducir el sistema de transferencia sin comprobantes.

Estos casos de antaño, de casi cincuenta años, enriquecen el conocimiento de la forma cómo se cometían estas conductas punibles, que hoy se conocen como delitos informáticos.

Señala el Doctor Tiedemann, en el artículo:

> *Se trae a colación un caso también ocurrido al sur de Alemania. El autor era programador sociedad alemana. Sirviéndose de un programa en el que figuraban los datos de los salarios de la empresa, introdujo informaciones sobre sueldos de personas ficticias y cuenta bancaria a la cual debían ser giradas tales remuneraciones; indicó su propia cuenta. Esa manipulación, que podría efectuarse con éxito en numerosas empresas habría sido detectada en la firma afectada, pues la computadora emitía formularios de sueldos, listas de control, resúmenes contables y balances, que eran controlados y evaluados cuidadosamente por la misma empresa.* (Tiedemann, 1985, pp. 2-3).

Al considerar significativo la casuística primigenia sobre las conductas delictivas iniciales mediante la ilícita utilización de las computadoras, que nos servirá más adelante para cotejar con la legislación y la tecnología moderna, destacamos la manipulación de consola ejecutada en el banco privado Herstatt, donde no se informó sobre la computadora de la corporación en cuanto a las múltiples operaciones en divisas, que se evitaron con interrupción para ocultar pérdidas bancarias dando apariencia de normalidad, de esta manera no se registraron altas sumas de dólares americanos.

El profesor recordó los sistemas para el procesamiento de datos operados a distancia que de manera creciente habían sido incorporados para esa época. Tiedemann(1985). En cuanto a las técnicas de manipulación antes descritas, se preguntaba si se puede acceder a la computadora, por ejemplo, a través de la red telefónica mediante una terminal que opera a distancia el autor puede efectuar la manipulación desde su casa con su propia terminal, sin necesidad de introducirse personalmente en la empresa perjudicada.

Referencias comportamentales ilícitas de hace cinco décadas, que llamaron la atención de los estudiosos del Derecho y de la tecnología para vislumbrar a futuro la necesidad de una

codificación actualizada para investigar y juzgar estas conductas especializadas, esto invita a la formación experta de peritos informáticos, máxime cuando la protección de la información, la protección de los datos y la defensa frente a los ataques informáticos se han convertido en una necesidad urgente. A diferencia de los delitos patrimoniales tradicionales, en los que la acción y el efecto suelen ser evidentes y simultáneos, en los delitos cometidos mediante computadoras ambos aspectos se presentan de forma separada. Esta característica dificulta considerablemente el descubrimiento y la investigación del hecho delictivo.

A ello se suma, el efecto continuado de esa forma de delincuencia. Si en la primera ocasión se actúa con éxito, este frecuentemente se vuelve permanente, especialmente en la manipulación de programas y de los llamados “datos básicos”, hasta que se descubre el hecho por casualidad o por un control específico. Y respecto de la personalidad de los autores de estas manipulaciones. En especial las frecuentes manipulaciones del input o del output por parte de empleados técnicos, no suponen conocimientos previos de computación. Por otro lado, el mencionado grupo de jóvenes, quienes por razones casi deportivas intentan penetrar las grandes computadoras comerciales, constituye un nuevo tipo criminológico.

La criminología y el derecho penal cobijaban la necesidad del análisis de las causas del crimen o delito, el estudio del autor o participe de las conductas delictivas y la técnica utilizada por estos. Sin desconocer que, en la actualidad, estas ciencias y técnicas siguen en avance, no solo para tipificar los comportamientos punibles sino para proteger los bienes jurídicos tutelados por el legislador, la protección de los datos, de la que se habla más de cincuenta años, sino también la protección frente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, como el Código Penal Colombiano a estas infracciones penales actualmente.

Al respecto, la dimensión del daño y formas de comisión estudio, El espionaje económico realmente plantea desafíos importantes

en términos de protección de datos y seguridad informática. La facilidad con la que se pueden transferir datos y programas de computación sin autorización representa una amenaza significativa para las empresas y organizaciones que invierten tiempo y recursos en su desarrollo. Es crucial estar al tanto de las medidas de seguridad necesarias para proteger la información confidencial y el know how comercial de una entidad.

De otra parte, el espionaje mediante computadoras no se utilizaba con propósitos económicos por empresas rivales, sino también con finalidades políticas por estados extranjeros. Se tiene igualmente suceso penal ocurrido en Alemania en la década de los 70, cuando se conoció de espionaje por medio de computadoras, obteniéndose informaciones que, en el año 1964, en Berlín se ejecutó un plan para recibir capacitación básica sobre computación con la finalidad de perfeccionar la industria de procesamiento de datos de esta república.

Otra modalidad de esa época de los 70 era el mencionado sabotaje, desde la perspectiva del resultado dañino y el modus operandi, con los cuales se destruían totalmente los programas y los datos con atentados incendiarios, con imanes y programas borradores especialmente elaborados, podía poner en jaque la continuidad de toda una empresa. Por lo tanto, los posibles autores de los sabotajes eran los servicios secretos de otros países, los fanáticos políticos y los empleados deseosos de venganza.

Sobre este particular, conoce de un juicio penal llevado a cabo en Alemania al final de la década de los 70; el ente acusador elevo cargos a un ingeniero por haber borrado comentarios relevantes y programas de archivos de la computadora, acarreando perjuicio económico y colocando en peligro el prestigio de la empresa. El acusado reconoció haber borrado los comentarios referidos al programa, pero en su defensa adujo que lo había hecho para evitar una sobrecarga al disco que contenía el archivo que previamente había grabado los programas con sus comentarios en un cassette; sin embargo, justificó su conducta, señalando que, si la información desapareció con posterioridad a ello, él no

era responsable. Como tal argumento no se pudo controvertir, el acusado fue absuelto el 13 de diciembre de 1979.

Históricamente tuvo repercusión el atentado con explosivos, realizado por miembros revolucionarios en contra del centro de cómputos de las industrias Man, ubicado en Ginsheim-Gustavsburg, como acto de protesta violenta contra el armamentismo y las industrias de armamentos.

Por otra parte, en los Estados Unidos, se conocieron atentados terroristas por la Guerra de Vietnam.

> El sabotaje en la modalidad de criminalidad mediante computadoras y se trató, el hurto de tiempo, que consiste en el uso ilícito de instalaciones de cómputo por los empleados de una empresa o por terceros que acarrean pérdidas cuantiosas, especialmente en cuanto al procesamiento de datos a distancia, efectuando alteraciones de los números de cuentas o facturas. Barrios (1985)

Un ejemplo es el uso en Alemania de los servicios de computadoras del estado por parte de funcionarios que creó dentro de ella, programas de provisión de servicios para computadoras sin autorización y mediante mención falsa del programa cometiendo el delito de abuso de confianza.

El profesor Tiedemann lamentó la legislación de la época de los 70, recabando que no debe sorprender que las normas penales existentes, sólo logren abarcar aquellos comportamientos en forma parcial y más bien casual, aunque con diferentes resultados en los diversos sistemas jurídicos. La instalación indebida de medios de cómputos no está prevista en ninguno de los tipos penales de la normatividad alemana. De tal manera, los actos de sabotaje relacionados con computadoras quedan abarcados por la figura del daño material, no solo el mero perjuicio mecánico sino también a la limitación de su capacidad de funcionamiento. Por consiguiente, borrar información de bandas magnéticas constituye daño, aunque el objeto mismo pueda seguir siendo usado para el fin previsto y lo destruido sea

la información contenida, y aunque la propiedad del objeto no sea el fin específico del hecho.

Del hurto de software, se derivan problemas para el derecho penal y el civil pues, la simple obtención de copias no constituye apropiación como acción del hurto, existiendo consenso en la doctrina acerca de la restringida posibilidad de proteger los programas de computación mediante el derecho de patentes; la controversia se da sobre la protección de los derechos de propiedad intelectual. En cuanto a los programas de computación, la ley refiere a la propiedad de software y debería prohibir igualmente su adquisición mediante aparente argumentación de buena fe por parte de quienes venden estos programas hurtados.

Contra el patrimonio en especial la estafa y el abuso de confianza, así como las falsificaciones de documentos y de reproducciones técnicas.

El tema del abuso de cajeros automáticos en Alemania en la época de los años 70, configuraban delitos de estafa, no aplicándose la ciencia cibernética en el campo bancario por el uso de las tarjetas plásticas para la obtención de dineros en esta clase de cajeros, que fueron utilizadas antes en Estados Unidos, Japón, Francia y Suiza. El uso de las tarjetas sustraídas por personas, la seguridad y protección de la información personal, financiera es fundamental en la sociedad actual, por lo que es necesario contar con leyes y regulaciones que penalicen el uso fraudulento de tarjetas y otros medios de pago. En muchos países, incluida Alemania, existen leyes específicas que sancionan este tipo de comportamientos.

Basados en estas consideraciones, antes de abordar el estudio detallado de los delitos informáticos conforme a la legislación colombiana vigente, haremos referencia a casos ocurridos hace más de 40 años, para luego contrastarlos con el actual Código Penal Colombiano y analizarlos desde el punto de vista típico. En sus inicios, la criminalidad informática se manifestó a través de la comisión de delitos comunes o tradicionales —como la

estafa, el fraude, el hurto, la falsificación documental, la extorsión y el peculado o apropiación indebida de recursos públicos—, empleando las computadoras como medio para su ejecución. Esta casuística evidencia cómo, de manera ilícita, en ciertos casos los ordenadores fueron utilizados para atentar contra bienes jurídicos tanto de la sociedad como de las personas en particular.

De igual modo, la computadora, conformada por circuitos y componentes integrados, constitutivos de una máquina digitalizada al ejecutar comandos en plataformas virtuales para el procesamiento de los expedientes y las pruebas del caso, estando bajo control de un programa o software, fue entonces utilizada para infringir derechos colectivos o particulares, vulnerando la fe pública, el patrimonio público y el patrimonio privado, entre otros.

La historia enseña que en la Segunda Guerra Mundial se utilizó la computadora predispuesta para aplicaciones militares que dio nacimiento a la computadora digital, distinta a las posteriores que estaban conformadas por circuitos integrados. Aquella se llamó ENIAC (Acrónico de Electronic Numerical And Computer) publicitada en 1946; sin dejar pasar lo comentado por Rodrigo Díaz López, cuando reflexionaba sobre los primeros programas de ordenador elaborado en 1843, por Ada Lovelace, para recordar los utilizados como programas militares y tareas ultrasecretas acabada de referenciar, fueron destruidos en los combates. Los artilleros de los Estados Unidos manejaban sus armas, con tablas de tiros que conformaban la dirección o trayectoria que podían eructar los proyectiles calculando la dirección del viento y la ubicación geográfica de impacto.

A continuación, se utilizó la computadora para la ejecución de ataques contra poblaciones y se utilizó en épocas pasadas para la vida delictual en hurtos, estafas, etc. Para llegar a la época moderna a los delitos informáticos y a los ataques cibernéticos.

Según Castaño (2018), la Ley 1273 de 2009 en Colombia representa un esfuerzo significativo para enfrentar los delitos informáticos. Sin embargo, es importante considerar cómo esta legislación se compara con las de otros países. Por lo tanto, resulta vital actualizar y fortalecer las leyes, ya que los delincuentes informáticos desarrollan constantemente nuevas tácticas. La cooperación internacional es esencial, ya que facilita la investigación y el enjuiciamiento de delitos que trascienden fronteras en un mundo interconectado. Además, la educación sobre ciberseguridad y la concienciación pública son igualmente importantes para proteger a los ciudadanos, dado que las leyes, por sí solas, no son suficientes si las personas no están informadas sobre cómo protegerse en el ciberespacio.

Es importante resaltar la existencia del delito informático a nivel organizacional. Los delitos informáticos son sucesos ilícitos que se llevan a cabo mediante el uso inadecuado de la tecnología, afectando la privacidad de los datos y la información de cibernautas, como empresarios o ciudadanos, con el objetivo de extraer o dañar información alojada en servidores o dispositivos. En un estudio, Acosta y Benavides et al. (2020) determinaron que los delitos informáticos y los riesgos afectan a empresas, gobiernos y otros niveles de la sociedad, comprometiendo la seguridad de redes financieras y sociales. Estas acciones antijurídicas, perpetradas a través de medios cibernéticos, tienen la finalidad de destruir, desprestigiar o chantajear a usuarios, ya sean empresarios, organizaciones privadas o estatales, políticos, o entidades religiosas que utilizan las TIC en diferentes plataformas o medios.

A nivel internacional.

Rico-Carrillo (2017) analizó los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. El estudio del ciberdelito vinculado al terrorismo, conocido como ciberterrorismo, exige analizar tanto su impacto como la respuesta de las naciones en materia de defensa cibernética. El ciberterrorismo, especialmente aquel de carácter yihadista en el ciberespacio,

representa una seria amenaza para la seguridad de los países occidentales, al generar daños humanos, sociales y económicos de gran magnitud. Sin embargo, el análisis legislativo por sí solo resulta insuficiente para brindar una defensa efectiva; por ello, la ciberdefensa debe concebirse como un entramado global. En este contexto, es esencial reconocer la función de las leyes y de los sistemas de información modernos, así como la articulación de recursos económicos, sociales y tecnológicos, destinados a proteger tanto a los ciudadanos como a las empresas frente a los ciberdelincuentes.

1.2 Normatividad colombiana: protección de la información y los datos

El Congreso de la República de Colombia promulgó la Ley 1273 del 2009, por medio del cual se modifica el Código Penal, designado de la protección de la información; dicha ley tipificó como delitos en el incorrecto uso de los datos personales en el Código Penal Colombiano, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

En Colombia se recogen en tipos delictivos en las leyes 1273 de 2009 y 1453 de 2011, de manera específica. Derecho y tecnología que como ciencias requieren de profundización y especialización; por tanto, como secuela, la necesidad de preparación y formación de peritos informáticos. Cada uno de los delitos que tipifica el Código Penal Colombiano como protección de la información y de los datos en los artículos 269A a 269G y sus circunstancias de agravación punitiva son conductas punibles que ameritan sanción punitiva. Se tienen, además, el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de comunicación, interceptación de dato informático, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales.

En este sentido, el proceso penal, conforme a lo dispuesto en la Ley 906 de 2004, regula la obtención de información contenida

en dispositivos informáticos con fines investigativos. En este contexto, el fiscal del caso puede emitir una orden para extraer una copia bit a bit de dicha información. Al respecto, Shick y Toro (2017) afirman que:

"El investigador se apoya en el registro que alcance la búsqueda, reconociendo el tipo de pruebas digitales confiables con un laboratorio en informática forense, evitando la modificación de la evidencia digital" (p. 443).

En consonancia, el Código de Procedimiento Penal establece:

El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, las autoridades competentes serán las encargadas de la operación técnica de la interceptación, y del procesamiento para realizarla mediante la orden y los costos serán a cargo de la autoridad que ejecute la interceptación (Ley 906, 2004, art. 235).

A continuación, se dará una breve explicación de cada una de las leyes de delitos informáticos en el Código Penal.

Tabla 1
Ley de delitos informáticos

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Artículo 269ª	Acceso abusivo a un sistema informático	*El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
Artículo 269B	Obstaculización ilegítima de sistema informático	*Sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema y datos informáticos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
Artículo 269C	Interceptación de datos informáticos	*Sin orden judicial previa intercepte datos informáticos provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*
Artículo 269D	Daño informático	*Sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
Artículo 269E	Uso de software malicioso	*El que, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca software malicioso u otros programas de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Artículo 269F	Violación de datos personales	*El que, con provecho propio o de un tercero, obtenga, sustraiga, ofrezca, venda, intercambie, divulgue, modifique o emplee datos personales contenidos en ficheros, archivos, bases de datos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
Artículo 269G	Suplantación de sitios web para capturar datos personales.	*Sin estar facultado para ello programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.*
Artículo 269H	Circunstancia de agravación punitiva	*Quien haya cometido delitos anteriores se aumentará en la mitad de las tres cuartas partes si la conducta o actuación se comete.*
Artículo 269I	Hurto por medios informáticos y semejantes	*El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.*
Artículo 269J	Transferencia no consentida de activos	*El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con*

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
		pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

Fuente: Castaño-Galviz, W. (2018).

1.2.1 Elemento probatorio o evidencia física informática

La evidencia y los medios probatorios son conceptos sencillos de comprender, ya que tienen una connotación especial desde el punto de vista judicial. Estos elementos se deben ser parte de un silogismo, evitando así errores judiciales. Se destaca que las equivocaciones no siempre ocurren en la construcción del silogismo debido a una incorrecta transición de las premisas a la conclusión, sino por una errónea formación de dichas premisas. Según la definición clásica, el silogismo es la forma de razonamiento deductivo que proviene del latín syllogismus y tiene su origen en la lógica griega. Este consta de dos proposiciones como premisas y una tercera como conclusión, siendo esta última una inferencia deductiva derivada necesariamente de las otras dos (Silogismo, 2012).

La vida y la libertad de un hombre puede depender de las reglas de la lógica, la valoración de las pruebas por parte del juez fallador; la evidencia tiene que ver con la valoración en el caso de la prueba pericial y, especialmente, el peritaje informático -con mayor razón- por constituir especialidad por las modernas y complejas tecnologías, se puede incurrir en más errores judiciales. Se debe tener la plena convicción más allá de toda duda razonable para endilgar responsabilidad al autor o partícipe de una conducta punible y para imponerle una pena; sospecha, duda, certeza, evidencia, son las fases del camino que puede conducir a la verdad. No solo es difícil definir la evidencia sino también la certeza, son subjetivas lo mismo que la duda, por esto la técnica cada día ha de ser más perfecta. La teoría de las

pruebas debe buscarse en la ley positiva o sea la ley escrita, pero con mayor extensión en la doctrina de la verdad o sea en las enseñanzas y consecución de la verdad.

De acuerdo con el profesor Brichetti (1973), cuando en su obra “La evidencia en el Derecho Procesal Penal”, ediciones Jurídica Europa América – Buenos Aires 1973 – al decir que: “toda la disciplina procesal está dirigida al descubrimiento de la verdad, sin prescindir ni apartarse de las garantías de la libertad individual y de la seguridad colectiva”. Y no puede ser de otra manera, ya que la obtención de la verdad constituye el término al que tiende toda forma de actividad intelectiva.

Opinión que, resaltó, la importancia de la evidencia, la razón y la justicia en los procesos penales o de la especialidad de derecho de familia, como perspectiva de esta presentación.

En consideración, es evidente y de gran utilidad en materia de la prueba pericial informática presentada por expertos ante el juez o magistrado, para que se obtenga por la concepción que no debe formarse de motivos endebles o superficiales, vagos o indeterminados sino sobre argumentos sólidos de la razón y de la experiencia. He aquí la incorporación probatoria especializada para que se pueda adoptar una determinada decisión en los procesos penales o de derecho privado.

No obstante, se indicó en los elementos materiales probatorios y se estableció en el Código de Procedimiento Penal o Ley 906 de 2004, que:

> “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” (Ley 527, 1999, art. 2).

La regulación colombiana evidencia que la Ley 527 de 1999 no fue la primera norma que trató lo concerniente a colombiana evidencia que la Ley 527 de 1999 no fue la primera norma concerniente a derecho y tecnología. Una labor de “arqueología

jurídica" podría concluir que fue la Ley 8ª de 1970 la pionera en la materia al autorizar en el artículo 7º al presidente de la República para, entre otras, "adoptar las medidas necesarias para generalizar el uso del computador en 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" (Cano, 2010, pp. 3-4).

Luego de la Ley 527 de 1999, la legislación colombiana viene alimentándose con normativas atinentes a las firmas digitales, firmas electrónicas, mensajes de datos, bases de datos, entidades certificadoras, las TICS, protección de datos personales, conductas delictivas informáticas, aspectos disciplinarios y judiciales electrónicos, títulos valores, teletrabajo y contratación electrónicas, facturas y votos electrónicos, últimamente su utilización en las funciones de la administración de justicia.

De igual forma, trae consigo importante relación sobre:

> Los demás elementos materiales similares a los anteriores y que son descubiertos, recogidos y custodiados por el fiscal general o por el fiscal delegado directamente o por conducto de servidores de policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o laboratorios aceptados oficialmente. (Ley 527, 1999, art.271)

En este mismo sentido, existen dos conjuntos de elementos o evidencias que constituyen material probatorio relacionado con el derecho de la información, de las comunicaciones y de la informática en general, los cuales, al provenir de la ejecución o consumación de conductas punibles, deben ser objeto de análisis y valoración por parte de expertos en estas materias. Dicho material comprende, entre otros, mensajes de datos, información proveniente de internet y correos electrónicos. En Colombia, su tratamiento exige una consideración científica y técnica rigurosa, ya que todas las labores realizadas por servidores públicos y

peritos requieren experiencia, idoneidad y capacidad profesional para elaborar los informes correspondientes conforme a la Ley 906 de 2004. Esto debe hacerse en concordancia con las disposiciones legales sobre delitos informáticos, así como con los manuales, reglamentos y directrices de la Fiscalía General de la Nación relativos a la cadena de custodia y a los protocolos para la recolección, presentación, descubrimiento, contradicción e incorporación de evidencias en el ámbito informático.

Ahora bien, el derecho informático es fundamental en el conocimiento y regulación de la sociedad con la información digital. Por lo tanto, el documento electrónico soporta y aporta un carácter representativo o declarativo al proceso judicial con objeto en el juez, sobre la certeza de los hechos enunciados en la demanda o en su contestación. Es relevante destacar un tercer elemento como el mensaje encriptado, es decir, un mensaje cifrado, que debe ser traducido mediante alguna aplicación informática. Al respecto, Gómez-Agudelo (2020) afirmaron:

Los documentos electrónicos en la "prueba electrónica". Otras representaciones como el correo electrónico, SMS (Short Message Service), y los sistemas de video conferencia aplicados a las pruebas testimoniales. Acerca de los SMS, es fácilmente en la comunicación y su empleo habitual en teléfonos móviles, por consiguiente, la aplicación WhatsApp, a través de un software multiplataforma de mensajería instantánea con contenidos de texto, imágenes, video y audio y la localización del usuario (p. 15). De esta manera, se tiene en cuenta el documento almacenado electrónicamente que apoya el proceso judicial correspondiendo al contenido en el medio electrónico original, como valor agregado en el proceso jurídico probatorio, de acuerdo con el artículo 8 de la Ley 527 de la Ley 527 de 1999. Para reconocer, los conceptos de firma digital y firma electrónica.

Delgado (2018). Dictamen pericial en informática, el autor mencionó:

a. El procedimiento establecido en la Ley 906 de 2014 regula la obtención de información para la investigación

> contenida en dispositivos informáticos. En este contexto, el fiscal del caso emite una orden para extraer una copia bit a bit de dicha información. Al respecto, Shick y Toro (2017) afirmaron que este proceso es fundamental para garantizar la integridad y autenticidad de los datos. Las etapas del procedimiento son las siguientes: **a)** obtención de los datos (acceso a la información), **b)** clonado de los datos y cálculo del hash, **c)** elaboración del dictamen, **d)** presentación del dictamen pericial al Tribunal, y e) valoración por el Tribunal (p. 70). Estas fases aseguran que la evidencia digital sea tratada con el debido rigor legal y científico

A su vez, Fernández (2018) expresó: “es importante una ruta y conservar el proceso denominado cadena de custodia, la evidencia tecnológica para garantizar la información desde un origen hasta un fin; incluyendo las firmas electrónicas o códigos hash”.

En este orden de ideas, Gómez-Agudelo sostiene que la evidencia digital debe cumplir con requisitos intrínsecos (autenticidad, integridad, habilidad y disponibilidad) y extrínsecos (legalidad y licitud) para ser apreciada en el proceso judicial. La valoración de la evidencia digital debe realizarse mediante una apreciación conjunta y crítica, sin perjuicio de la facultad del juez. Además, se reconoce el valor probatorio de chats, fotos, videos o correos electrónicos, siempre que se demuestre que no han sido manipulados. Por lo tanto, la normatividad como la jurisprudencia han acreditado la aplicación del principio de equivalencia funcional, el cual establece que el mensaje digital tiene eficacia y validez jurídica y probatoria, asegurando la autenticidad del contenido, la seguridad del emisor y la responsabilidad de la persona que firma el mensaje (Gómez-Agudelo, 2020).

1.3 Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales

En este segmento se analizó la Ley 527 de1999 para entronizar posteriormente, sobre los delitos informáticos, para proseguir con la prueba por expertos en informática.

La ley define, reglamenta el acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación que se aplica a todo tipo de información en forma de mensajes de datos, los cuales definió "La información en los diferentes modos de envíos, almacenada o notificada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax" (Ley 527, 1999, art.2). Se observó tiene relación directa con la enumeración que estableció la Ley 906 de 2004, respecto de los elementos materiales y evidencia físicas probatorias.

La Ley 527 de 1999, alude ampliamente al comercio digital y a la firma digital, a las autoridades que certifican esta clase de rúbricas; también al comercio electrónico, intercambio electrónico de datos y al sistema de información utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. Temas netamente digitales que en el ejercicio de la justicia y del Derecho, son considerados como técnicas o sistema especializado. Con fuerza de ley se estableció así mismo que:

> Siguiendo este razonamiento, no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos... Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. (Ley 527, 1999, p.1)

En este sentido, uniendo en solo cuerpo lo técnico y lo jurídico, entrelazándose las previsiones de ley con las digitales. Razón por la cual, a la firma digital el legislador de igual manera le otorga valor probatorio y establece que se entenderá a satisfacción cuando se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación o que el método sea confiable en la generación del mensaje. Son cuestiones técnicas que deben

ejercitarse dentro de las actuaciones judiciales de todas las áreas.

Así, pues, los mensajes de datos serán admisibles como medios de prueba, dice la ley, lo que se concatena con los elementos probatorios del Código de Procedimiento Penal antes enunciados y permiten la trascendencia jurídica de esta clase de documentos y firmas. Por esto, la normativa legal señala, para la ponderación de la prueba en estudio, que se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas, relacionándose esto con la Ley 906 de 2004; conexión que permite la necesidad de analizar en esta parte todo lo relacionado con el delito informático y la prueba pericial.

Cada uno de los delitos que tipica el Código Penal colombiano como protección de la información, de los datos en los artículos 269A a 269G y sus circunstancias de agravación punitiva, son conductas punibles que ameritan sanción punitiva. Se tienen, además, el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de comunicación, interceptación de dato informático, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales.

El tratadista Pabón (2010), enseñó: como efecto del insospechado avance de TIC, ha surgido un nuevo género delictivo denominado precisamente delitos informáticos" (p.9).

Algunos autores a pesar de la diversidad de conductas informáticas delictivas y diversos bienes afectados, por considerar que estos comportamientos se encuentran en otros tipos penales, estiman que la técnica sería armonizar estos delitos y agravarlas por el uso de los sistemas informáticos. De esta manera, aluden a los casos de los delitos patrimoniales contra los derechos de autor,el orden social, económico y la seguridad pública o la intimidad,no estando de acuerdo con la clasificación que se ha dado en el Código Penal a los delitos informáticos.

El Derecho y la tecnología, la informática y el derecho penal se unen para describir de manera abstracta cada comportamiento, máxime si exige conceptos básicos de la informática. Existe la informática como ciencia; también tiene existencia la informática jurídica que, como asignatura aparece en la malla curricular de varias universidades; además,la ley penal colombiana seleccionó la protección de la información y de los atentados informáticos en el Título VII bis del Código Penal para indicar esta especial conformación de delitos.

El Derecho y la tecnología, la informática y el derecho penal se unen para describir de manera abstracta cada comportamiento, máxime si exige conceptos básicos de la informática. Existe la informática como ciencia; también tiene existencia la informática jurídica que, como asignatura aparece en la malla curricular de varias universidades; además,la ley penal colombiana seleccionó la protección de la información y de los atentados informáticos en el Título VII bis del Código Penal para indicar esta especial conformación de delitos, integridad y disponibilidad de los datos y de los sistemas informáticos. En efecto, profesional de la informática que debe tener conocimiento de derecho penal y abogado que ha de conocer del derecho informático o del peritaje informático. Los sistemas informáticos permiten almacenar datos y procesar información.

La estructura central será el procesamiento de la información en el ordenador y los dispositivos pertinentes ya mencionados como herramientas dentro del sistema informático, que han de organizarse para lograr el objetivo buscado por la persona que maneja la máquina o computadora. El sistema informático procesa información de ingreso y obtiene una información como resultado según la clase de ordenador: analógico si el tratamiento se hace por señales eléctricas o digital si es por medio de lenguaje y manejo de alfabeto binario como enseña Chacon (2007), al escribir sobre los sistemas informáticos, estructura y funciones.

La conducta por sí sola es delito de peligro, que ocasiona daño o lesión al bien jurídico tutelado, antes mencionado. Se trata de

un comportamiento objetivo o visible establecido en el acceso al sistema. Es instantáneo en cuanto al acceso y es prolongado en el tiempo o permanente en cuanto al mantenerse el autor del delito dentro del sistema en contra de la voluntad del titular. Si no hay acceso ni se mantiene el autor de manera indebida o ilícita en un sistema informático, no existirá delito. En caso positivo, debe ser antijurídica la conducta típica, cuando de manera efectiva se lesione la privacidad o confidencialidad como objeto de protección. Se requiere, además, que se obre con dolo o intención criminal de causar daño a la prerrogativa jurídica materia de tutela o protección, como son la información y TIC.

El acceso, como lo explicó el tratadista Pabón, antes nombrado, es el mecanismo de extraer información de la memoria de una computadora o de un sistema informático en alguno de sus elementos cinta magnética, disquete o CD ROM (Pabón, 2010).

Lo clasifica en acceso aleatorio, acceso directo, acceso directo a la memoria y acceso remoto, el primero sin intervención temporal; se accede sin necesidad de tener que leer los precedentes o bloque de informaciones referidas a un mismo encabezamiento como, por ejemplo, las relativas a los clientes de un establecimiento de comercio. Tratándose de una base de datos, cada uno de los bloques de información se denomina registro.

Con el acceso directo a la memoria central, se obtiene la lectura o escritura de datos consignados sin necesidad de incursionar en el procesador; la información se traslada a los elementos periféricos mientras que el acceso remoto se obtiene mediante un cable, una línea telefónica o una red. Por lo tanto, los accesos simultáneos son cuando se involucran en la gestión o acción delictiva varias computadoras.

Es actividad delictiva autónoma e independiente de cualquier otra que se prevé como delito en el Código Penal, todo debido a la tecnología -que cada día avanza- para la elaboración de registros por medio de la computación y las bases de datos,

para su conducta o almacenamiento y pueden tener relación con la dignidad humana, la vida ocupacional o profesional o académica, datos de salud de las personas o sus cuentas bancarias o financieras que la ley protege; sin bienes jurídicos con valor o mérito personal o social, que corresponde a derechos constitucionales.

Después de todo, la obstaculización ilegítima del sistema informático o red de telecomunicaciones como delito está descrito en el artículo 269B del Código Penal, conducta que no requiere de resultado material sino por la sola acción se sanciona al autor o partícipe de la obstaculización, por cuanto causa peligro al bien jurídico tutelado por el legislador; disposición penal que es subsidiaria, siempre y cuando no se prevea delito sancionado con pena mayor. El comportamiento ejecuta quién no estando facultado, impida u obstaculice el funcionamiento o el acceso normal a un sistema o los datos informáticos allí contenidos; o a una red de telecomunicaciones que alternativamente podrá ejecutarse. Verbos transitivos mediante los cuales se cumple la acción de impedir u obstaculizar el sistema o la red enunciadas.

Estas redes de comunicación básicamente requieren del hardware y del software y se pueden clasificar en dispositivos de usuario final y dispositivos de red. El primero incluye las computadoras, impresoras, equipo de escáneres y servicios del usuario de la red; el segundo concierne a los elementos que se conectan entre sí, para el intercambio de datos e información.

La interceptación de datos informáticos es otra modalidad delictiva independiente de las anteriores y de otras conductas ilícitas del estatuto penal colombiano, prevista en su artículo 269C y que se ejecuta por cualquier persona que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático o de las emisiones electromagnéticas provenientes de un sistema de esta naturaleza cuando las transporte. la acción que se exige por la norma punible es la interceptación. Se entiende como una actividad, acción o movimiento que objetivamente genera un peligro o daño al bien jurídico tutelado por la ley, en la medida

en que interfiere en la comunicación de datos informáticos, ya sea en su ingreso o en su salida. Se trata de una modalidad asimilable al hurto, no en el sentido tradicional que exige como objeto material una cosa corporal o un bien mueble ajeno, sino en cuanto a la acción de sustracción o apoderamiento de datos pertenecientes a empresas, entidades o personas naturales.

A continuación, los documentos informáticos corresponden a un conjunto de datos como símil de información e informática como ciencia que estudia la técnica, los métodos o procesos sistematizados, con la finalidad de ser almacenados, procesados y trasmitirlos como datos o información. Permite definir a aquellos con palabra naturalmente entendible, de conformar un suceso o evento que se traduce como documento que recibe o ingresa a una máquina computarizada representando entonces, los datos, una información que el programador procesa para la construcción de un resultado. Ese dato permitirá configurar una representación, un símbolo o efigie, que en su conjunto o agrupación puede conducir a un banco de datos sobre determinada materia o determinado tema, que puede ser utilizado por varias personas.

Datos informáticos que son materia de protección legal, como anteriormente se ha destacado; el sistema que trata de evitar los datos personales en las entidades públicas o privadas sean revelados con perjuicio de quien ostenta este derecho, impidiéndose que se vulnere la dignidad humana, honra u honor. Cuando existen datos que se relacionan con los documentos o información conseguidos luego sobre estos, se han entendido como metadatos, resultado de lo producido, concatenados por su contenido, su calidad, disponibilidad y secuencia histórica. Conjunto que permite hacer un inventario de lo conseguido desde el primer suceso o evento, su búsqueda, recuperación, transferencia, evaluación, archivo y conservación, siendo garantía de la real o material y verdadera información inmersa en los datos recopilados.

Esta descripción se encuentra en el artículo 269D de la codificación en estudio, se ejecuta por persona indeterminada

(cualquiera puede realizar la acción) de destruir, eliminar, modificar o suprimir, verbos que en forma alternativa encierran sinonimia, acciones que se dirigen en contra los datos informáticos o del sistema de tratamiento, de información o sus partes o componentes lógicos, elementos que pertenecen al objeto materia de protección legal. Objetos que podrían ser, por ejemplo, las carpetas que crean como usuarios en los que guarda archivos en discos duros o portátiles, conectados a un equipo de almacenamiento de información. De igual manera, el almacenamiento de gráficas, textos, imágenes, grabaciones, entre otros elementos documentales que reciben el daño, se sanciona en el código como delito.

El uso de un software malicioso es una acción tipificada en el artículo 269E de la Ley 599 de 2000 en estudio, tampoco requiere de sujeto activo cualificado o calificado, sino que cualquier persona puede ser el autor o partícipe de esta actividad de uso del programa malicioso: se configura cuando el delincuente origine, negocie, obtenga, destruya, comercialice, envía, indexe, o extraiga del territorio colombiano, software malicioso u otros programas para efectos destructivo. O sea, legalmente se prevén acciones alternativas mediante verbos de acciones que se dirijan voluntariamente al uso del elemento o programa malicioso, no es menester recalcar que este comportamiento se estructura como delito con el uso de software malicioso a sabiendas que lo es, configurándose la intención de su uso con el fin de producir, destruir o consumar alguna de las acciones enumeradas en la disposición punitiva. Nadie usará un elemento dañino por imprudencia o negligencia, se necesita de la consciencia para usar delictivamente un programa de esta condición, iteramos sabiendo que es dañino.

En ese sentido, se puede decir que un software es, el conjunto de programas que permiten a la computadora efectuar labores determinadas. Se habla de dos clases de software, de sistemas operativos y de sistema aplicativo. El primero, es el más relevante para la función de control de un computador y eficacia de los programas que registre. El básico de programación, incide en el funcionamiento del aparato que llamamos hardware:

en un segundo orden, el componente - software – que controla los dispositivos físicos llamados hardware. En sí, aquel elemento está estructurado con programas que podrán ser, por ejemplo, excel, paint, word, etcétera. Utilizando procesadores de palabras como el blog de notas, Microsoft Word, también software de imágenes, contabilidad, comunicación, audio que, al ser alterados mediante los comportamientos señalados en la ley penal, conducen a la comisión de los delitos que estamos describiendo y explicitando.

El hardware y el software constituyen las piezas esenciales de la computadora. La primera como parte física: la CPU (unidad central de procesamiento) con los circuitos, los cables, el teclado, y el software que es la parte que no se nota ni se toca como los programas, los datos y la información recopilada, archivos o documentos. Las funciones de las máquinas computarizadas corresponden a varias unidades: la unidad de la memoria, la unidad de procesamiento y una unidad periférica para el ingreso de datos y los dispositivos de salida para la conectividad con los medios externos. En estas funciones del recibo de datos, su procesamiento y emisión o transmisión a otra máquina, datos o información que quedan almacenados; se tergiversó por quien procuró ingresar al campo de la criminalidad y dio origen a los delitos que ocupan nuestra atención.

Ahora bien, la siguiente conducta, prevista en el artículo 269F, considerando que es una de las de mayor ejecución en el mundo informático actual como delito, es la violación de datos personales que podrá cometer persona indeterminada buscando un provecho propio o en pro de un tercero para obtener, compeler, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear códigos personales contenidos en ficheros, archivos, bases de datos o medios semejantes; provecho que se busca de manera dolosa o proclive en perjuicio de la dignidad humana, la integridad moral, buen nombre, honra o del honor de la víctima.

El autor de la violación de los datos en perjuicio de la víctima tiene como medios, la sustracción o apoderamiento de los

elementos enumerados, con un fin, su utilización o uso posterior ilícito, ilegal o delictivo, que lógicamente merece la sanción de prisión prevista en la norma. Si repasamos los verbos acabados de estipular, veremos que existe multiplicidad de comportamientos que se podrán producir con finalidad de lucro o provecho indebido.

Los datos personales, las imágenes personales o la información que corresponde a la personalidad de cada ser humano (que no sea de carácter público) o pertenece a la intimidad como derecho fundamental según la Constitución Política colombiana que igualmente ampara el Código Penal en varios capítulos, entre ellos, el bien jurídico de la integridad moral con los tipos penales de injuria, calumnia, integridad moral y concretamente la protección de los datos personales. Por lo que antes de la Ley 1273 de 2009, los fiscales y jueces adecuaban ciertas infracciones, sobre todo cuando se divulgaban imágenes o videos de carácter íntimo o erótico en el tipo penal de la injuria por vía de hecho, como injuria por vía de hecho, prevista en el artículo 226 del Código Penal. Las fotos o videos amparados por el derecho a la intimidad se publicaban en redes sociales u otros medios de divulgación masiva y se tomaban como delito menor o de bagatela. Se adecuaban como injuria por vía de hecho como se toman las imputaciones deshonrosas, el insulto verbal, la bofetada, el escupitajo, entre otros.

A pesar del grave perjuicio que se ocasiona con colocar a la luz pública esta clase de fotos o videos, donde además se exigía la querella instaurada solamente por la persona víctima o perjudicada; el autor del comportamiento injurioso no recibía sanción ejemplar y los delitos eran constantes. Hoy se tiene el tipo penal 269F de la violación de datos personales para que corresponda a la tutela o amparo de la intimidad (derecho humano o fundamental) y a su sanción con mayor drasticidad; más cuando se trate de aspectos personales de carácter sexual. Por eso, el ofrecimiento, la compra o la venta de películas o videos de esta naturaleza, también quedan inmersas en el tipo penal y no en una presunta injuria por vía de hecho.

La suplantación de sitios web para capturar datos personales no es de menor gravedad. Según la redacción que hizo el legislador en el artículo 269G del estatuto de los delitos en Colombia, se tipifica cuando el sujeto activo de la conducta con un fin u objeto ilícito y sin estar facultado para ello, ejecute alguna de las siguientes acciones: diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes que son el objeto material del delito; se reitera, con un fin ilícito. Este fin, es el resultado que conscientemente busca el autor o el copartícipe para la suplantación de los sitios Web y lograr capturar datos personales que se encuentren en páginas electrónicas como palabras, gráficas, vínculos o enlaces de redes de conexión entre documentos o evidencias digitales.

El sitio web no es otra cosa que el portal o colección de páginas relacionadas con internet, al cual se accede a través de una URL o portada, que las organiza para el correspondiente tráfico web con sitios de correos electrónicos, noticias, eventos, bolsa de valores, o sitios de archivo, de blog o bitácoras de empresas y comercio electrónico como Facebook, Twitter, Instagram y otros sitios de directorios, juegos, descarga de documentos o información enciclopédica; buscadores como Google y Yahoo.

Para entender la definición de sitio web, es necesario considerar todos los escenarios que ofrece el sistema, son accesibles mediante una conexión a Internet. Asimismo, existen plataformas como los motores de búsqueda que facilitan la localización de páginas específicas, las cuales están escritas en distintos códigos de programación.

Hoy existe facilidad para crear páginas web siendo herramientas que no requieren de mayor experiencia, lográndose diseños, montajes, videos, publicaciones, catálogos de productos, pero todo dentro de la normatividad legal. Al vulnerarse dolosamente un sitio web, la ley penal se inclina por la sanción correspondiente.

Este artículo del Código Penal contiene circunstancia de agravación punitiva cuando el individuo modifica el sistema de resolución y usuario a una IP diferente, que accede a su banco o

a otro sitio personal o de confianza. Hecho de común ocurrencia en la vida bancaria o financiera actual. El legislador quiso con mayor objetividad o claridad, estipular este comportamiento al notar la inducción a error de la víctima mediante el engaño como una especie de estafa, engaño o artificio que se prevé como delito patrimonial y como provecho de cosa mueble ajena.

El estado colombiano hace esfuerzos para la protección de los ciudadanos, sin embargo, los mecanismos han sido insuficientes para controlar a los delincuentes; por lo mismo, consideramos que debe aleccionarse a todos los habitantes para que conozcan de estas acciones delictivas, instauren las correspondientes denuncias y consideramos que el flagelo no ha sido controlado por la falta de expertos o peritos informáticos que lideren estas recomendaciones o investigaciones en favor de los perjudicados. Se utilizan no solo las redes sociales para la ejecución de engaños sino las llamadas telefónicas y la suplantación de sitios Web para la captura de datos personales.

Para los delitos mencionados del 269A al 269G, se prevé un precepto legal que enumera determinadas circunstancias genéricas de agravación punitiva: Si la conducta se cometiere sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero nacionales o extranjeros; cuando se comete el delito por servidor público en ejercicio de sus funciones; aprovechando el autor la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con éste o revelando o dando a conocer el contenido de una información en perjuicio de otro, obteniendo provecho para sí o para otro.

Dentro del contexto que se trae, refirió en este acápite sobre los atentados informáticos como son, el hurto de medios informáticos y semejantes, previsión legal en contra del individuo superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 (hurto simple) manipulando un sistema informático, una red del sistema electrónico, telemático u otro medio semejante o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos. O

sea, es el comportamiento de apropiarse o apoderarse de un bien mueble ajeno como se exige para el hurto simple, pero el legislador conserva la especialidad de las conductas delictivas informáticas, y la describe en el artículo 269 literal I del Código Penal, individual y separado del tipo básico. El delincuente debe superar las medidas de seguridad informáticas para hurtar medios informáticos mediante manipulación de un sistema, red o sistema telemático. Hay traslado del estudio de este delito al de hurto simple sin perder la estructura delictiva el de carácter informático.

La transferencia no consentida de activos es conducta sui géneris enlistada en el artículo 269J: exige del autor o partícipe, ánimo de lucro que es común a los delitos patrimoniales. Se comete el delito mediante la manipulación informática o artificio semejante, o sea, el engaño o subterfugio dirigido a conseguir la transferencia no consentida de cualquier activo es evidente, con perjuicio de otra persona; por ello, se llama en la doctrina “estafa informática” por la inducción al error o a mantener a la víctima en dicho error. Recalca el legislador “siempre que no constituya delito sancionado con pena más grave” (Ley 599, 2000, art.269). Nuevamente, la ley prevé un caso especial informático en cuanto a los medios utilizados para lograr el fin de provecho o lucro (ánimo delictivo). En los medios o instrumentos utilizados para la trasferencia de activos el legislador convierte el delito en un hecho punible especial debido al tráfico de programas computarizados.

La manipulación de equipos terminales móviles es delito descrito en la Ley 1453 de 2011, consignándose acciones ya vistas en la Ley 1273 de 2009 como son la manipulación, reprogramación, remarcación o modificación de servidores, requiriendo un elemento final; en otras palabras, quien ejecute alguna de las acciones delictivas alterando comunicación y buscando efectos lesivos al bien jurídico tantas veces mencionados.

El fundamento del artículo 29 de la Constitución Política de Colombia establece: “Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso” (Constitución, 1991,

art. 29). Ejemplo de lo anterior, Meza. (2017) tuvo en cuenta, el acopio a correos electrónicos la Ley 527 de 1999, se implementó parcialmente el consentimiento informado, esto significa que está en contra el derecho fundamental a la intimidad de los aludidos; seguidamente, el rastreo de computador de una de las partes sin orden de la autoridad penal competente. (p. 98)

La sentencia SU 159 de 2002 de la Corte Constitucional, se refirió a los casos para anular un proceso por violación a garantías fundamentales; señaló que el principio de nulidad solo afecta el acto probatorio, a menos que en el proceso no existan evidencias válidas y precisas que sustenten la sentencia. En este contexto, garantizar que todas las pruebas presentadas sean admisibles y cumplan con los requisitos legales para que puedan influir en la decisión del tribunal.

A continuación, los siguientes autores:

> Abel, X. (2019) dijo:
>
> El mensaje o la conversación digital, se está impugnando, si esta sea ha manipulado, mediante la mutilación, sustitución o añadido de palabras o expresiones. Es distinguido la prueba pericial informática sobre el dispositivo electrónico que intervienen en el proceso de comunicación. (p. 575)

El papel del perito es fundamental que cuente con certificación en manejo de herramientas forenses, y con una experiencia, al momento de establecer la autenticidad de la evidencia digital. Por lo tanto, el autor, Guimaraes (2019) afirmó “El valor del documento electrónico relacionado, con otro medio de prueba, la seguridad y la autenticidad, con estos dos medios se tiene el grado de credibilidad”. (p. 534)

1.4 Las redes sociales

En este sentido, se pronuncian ampliamente los delitos informáticos que vulneran derechos personales y colectivos. Seguidamente se pasa a la percepción de la violencia digital

en las redes sociales que se presenta como ciberacoso: comportamiento frecuente que se estudia en el artículo producido en la alianza Universidad Simón Bolívar y el diario La Opinión de Cúcuta, intitulado “Violencia en las redes”, donde se presenta lo siguiente: Miguel, un joven interesado en la política nacional, publicó en su cuenta de la red social Facebook, a manera de sátira, una caricatura de la diosa Temis -que representa la justicia- con el rostro totalmente tapado con una sábana y a su lado la figura de dos hombres, en cuyo mensaje se lee: Sí, antes se vendaba los ojos, pero ahora se tapa la cara de la vergüenza, criticando a los juristas del país.

En todo caso, en las redes sociales es notoria la violencia en el tema de política, así como la discriminación e injurias; no hay respeto por las ideas sino agresiones que rayan con la vulneración de derechos ajenos que afectan la convivencia ciudadana, hoy protegida mediante la Ley 1801 de 2016, llamado Código Nacional de Policía y bordea el ámbito del derecho penal. Violencia que se nota en los enfrentamientos no solo políticos sino de cultura, opinión o entre estudiantes de escuelas, colegios y universidades; cuando se ridiculiza u ofende a las personas en su dignidad humana.

¿Quién responde por la afectación de los derechos de imagen y buen nombre en las redes sociales? En efecto, se pregunta González (2020), en publicación que hace el periódico Ámbito Jurídico en nuestra patria colombiana, quien dice: Sin que sea el derecho comparado el asunto de este artículo, la responsabilidad de los llamados “intermediarios tecnológicos” está definida -por lo menos normativamente- desde el año 2000, en la directiva europea y, desde el 2002, en la normativa española denominada ‘Ley de servicios de la sociedad de la información’. Vacío que se acaba de resaltar, siendo más un lamento frente a la falta de capacitación, seminarios o talleres sobre este tema específico de la afectación en redes sociales de los derechos humanos o fundamentales, que continuamente vemos en nuestra tierra:

> Determinando, la responsabilidad de las redes sociales o del administrador de un blog cuando a través suyo se

> vulneran derechos constitucionales, como a la propia imagen y al buen nombre, es un tema cotidiano. De hecho, podría afirmarse que, actualmente, la difamación solo logra su cometido si se viraliza a través de intermediarios tecnológicos. (González, 2000, p.1)

La regulación de esta materia, que describa y sancione esta clase de violencia, cuando ingresa en el campo personal, honroso u honorífico, es necesaria.

Urueña Centeno (2015) “el ataque se desarrollaría desde cualquier lugar del mundo, ofreciendo ventajas en el ciberdelincuente”. Por lo tanto, se sienten seguros en que su acción delictiva se ejecuta a distancia; con impunidad, cuya función la realiza en el anonimato de sus ciberacciones y la falta de protección individual. De esta manera, el delito informático o es una acción ilegal que implementa la informática para destruir y dañar ordenadores, medios electrónicos y redes de internet”, a través de los abusos informáticos. Se resaltó, el ciberterrorismo entre el ciberespacio y el terrorismo, para conseguir sus fines, de intimidación, atemorizar y causar daño a sus víctimas.

Chicharro-Lázaro (2013) definió ciberterrorismo como “el uso de las nuevas tecnologías con fines terroristas” para hacer daños, con ataques de cualquier tipo contra equipos informáticos, redes o información contra los sistemas individuales y de redes, a través de las siguientes actividades: servirse de internet para su propaganda, incitación, amenazas, proselitismo, financiar sus ataques y reclutar a nuevos simpatizantes en servir a la causa terrorista.

En este sentido, Ruiz-Díaz (2016), identificó en el nuevo espacio virtual, donde se cometen determinados delitos, a través de los grupos delictivos tipificados en la legislación española entre ciberdelincuencia.

Por otro lado, Toro-Álvarez (2023) analizó el proceso de judicialización y sentencia en los casos de violación de la ley, centrándose especialmente en los delitos cibernéticos

que involucran material de abuso sexual infantil (MASI). A través del estudio de casos documentados en la legislación estadounidense, es posible identificar diferencias significativas en la manera en que se aborda este tipo de delito en comparación con otras jurisdicciones. En Estados Unidos, el marco legal para la persecución de delitos relacionados con MASI es robusto, destacando leyes federales como el *Child Pornography Prevention Act y el Protect Our Children Act*. Estos marcos legales permiten la implementación de sanciones severas y la utilización de tecnologías avanzadas para la identificación y captura de delincuentes. Además, se hace énfasis en la cooperación internacional para abordar la naturaleza global del cibercrimen. (Toro-Álvarez, 2023).

Este análisis revela no solo las complejidades del proceso judicial en casos de MASI, sino también la necesidad urgente de una mayor armonización legal y cooperación internacional para enfrentar estos delitos que trascienden fronteras.

Choi et al. (2022) indican que estos procedimientos requieren técnicas de investigación para identificarlos e individualizar a los delincuentes en línea, lo cual representa una dificultad en el sistema de justicia penal. Holt, T.J., y colaboradores (2015) afirmaron que esta dificultad se presenta en los escenarios digitales, donde los delincuentes pueden usar técnicas de sigilo para disfrazar su identidad y ubicación a través de ciertos navegadores de internet y redes sociales.

Los autores Steinmetz, et al. (2019) destacan que el ciberdelincuente realizó el crimen organizado o individual para evadir la detección y amplificar del delito. Los autores Cascavilla et al., (2021), mencionaron la agilidad que tiene el ciberdelincuente en cambiar el nombre del usuario y su ubicación en el contexto geográfico, facilitando el cambio de identidad y utiliza diferentes direcciones IP (identificadores lógicos definidos por el protocolo de Internet IP) y equipos o conexiones a redes móviles, inalámbricas o cableadas.

Para Dodge y Burruss (2019), el ciberdelincuente incluye una infección de software malicioso o en caso de material de

abuso sexual infantil (MASI), donde las imágenes y videos son expuestos en el ciberespacio teniendo huellas significativas en las víctimas, para ocasionar pérdidas en las empresas, financieras, organizacional, daños a la reputación y afectación al bienestar emocional (Choi & Toro-Álvarez, 2017).

En el estudio de Holt y Bossler (2015), se menciona que la victimización secundaria en el escenario en línea produce daños en las víctimas, siendo un peligro, ya que los datos personales robados circulan en repositorios ilegítimos en el ciberespacio o en línea.

El abuso sexual infantil según Strasburger et al. (2019), señala que el material comprometido puede seguir distribuyéndose y compartiéndose en línea durante años, lo que causa consecuencias devastadoras para las víctimas en términos de pérdida económica, interrupción de la vida cotidiana y daño emocional y psicológico.

Desde este entendimiento, el cibercrimen puede causar un daño masivo, ya que los delincuentes actúan como atacantes en los dispositivos infectados a cada segundo (Akhgar & Brewster, 2016). Este tipo de delito aumenta día a día, impulsado por el anonimato en línea y la reducción en la supervisión, lo que a su vez origina una mayor reincidencia entre los perpetradores (Nadolna & Rudenko, 2021). Por tanto, estos análisis demuestran la habilidad del ciberdelincuente para efectuar robos y daños en cada nivel social; originando, la reflexión en el ciberespacio para la interacción y el cuidado que debe tener el cibernauta.

1.5 El desarrollo del proceso colombiano y la intervención de peritos informáticos

De suma importancia para conocer el desarrollo del proceso colombiano y la intervención de los peritos en la actuación judicial, es la normatividad vigente sobre la prueba pericial. En ella se regula no solo la procedencia de este especial medio de conocimiento, los requisitos que deben cumplir los peritos, la presentación de informes y señalamiento de la base pericial,

sino, además, se reglamenta la rendición del informe pericial, el momento procesal para su presentación por alguna de las partes – Fiscalía o defensa - y especialmente, su tramitación dentro de la audiencia del juicio oral o de debate probatorio.

He aquí la trascendencia de observar y explicar cada norma relativa a la prueba pericial. Se debe indicar primero su procedencia: Es procedente cuando sea necesario efectuar valoraciones que requieran conocimientos científicos, técnicos, artísticos o especializados... Al perito le serán aplicables, en lo que corresponda, las reglas del testimonio.

Se exige que exista la necesidad de llevar a cabo valoraciones por parte del perito con conocimientos científicos, técnicos, artísticos o especializados. La ciencia, la técnica o tecnología y el arte, son parte especial para debates en un juicio oral, que para el caso que corresponde a los delitos informáticos deberá el experto dar luces al debate probatorio para llevar al juez fallador la convicción sobre determinado hecho que se ha considerado por la Fiscalía como conducta punible. Experto en la ciencia de la informática, del derecho informático, de la protección de la información y los datos, de los atentados informáticos, tratados en la ley penal colombiana.

Los peritos son seleccionados o designados por el fiscal general de la Nación o su delegado ante los jueces de la República, tribunales superiores de distrito judicial o la Corte Suprema de Justicia. Peritos oficiales o servidores públicos del Estado que regula la norma siguiente:

> Artículo 406. prestará por expertos calificados que pertenecen a la policía judicial, así como por profesionales del Instituto Nacional de Medicina Legal y Ciencias Forenses. Estas entidades, tanto públicas como privadas, también podrán incluir a particulares especializados en la materia de que se trate, garantizando así que las evaluaciones y análisis realizados cuenten con la experiencia necesaria para contribuir efectivamente al proceso judicial. Esta diversidad en la fuente de peritos permite una mayor

precisión y objetividad en los dictámenes, lo cual es fundamental para el correcto desarrollo de los casos legales.

La policía judicial como auxiliar de la justicia, en este caso del fiscal investigador, posee expertos en varias áreas de la ciencia y de la técnica; ellos son los llamados a dar luces no solo al ente persecutor de la acción penal sino al juez de conocimiento, cuando se presentan en la fase del debate probatorio frente a la defensa del acusado en la audiencia de juicio oral. La Fiscalía con anterioridad, en el escrito de acusación habrá mencionado al funcionario de policía judicial que le servirá de sustento para lograr las pretensiones acusadoras, que reiterará donde se consagra descubrimiento probatorio de la Fiscalía.

El informe pericial corresponde a estudios o análisis hechos por el (los) experto (os) que ha de suscribir dicho informe. Dice la norma que: las investigaciones o los análisis se realizarán por el perito o los peritos, según el caso. El informe será firmado por quienes hubieren intervenido en la parte que les corresponda. Todos los peritos deberán rendir su dictamen bajo la gravedad del juramento.

En las formalidades reguladas en el Código de Procedimiento Penal colombiano para la eficacia de esta clase de prueba, el juez puede limitarla en cuanto a la cantidad de los expertos al señalar la disposición.

No todas las personas podrán ser peritos; la Ley 906 de 2004 indica quiénes tendrán esta calidad, señalando en su artículo 408, que podrán ser peritos:

Las personas con título legalmente reconocido en la respectiva ciencia, técnica o arte, dejando entrever excepción en ciertas circunstancias. Empero, el legislador que amplía este campo, señalando que, a los efectos de la cualificación podrán utilizarse todos los medios de prueba admisibles, incluido el propio testimonio del declarante que se presenta como perito.

Sin embargo, las normas de procedimiento legal, a su vez refieren a las personas que no pueden ser peritos; se restringe en su artículo 409 la presentación (en todo caso) de:

- Los menores de dieciocho (18) años, los interdictos y los enfermos mentales.
- Quienes hayan sido suspendidos en el ejercicio de la respectiva ciencia, técnica o arte, mientras dure la suspensión.
- Los que hayan sido condenados por algún delito, a menos que se encuentren rehabilitados.

Circunstancias lógicas por la inhabilidad de los menores de edad, tratados de manera especial en la Ley 1098 de 2006 – Código de Infancia y Adolescencia – en concordancia con el artículo 33 del Código Penal que alude a los inimputables diciendo que: Los menores de dieciocho (18) años estarán sometidos al Sistema de Responsabilidad Penal Juvenil.

En el supuesto de ejecutar o consumar una conducta delictiva, asimismo, las personas que estén suspendidos en su campo de acción u ocupación, ciencia, técnica o arte, no podrán ejercitar el cargo de peritos; como no puede serlo quien haya sido cobijado por sentencia condenatoria (en firme o ejecutoriada) por cualquier delito (doloso, culposo o preterintencional).

En párrafo precedente se expresó que existen en Colombia expertos que son coadyuvadores de justicia. La Fiscalía cuenta con la policía judicial y también con los peritos del Instituto de Medicina Legal, es decir, el funcionario del Estado está obligado a fungir como perito, pero ante ausencia de ellos, es permitido designar expertos particulares surgiendo la obligación legal para la aceptación del nombramiento a no ser que el nombrado esté cobijado por causales de impedimento legalmente enumeradas en la codificación procesal penal. Señala la normativa 410 que “El nombramiento de perito, tratándose de servidor público, es de forzosa aceptación y ejercicio. Para el particular solo lo será ante falta absoluta de aquellos.

El perito puede declararse impedido de acuerdo con las mismas causales que señala la ley para los jueces, en el caso que no se separe del conocimiento de determinado asunto ejecutado en tal condición, se puede recusar por las partes o intervinientes en el proceso penal. Cuando se declara impedido en la audiencia preparatoria el perito, deberá el juez excluirlo de la obligación de rendir el peritaje.

Dice enseguida la Ley Código de Procedimiento Penal (Ley 906 de 2004), "que podrá declararse impedido el experto excepcionalmente, en la audiencia del juicio oral y público" (p.1), (por cuanto ya ha sido superada la etapa del descubrimiento, enunciación y solicitudes de pruebas para llevar a la audiencia del juicio oral). Audiencia de juzgamiento de obligatoria asistencia de los peritos, para ser interrogados y contra interrogados en relación con los informes periciales que hubiesen rendido. O dentro de ella, para que rindan en dicha audiencia los de debate probatorio, el correspondiente dictamen pericial (artículo 412 ejusdem).

Informes periciales que las partes – Fiscalía y defensa – podrán acudir al debate del juicio oral (413) para ser interrogados y contra interrogados (414), siendo la base de la opinión pericial la esencia del trabajo realizado por todo especialista. Textualmente señala la ley, lo siguiente:

Artículo 415. "Base de la opinión pericial: Toda declaración de perito deberá estar precedida de un informe resumido en donde se exprese la base de la opinión pedida por la parte que propuso la práctica de la prueba" (p.1). Categóricamente indica igualmente la norma que, dicho informe deberá ser puesto en conocimiento de las demás partes al menos con cinco (5) días de anticipación a la celebración de la audiencia pública donde se recibirá la peritación. De la misma manera, sentencia que, en ningún caso, el informe de que trata este artículo será admisible como evidencia, si el perito no declara oralmente en el juicio.

Es necesaria, entonces, la base de la opinión conforme al pedimento de la parte que propuso la prueba pericial. Asimismo,

es obligación de la parte que presentó la prueba poner en conocimiento de las demás partes, al menos cinco días antes de la celebración de la audiencia de debate probatorio, el informe resumido que, por razón legal, debió haberse descubierto en su oportunidad procesal. Esta exigencia implica que, si no se pone en conocimiento de las partes el informe resumido, podrá aplicarse la sanción prevista en el artículo 346 de la misma obra procesal, que establece que los elementos probatorios y la evidencia que deban ser descubiertos y no lo sean, ya sea con o sin orden especí¿ca del juez, no podrán ser aducidos al proceso ni convertirse en prueba, ni practicarse durante el juicio.

Se prevé grave sanción por el incumplimiento del deber de revelación de información durante el procedimiento de descubrimiento de elementos materiales probatorios, de no efectuarse debe imputarse la omisión a la parte – fiscalía o defensa – cuando el experto ha rendido oportunamente su informe pericial. No hacer entrega de este documento a la parte contraria es dejar sin demostración hechos o circunstancias especiales en la ciencia, técnica o arte, quien incumplió la obligación legal se debilita en cuanto a su teoría del caso o pretensión judicial. No descubrir o revelar el informe pericial constituye falencia grave por desconocimiento del claro tener de al menos con cinco (5) días de anticipación a la celebración de la audiencia pública en donde decepcionará la peritación, para hacer la entrega física del informe pericial a la parte contraída. Omisión que en principio de la vigencia del Código de Procedimiento Penal – y todavía – ha frustrado pretensiones acusatorias o defensivas.

Asimismo, el experto tiene prerrogativas para elaborar o llevar a cabo su peritaje accediendo a los elementos materiales según la disposición número 416 que refiere “Los peritos, tanto los que hayan rendido informe, como los que sólo serán interrogados y contra interrogados en la audiencia del juicio oral y público, tendrán acceso a los elementos materiales probatorios y evidencia física a que se refiere el informe pericial o a los que se hará referencia en el interrogatorio”. Derecho a observar o conocer los medios mediante los cuales rendirán

declaración como perito. Declaración que, de igual manera, está reglamentada en cuanto a las preguntas que podrán formular:

- Sobre los antecedentes que acrediten su conocimiento teórico sobre la ciencia, técnica o arte en que es experto.
- Los antecedentes que acrediten su conocimiento en el uso de instrumentos o medios en los cuales es experto.
- Acreditación en su conocimiento práctico en la ciencia, técnica, arte, oficio o afición aplicables.
- Sobre los principios científicos, técnicos o artísticos en los que fundamenta sus verificaciones o análisis y grado de aceptación.
- Sobre los métodos empleados en las investigaciones y análisis relativos al caso.
- Sobre si en sus exámenes o verificaciones utilizó técnicas de orientación, de probabilidad o de certeza.

La corroboración o ratificación de la opinión pericial por otros expertos que declaran también en el mismo juicio, y sobre temas similares a los anteriores:

Para absolver todos los puntos enumerados el experto en ciencia, técnica o arte tiene en todo caso, derecho de consultar documentos, notas escritas y publicaciones con la finalidad de fundamentar y aclarar su respuesta. Garantía procesal y probatoria que ha de informar y explicar la parte a su perito. Se considera, que si se presenta esta clase de omisiones la culpa es de quien descubrió, enunció y solicitó la prueba pericial, que el juez decretó a su favor; negligencia que favorece a la parte contraria, llámese acusado o fiscalía, según de donde provenga la omisión.

Ya se ha recalcado que el interrogatorio lo formula a quién se le ha decretado la producción probatoria, prueba que ha sido decretada por el juez en la audiencia preparatoria del juicio oral y se resalta, que el contra interrogatorio lo realiza la parte contraria. Para este efecto de la confrontación – parte del

derecho constitucional de contradicción – existen también reglas procedimentales para observar en el desarrollo de la audiencia de juzgamiento.

Legislación Colombiana del código general del proceso. El contra interrogatorio del perito se cumplirá observando las siguientes instrucciones:

1. La finalidad del contra interrogatorio es refutar, en todo o en parte, lo que el perito ha informado.
2. En el contra interrogatorio se podrá utilizar cualquier argumento sustentado en principios, técnicas, métodos o recursos acreditados en divulgaciones técnico científicas calificadas, referentes a la materia de controversia (Artículo 418).

Refutación que presentó el experto mediante su declaración ante el juez fallador. Es la contradicción del dictamen del perito, para debilitarlo o lograr la parte contraria que pierda su credibilidad y no convenza o lleve la convicción necesaria al juzgador. Para este efecto probatorio se podrá utilizar argumentos o sustentos técnicos- científicos calificados o reconocidos por la academia o la investigación.

En situaciones como las que se están viviendo, de administración o impartición de justicia, debe acudirse a los medios virtuales y esto opera para cuando el perito no puede asistir a la audiencia de juicio oral a dar su declaración especializada; se permite el audio-video o cualquier sistema de reproducción virtual, o el traslado del funcionario a la residencia o lugar de habitación o trabajo del experto. El legislador de 2004 de la Ley 906 del Código de Procedimiento Penal, vislumbró estos medios que atañen a la tecnología y a la informática. Señala su artículo 419 textualmente lo siguiente; Si el perito estuviera físicamente impedido para concurrir a la audiencia pública donde se practicará la prueba, de no hallarse disponible el sistema de audio-vídeo u otro sistema de reproducción a distancia, ésta se cumplirá en el lugar en que se encuentre, en presencia del juez y de las partes que habrán de interrogarlo".

Ahora bien, la finalidad de las pruebas, en objetivo del peritaje informático es la convicción que adquiere el juez más allá de toda duda razonable sobre los hechos y la responsabilidad del acusado; en consecuencia, importante es la apreciación del operador de justicia siguiendo las pautas marcadas en la normativa que reza:

Artículo 420. Apreciación de la prueba pericial. Para apreciar la prueba pericial, en el juicio oral y público, se tendrá en cuenta la idoneidad técnico-científica y moral del perito, la claridad y exactitud de sus respuestas, su comportamiento al responder, el grado de aceptación de los principios científicos, técnicos o artísticos en que se apoya el perito, los instrumentos utilizados y la consistencia del conjunto de respuestas.

Se resaltó la idoneidad del perito, la cual se adquiere con el conocimiento prolijo de estas técnicas en derecho probatorio con inclinación extendida en cuanto a la informática. Se menciona como virtud o cualidad del perito que declara en la audiencia pública, la moral; la integridad moral como parte de la ausencia de antecedentes penales o disciplinarios, relevándose para la ponderación o mérito del dictamen en el interrogatorio y contra interrogatorio que realizan las partes en el debate correspondiente, respuestas claras y creíbles en lo atinente al objetivo propuesto por el practicante de la prueba. Si la respuesta no se acomoda a la ciencia o a la técnica no llevará convicción al fallador, si las respuestas son vagas o superfluas no conllevará a la certeza que ha de obtener el juez o magistrado. Más grave aún, si la parte contraria le formula preguntas que pueden ser de índole capcioso o sugestivo, mediante las cuales el perito declarante pierde su horizonte, tranquilidad u objetividad, dejando en el ambiente judicial del estrado donde se encuentra específicamente al juez, lagunas o dudas; esa prueba pericial no servirá para sostener fuertemente la teoría del caso de la parte que ha llevado a la audiencia de juicio al presunto perito.

Ha de concluirse entonces que el perito debe ser verdadero experto en la materia, en este caso, de la tecnología de la informática, la información y los datos, en el momento en que

funja como experto a favor de las pretensiones de la fiscalía o de la defensa. El éxito o prosperidad de un asunto penal adelantado por la fiscalía o controvertido por la defensa depende de los medios probatorios presentados, debatidos, incorporados y valorados por el juez en la sentencia de carácter absolutorio o condenatorio.

El perito declarante en juicio podrá expresar hechos, circunstancias modales, temporales o de lugar, que desemboquen el objeto materia del informe pericial, sin estar permitidas valoraciones sobre inimputabilidad o la manera de aplicación del derecho. Su opinión pericial que puede ser expuesta como tesis o criterio moderno o actualizado, ha de atenerse a lo siguiente: para que una opinión pericial referida a aspectos nóveles del conocimiento sea admisible en el juicio, se exigirá como requisito que la base científica o técnica satisfaga al menos uno de los siguientes criterios:

- Que la teoría o técnica subyacente haya sido o pueda llegar a ser verificada.
- La teoría o técnica subyacente haya sido publicada y recibido la crítica de la comunidad académica.
- Que se haya acreditado el nivel de confiabilidad de la técnica científica utilizada en la base de la opinión pericial.
- Que goce de aceptabilidad en la comunidad académica.

La ley colombiana contempla aspectos importantes como el inmediatamente anterior, buscando siempre que las pruebas en este referido (correspondientes a la informática), permitan su valoración por el juez quien es perito de peritos. Se le exige al juez el conocimiento de ciertas ciencias o técnicas medianamente asimilables para que al absolver o condenar al acusado, pueda reflejar la justicia y el derecho impregnados en la sentencia. Sentencia justa, nunca imbuida en el error por desconocimiento o ignorancia; por ello, el perito debe arrojar luz en todo debate, luz que necesita el juez para la aplicación de la Constitución y la ley.

El avance de la tecnología ha transformado acontecimientos en la sociedad, se implementan la evidencia digital, para certificar hechos relevantes en el caso. Toro (2019) la define “Toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado” (p. 30). Por lo tanto, se almacena, en las tablets, computadores, celulares, y que establece en un medio de prueba, presentándose al proceso un chat, foto, video o conversaciones de WhatsApp. En este sentido, se dan por el medio de prueba documental, en la diferente información digital que está compuesta por bytes de información y diferentes al momento de incorporarla, controvertirla y valorarla en el proceso judicial.

1.6 Mensajes de WhatsApp y correos electrónicos

El sistema de mensajería instantánea más utilizada en el mundo es el WhatsApp; es el más común que se conoce y por lo tanto, son elementos materiales probatorios debatidos en los estrados judiciales de nuestro país: el intercambio de mensajes de texto y de voz, ficheros de audio y de voces que se utilizan para demostrar determinadas conversaciones entre determinados interlocutores, pero debe tenerse en cuenta la posibilidad que los mensajes puedan ser manipulados, no sólo a la hora del envío del propio mensaje -como ya ha sido demostrado por los expertos- sino también una vez los mensajes van a su destino o son recibidos, es decir, directamente sobre la base de datos en la que se almacenan los mismos. Éste es el archivo sobre el que debe practicarse la prueba pericial informática cuando se presentan los mensajes de WhatsApp en un procedimiento judicial, por lo que es de vital importancia que dicho fichero permanezca íntegro o, al menos que, si se manipula maliciosamente, esta alteración pueda ser advertida tras un análisis forense por parte de un perito informático.

En materia de la prueba pericial los chats de WhatsApp y los correos electrónicos son recurrentes, pero se llevan ante los estrados judiciales tomándose los trillados pantallazos que al final son debatidos constantemente por los expertos, derrumbando su mérito probatorio. Se requiere la garantía de validez del medio de prueba.

Vita (2020), en su artículo “cómo certificar un chat de WhatsApp para que funcione como prueba en un proceso judicial”, explicó cómo avalar la validez del mensaje de datos, para ello, es necesario garantizar un análisis pericial que certifique no haber sido manipulado. Condición válida para la prueba de delitos, pues en la eventualidad que se quieran denunciar situaciones como, por ejemplo, amenazas recibidas por correo electrónico, donde el material probatorio es virtual, se hace necesaria la certificación digital por las empresas dedicadas a esta función; debido a que hay programas para editar y modificar todo. En otras palabras, quiere decir que un pantallazo de WhatsApp puede dar al juez indicios de que se cometió la conducta, pero solo se admite como prueba si un perito certifica que no ha sido modificado.

El experto sabrá que existen identificadores en los sistemas de información (contraseñas o huellas) que, en caso del chat, debe probarse que proviene de determinado celular. Mensaje que ha de conservarse íntegro o completo para que sea tenido como prueba, esto se hace a través del sistema hash, que es un algoritmo que obtiene del interior del mensaje, un código alfanumérico que cumple las veces de huella y este permite demostrar si la evidencia fue modificada de alguna manera, lo que permite evidenciar si fue modificado o no el mensaje.

Viene al caso el siguiente extracto de providencia del Tribunal Supremo. Sala de lo Penal Sede: Madrid Sección: 1 Nº de Recurso: 2387/2014 Nº de Resolución: 300/2015 Fecha de Resolución: 19/05/2015ª, al decir que: La resolución judicial que presenta, se refiere a un caso específico donde se han presentado como prueba unas conversaciones obtenidas a través de capturas de pantalla de un teléfono móvil. El tribunal ha emitido un fallo al respecto, determinando la naturaleza jurídica de estas pruebas y su admisibilidad en una eventual apelación.

Siguiendo con la posición doctrinal foránea, puede afirmarse que, si el acusado no admite o reconoce ser el autor de determinados mensajes, debe acudirse a la prueba pericial; así lo enseña la sentencia de la audiencia provincial de Madrid número 51/2013

(23 de septiembre) al concluir el informe o dictamen pericial sobre la aseveración fáctica; siendo distinto, cuando el imputado o acusado ha reconocido la evidencia digital como de su autoría.

Las conversaciones por WhatsApp se han convertido en una de las formas más comunes de evidencia en los debates probatorios judiciales. Según Rubio (2014), en su blog publicado el 14 de septiembre de 2014, se destaca la creciente demanda de peritajes informáticos sobre la autenticidad de las conversaciones realizadas a través de esta popular aplicación de mensajería. Además, menciona que este tipo de análisis también se extiende a otras aplicaciones similares, como Line y Telegram.

Para la labor pericial, es fundamental considerar lo siguiente:

Según WhatsApp Inc., la empresa responsable de la aplicación no almacena en sus servidores el contenido de las conversaciones entre los usuarios. Esto implica que ni el fiscal, ni el juez, ni el perito podrán solicitar a la empresa la certificación de dichas conversaciones. Una vez que los mensajes han sido enviados, el usuario que los envió tiene la opción de eliminar la conversación, lo que puede resultar en la ausencia de cualquier rastro. Se hace referencia a los mensajes enviados, a no ser que, en una experticia informática forense, examinación del teléfono móvil, el perito informático los recupere. Esto se complica cuando el móvil ha sido hurtado o extraviado o cuando se suplanta un número telefónico para enviar mensajes. La dificultad probatoria también radica en demostrar qué persona envió los mensajes, requiriéndose entonces la certificación del perito sobre la originalidad o autenticidad de los mensajes, que de acuerdo con la ley deberán estudiarse en conjunto con las pruebas producidas o aportadas en el juicio oral (Rubio, 2014).

La Corte Constitucional y la Corte Suprema de Justicia – Sala de Casación Penal – en múltiples providencias han tratado en materia. Al transcribir apartes de la ley procedimental penal colombiana en un segmento anterior, se hizo referencia al desarrollo del proceso penal con sistema acusatorio, donde a la

Fiscalía le compete como facultad soberana del Estado investigar a los autores o partícipes de conductas punibles; así se señala en el artículo 250 constitucional y en el séptimo principio rector de la Ley 906 de 2004, ente acusador que requiere del auxilio de la policía judicial y de los peritos oficiales como de los expertos del Instituto Nacional de Medicina Legal.

La parte de la defensa del indiciado, imputado o acusado de igual manera, con base en el principio de igualdad de armas o igualdad de oportunidades procesales y probatorias, se ve en la necesidad de acudir al experto o al técnico para sacar avante su teoría defensiva, sus pretensiones de favorecer legalmente a su prohijado. Como se observó en párrafos en precedencia, se presentan varias etapas para la selección, preparación, descubrimiento, enunciación y solicitud probatoria, siendo la producción e incorporación de la prueba pericial el logro final para que su valor o mérito lleve al juzgador a admitir la teoría o argumentación o demostración de lo pedido por la parte, se dictará sentencia absolutoria o fallo de condena al acusado.

Para continuar con aspectos sustanciales de esta clase de medios probatorios, se debe diferenciar entre informe y prueba periciales, lo que se hará de la mano de la Corte Suprema de Justicia colombiana -Sala de casación penal-; el abogado defensor alegaba en el caso llevado ante la Suprema Corte que en el proceso penal se habían desconocido las reglas de producción y apreciación de las pruebas sobre las que se soportó la sentencia de condena del acusado que representaba. Argumentada que no se le reconoció el derecho a la duda. La Honorable Suprema Corte enseña lo concerniente a la aducción o producción, por su importancia trascribiremos in extenso lo siguiente: Toda declaración del perito reza el artículo anteriormente citado (415) deberá estar precedida de un informe resumido en donde exprese la opinión pedida por la parte que propuso la práctica de la prueba. El inciso final del mismo precepto señala que:

> En ningún caso, el informe de que trata este artículo será admisible como evidencia, si el perito no declara oralmente

> en el juicio...citar al perito o peritos que los suscriben, para que concurran a la audiencia del juicio oral y público con el fin de ser interrogados y contra interrogados. (Ley 906, 2004, p.1)

Queda evidenciado entonces, que existe a partir de su regulación legal, una marcada diferencia entre los informes y la prueba periciales, tópico este que fue ampliamente abordado por la Sala en anterior oportunidad, de la siguiente manera:

> La prueba pericial es un acto procesal que normalmente se lleva a cabo en la audiencia del juicio oral, mediante la comparecencia personal del experto o expertos, para salvaguardar los principios de contradicción e inmediación; y se rige por las reglas del testimonio, pues las partes interrogan y contra interrogan a los peritos sobre los temas previamente consignados en el informe. (Ley 906, 2004, art.405)

La finalidad del interrogatorio formulado al perito para que explique su informe, sus notas o conclusiones de manera sencilla o entendible por el juez y las partes, centrándose en la crítica de la prueba pericial en sí y no a la base de opinión, cuando es interrogado o contra interrogado hace que ayude a comprender el tema especializado expuesto en la audiencia.

El tema de la prueba pericial, aplicable a los peritajes informáticos como sustento de nuestro llamar a la capacitación de expertos en esta materia. El aspecto doctrinal expuesto por la Suprema Corte en la decisión en estudio alude al seguimiento de esta línea por parte de la Sala de Casación Penal, al estampar la siguiente consideración: “Por supuesto, la prueba pericial ha de tener lugar en el juicio oral, donde las partes pueden intervenir en el interrogatorio cruzado, sin más limitaciones que las derivadas de la constitución y la ley” (Corte Suprema de Justicia, Casación No. 25920 2007, p.1).

Es trascendental precisar que el perito no está obligado, en ciertas circunstancias a concurrir ante el señor juez, al estrado

judicial, como lo expusimos en el primer aparte sobre las normas que regulan la prueba pericial; si es imposible surge la posibilidad de pedir al juez la asistencia de un nuevo perito, quien examinado el objeto de la prueba verterá su informe en la audiencia de juicio.

De este modo, si, ninguna de estas opciones se hace factible (no se halla disponible el perito para rendir su dictamen y no es posible efectuar otro examen al objeto o fenómeno) estima la Corte por el camino de la excepcionalidad, con un criterio de razonabilidad y ponderación se tenga en cuenta los derechos de las partes; recuérdese, dentro del presupuesto adversarial de igualdad de armas, tanto la fiscalía como la defensa deben presentar este tipo de pruebas para favorecer su teoría del caso y cumplimiento de exigencia legal. El artículo 10 de la Ley 906 de 2004 indica:

> La actuación procesal se desarrollará teniendo en cuenta el respeto a los derechos fundamentales de las personas que intervienen en ella y la necesidad de lograr la eficacia del ejercicio de la justicia. En ella los funcionarios judiciales harán prevalecer el derecho sustancial. (Ley 906, 2004, p.1)

Por lo demás, esta facultad excepcional otorgada a las partes no afecta profundamente los principios de inmediación, contradicción y oralidad, tan caros en la sistemática acusatoria, dado que el experto acude a la audiencia pública ante el juez a exponer su particular visión, acorde con sus conocimientos, pudiendo interrogársele y contra interrogársele al respecto.

Lo fundamental -advierte la Sala- es que el informe o informes contengan elementos suficientes -particularmente, en el campo descriptivo, acerca de lo observado por quien examinó el objeto o fenómeno a evaluar- que permitan al experto citado a la audiencia contar con bases sólidas a fin de explicar adecuadamente qué fue lo verificado, cuáles los métodos y técnicas utilizadas, los resultados arrojados por la experticia y las conclusiones que de ello se pueden extractar.

El informe pericial se rinde por el experto en un documento; puede hacerse en video, grabación u otro método similar, que por ley tienen también la calidad de prueba documental, pero es muy distinto su ropaje o condición porque pertenece a la prueba de expertos en ciencia, técnica o arte, que la matiza como medio probatorio especial de carácter pericial. He aquí la importancia de delimitar o distinguir el documental.

La Sala de Casación Penal enseña “La autenticidad del documento es una calidad o cualificación de esta cuya mayor importancia reluce al ser tomado como ítem de su valoración o asignación de mérito, después que se ha admitido o incorporado formalmente como prueba en la audiencia pública” (Sala de Casación Penal).

El primer método consiste en el reconocimiento de quién lo ha elaborado, manuscrito, firmado. Para el efecto, dicha persona tendría que acudir a la audiencia y aceptar que es el creador del documento, que deberá exhibirse.

El segundo método consiste en el reconocimiento; se puede citar como ejemplo: el fiscal presenta un contrato que pretende hacer valer como prueba de cargo y el acusado admite ser su creador. Este se tendrá como auténtico. (Corte Suprema de Justicia, Acta Nº 289, 2012, parr.3)

Resalta aquí, la diferencia para hacer ver que el informe escrito del perito por sí solo no tendrá valor probatorio hasta tanto no se descubra, enuncie, se solicite en la audiencia preparatoria – que ahora se precisará en cuanto a su trámite – por último, se debata en la audiencia de juzgamiento, se incorpore al caudal probatorio de la fiscalía o de la defensa, según el caso, y al dictar sentencia el juez la pondere con acuerdo a las reglas que con anterioridad hemos detalladamente reiterado. La enseñanza de la Sala dedicada a la casación penal dice: Concluye que así el informe del perito esté contenido en un documento, su carácter es de prueba pericial y en consecuencia el experto debe ser citado al juicio público y oral con la finalidad del interrogatorio y contra interrogatorio, que se convertirá en prueba.

Acorde con lo anotado antes, puede concluirse que sólo pueden ser objeto de apreciación aquellos medios de prueba en cuyo proceso de producción y aducción se respetaron los derechos fundamentales y los requisitos formales que establece la ley como condición de su validez. (Corte Suprema de Justicia, AP965, 2017, p.1).

Significa lo anterior que, las partes del proceso penal fiscalía y defensa, deben estar capacitados para presentar, revelar o descubrir el informe pericial informático o de otra índole, so pena de ser inadmitido, rechazado o excluido por el juez que celebre la audiencia preparatoria. El desconocimiento de alguna de las partes sobre este tema, a pesar de tener dentro del listado de elementos probatorios un excelente o sustentado informe pericial puede llevarla a perder sus pretensiones, pudiéndose llegar a la consumación de una eventual injusticia. No probar la fiscalía su teoría del caso podrá tomarse como falla del servicio de la administración pública del Estado, y no demostrar el defensor su teoría del caso podrá encausar una posible injusticia en perjuicio del acusado, su familia y la sociedad.

No puede perderse de vista por los mencionados ente y particulares que la prueba pericial informática debe seguir el curso que reglamenta la ley procesal penal colombiana para darle el mérito correspondiente, como función que está ligada a la ponderación sobre la tesis expuesta por la fiscalía, si alcanza el grado de certeza y confiabilidad que ofrezca los elementos probatorios.

Si, por el contrario, en el evento en que la defensa ofrezca una teoría del caso –a lo cual no está obligada- debe determinar cuál resulta airosa en ese proceso de confrontación. No en vano se le conoce como el juez de conocimiento. (Corte Suprema de Justicia, Rad.36562, 2012, p.1).

Quien tiene la facultad soberana de la persecución penal – artículo 250 superior o constitucional y 7º del Código de Procedimiento Penal – además, debe establecer y registrar los hechos jurídicamente relevantes en la audiencia de formulación

de imputación, escrito de acusación y audiencia de formulación de acusación. Son exigencias legales que de omitirse el resultado será el antes mencionado. En la audiencia preparatoria las partes deberán argumentar la pertinencia, conducencia y utilidad de cada medio probatorio que pretende producir o practicar en la audiencia de juicio oral, que encaje en la(s) norma(s) penales que describen las conductas delictivas. Resaltándose en distinción entre hechos jurídicamente relevantes, hechos indicadores y medios de prueba.

En todo caso, es de esperarse que, si las partes han preparado suficientemente su caso, deben estar en capacidad de explicar de manera sucinta y clara la relación del medio de prueba con los hechos que integran el "tema de prueba". (Corte Suprema de Justicia, Rad. 51882, 2018, s/p).

Circunstancias que dan especial relieve jurídico y judicial a la prueba pericial en la temática de la presente exposición, al peritaje informático, que se encuentran en las providencias de los falladores como tema del juez, como experto previo las valoraciones científicas, técnicas o artísticas correspondientes.

Es por esta misma razón, por la que los peritos pueden conceptuar sobre la base fáctica de las causas de inimputabilidad (art. 33: inmadurez psicológica, trastorno mental, diversidad sociocultural o estados similares), más nunca sobre la calificación o consecuencia jurídica de estas (art. 421). (Corte Suprema de Justicia, Rad. 57143, 2020, s/p)

La Corte Constitucional en múltiples jurisprudencias ha tratado el tema de la tecnología y las conductas con las que se ha quebrantado mediante estos medios los derechos humanos. Por lo tanto, la Corte ha despachado solicitudes sobre rectificación como requisito de procedibilidad de la acción de amparo frente a los medios de comunicación masiva o comunicaciones convencionales, requisito extensible a otros sistemas de información.

En la sentencia T-263 de 2010, tras definir el requisito de la rectificación previa para la interposición de la acción de tutela, la Corte señaló que la presentación de esta solicitud da lugar a que "el periodista o el medio de comunicación – u otra persona que informe", debido a la amplitud tecnológica que hoy se presenta con recursos como el internet -, tiene el deber de responder si se mantiene o rectifica en sus aseveraciones. (Corte Suprema de Justicia, Sentencia T-593/17, 2017, s/p).

La corporación constitucional afirma en el siguiente caso, que la empresa demandada posee cuenta el poder de manejo sobre la plataforma BLOGGER.COM, pudiendo eliminar blogs, cuando tenga a bien, por vulneración a la política de contenido. La Corte ordenó a Google Inc suprimir blogs, por su contenido anónimo sobre la condición del delito de estafa e imputaciones injuriosas contra el demandante y su empresa.

> Se exhorta al Ministerio de Tecnologías de la Información y las Comunicaciones para que establezca una regulación nacional con miras a lograr la protección de los derechos de los usuarios de Internet, especialmente en lo que tiene que ver con publicaciones que atenten contra el honor de las personas en Internet. (Corte Suprema de Justicia, Sentencia T-063A/17, 2017, s/p)

La población reclusa no pierde ciertos derechos; en este campo señala que corresponde al Estado como garante de prerrogativa a la comunicación e información a los reclusos internos, garantizar la prestación (por su propia mano o a través de terceros) de los servicios requeridos para la comunicación, la vigilancia permanente del buen funcionamiento de los servicios prestados, la implementación progresiva de las nuevas tecnologías que permita facilitar y mejorar el acceso a la comunicación y a la información de los reclusos en el marco de la regulación de estos derechos.

"Por supuesto, tal accesibilidad no puede desconocer las condiciones de seguridad propias de quienes están privados de la libertad" (Corte Suprema de Justicia, Sentencia T-276/17, 2017, s/p).

En consecuencia, la normatividad colombiana mencionó que todo delito o ejecución de este, con valor económico y comercial, es sometido al control de legalidad ante el juez dentro de las 36 horas, seguidamente, a la obtención del elemento de prueba, en resumen y a colación, las TIC, debe ser vigilado incidiendo en la interpretación.

El ciberespacio es transnacional, Suarez-Fonseca (2021), indagó sobre los elementos que afectan como la confiablidad, privacidad, probidad, disponibilidad, habeas data, es decir, el derecho a la libre disposición, inviolabilidad, acopio y transferencia de datos e información digital.

López-Soria (2020) afirmó, es un acto negativo, lesivo, se han venido desarrollado en varias teorías del delito, como el delito; también manifestó que “toda conducta punible supone una acción típica, antijurídica, culpable y que cumple otros eventuales presupuestos de punibilidad”, en Colombia

Según Caro (2021), Roxin destaca que “el elemento de la voluntad es un medio para la teoría subjetiva en la configuración del dominio del hecho”. Esto resalta la importancia de la intención y la voluntad en el análisis del autor sobre cómo se establece la responsabilidad penal.

Castañeda (2017) que “el dolo y la culpa no son elementos de la culpabilidad, pero sí son elementos del tipo penal subjetivo que previamente están establecidos en la norma”; también mencionó, “la reprochabilidad ubica al sujeto en circunstancias que le hacían exigible el comportamiento conforme a le ley, pero no la obedeció”.

CAPÍTULO II
DE LA PRUEBA PERICIAL

CAPÍTULO II
DE LA PRUEBA PERICIAL

El Derecho consigna su opinión sobre los temas contenidos en los códigos Penal y de Procedimiento Penal, que tiene repercusión en otras áreas. Para el presente estudio se extraerán apuntes importantes sobre el tema, el desarrollo y profundización de la prueba pericial, que conduce al peritaje informático en lo que refiere a su presentación, descubrimiento, enunciación, solicitud probatoria, decreto de la práctica de la prueba, su producción e incorporación o introducción como prueba en la audiencia del juicio oral, y por último, la valoración del juez en la sentencia para absolver o condenar al acusado por un delito informático o por otra conducta punible donde intervenga el experto o perito en informática.

Es así, que el perito debe conocer la manera como fundamenta la base de su opinión especializada; sustentará su informe pericial en la vista pública de debate probatorio y absolverá las preguntas que le formulen la parte que lo presenta o quien lo confronta o controvierte. Se ha recabado en este aspecto sustancial para concluir que, el perito debe estar capacitado o ilustrado profundamente sobre esta área del derecho penal y la ingeniería que explica la informática.

Así lo explicó Chiesa y Reyes (2005) quien había manifestado que el experto no puede sustentar su opinión en informes o conclusiones de personas no conocidas o no sustentadas en pruebas o informes de terceros, o en reseñas publicadas por los periódicos.

La doctrina presentada por el maestro del derecho penal de Puerto Rico, Chiesa (2005), aborda una pregunta formulada por la Corte Suprema de Justicia colombiana: “¿Debe concurrir necesariamente el perito que expidió el informe?”. Esta cuestión se convierte en una enseñanza valiosa para el experto en

informática, ya que subraya la importancia de la presencia del perito en las audiencias para explicar y defender su informe, ¿asegurando así la validez y comprensión de su análisis técnico?

Según la ley, en derecho comparado es necesario que la base de opinión pericial sea sustentada con el testimonio del experto o perito que examinó y elaboró el correspondiente informe. El peritaje exige la participación del perito en la audiencia de juicio oral, para que explique las técnicas, exámenes y conclusiones a las que llegó, resultando sin valor probatorio la sola presentación del informe. Es posible que el perito no pueda concurrir a esta sustentación, pudiendo ser otro que no elaboro directamente el informe.

Por consiguiente, La Corte Suprema de Justicia. Sala de Casación Penal. Sentencia del 17 de septiembre de 2008. Radicación 30.214. Estima la Sala, bajo estos mismos presupuestos argumentales, que en casos excepcionales, referidos a la imposibilidad absoluta de que el perito pueda rendir su versión en audiencia pública –ha fallecido, se ignora su paradero, no cuenta ya con facultades mentales para el efecto, solo por vía enunciativa en el ánimo de citar ejemplos pertinentes-, y a la pérdida o desnaturalización del objeto sobre el cual debe realizarse el examen o experticia, es posible que acuda a rendir el peritaje una persona diferente de aquella que elaboró el examen y presentó el informe; la posibilidad de que aún en curso de la audiencia de juicio oral, desde luego, durante la etapa de práctica de pruebas, dada la imposibilidad de que ese perito inicial brinde el testimonio.

Con la presentación, se advierte el riesgo que corre un informe pericial ante posible decisión de inadmisión, rechazo o exclusión en la audiencia preparatoria como se dijo en pasado párrafo, sin embargo, el ser decretado la prueba pericial y ser debatida en juicio oral, no significa que tendrá éxito su contenido o la declaración del perito, ante el ataque o controversia que se presenta en el contra interrogatorio (oportunidad procesal para atacar su credibilidad). Por esto mismo, existe fase de filtración o purificación de los medios de prueba que cada parte

pretende llevar a la audiencia de juzgamiento determinado medio probatorio; donde es trascendental la demostración de la pertinencia, conducencia y utilidad del medio de prueba. De lo contrario, puede ocurrir que la parte contraria solicite la admisión del medio o evidencia probatoria.

En el siguiente extracto de providencia del Tribunal de Medellín, que recrea este evento procedimental, sobre la solicitud de pruebas, la verificación de la pertinencia y conducencia del medio probatorio y para la admisión rechazo o exclusión de ellos, como actos que corresponden exclusivamente a las partes en cada caso, siendo el escenario propicio en la audiencia preparatoria.

“En sentido contrario, no le corresponde al juez asumir ese rol... si las partes al solicitar las pruebas no fundamentan las exigencias de pertinencia, conducencia y utilidad, deberá declararse su inadmisión, rechazo o exclusión” (Tribunal Superior de Medellín, Rad. 2012-19107, 2016, s/p).

Ahora bien, en el caso internacionalmente conocido, ocurrido en territorio ecuatoriano, la Corte Suprema de Justicia colombiana, decretó auto inhibitorio y el archivo de diligencias preliminares seguidas en contra de congresista patrio, indagado por haberse mencionado en computador de un comandante de la FARC, allí ultimado, al tener en cuenta la ilegalidad de la actividad policial que ingresó al país vecino. En el proceso 29877 mediante Resolución de 18 de mayo de 2011, se concluyó, que, ante la exclusión probatoria de los elementos recogidos en la República del Ecuador, no era menester, verificar su autenticidad.

Exclusiones probatorias que se evidencian por la falta de conocimiento de la ley y de las técnicas propias de la informática; a pesar en este último caso, del grado del militar se observa que desconocía los aspectos sustanciales y probatorios para el manejo de la evidencia digital o computacional.

El tratadista español Climent (1999) señala que la prueba pericial ha sido definida como el medio de prueba consistente en la declaración de conocimiento que emite una persona que

no sea sujeto necesario del proceso acerca de los hechos, circunstancias o condiciones personales inherentes al hecho punible, conocidos dentro del proceso y dirigida al fin de la prueba, para la que es necesario poseer determinados conocimientos científicos, artísticos o prácticos.

Igualmente indicó el profesor que, toda peritación supone la realización de diversas actividades que consisten en la descripción del objeto a periciar, la relación de las operaciones técnicas efectuadas y las conclusiones obtenidas o dictamen. Es decir, el acto pericial comprende el reconocimiento o percepción del objeto a periciar, la realización de las necesarias operaciones técnicas o análisis y la deliberación y redacción de conclusiones.

Para la pericia técnica que corresponde a la informática -parangonando al autor- indica, ha quedado sentado que el perito realiza casi siempre una previa labor perceptiva sobre los hechos u objetos con respecto a los cuales ha de emitir su dictamen. El perito es un receptor de la prueba como lo es el juez, pero en su conjunto.

En materia probatoria se califica al juez como perito de peritos; por lo anteriormente expuesto hay una percepción por el perito juntamente con el juez, una percepción asociada, una verificación ocular conjunta en que existen dos receptores de la prueba que actúan juntos: el juez para convertir en percepción propia la explicación técnica del perito y, de otra parte, el juez controla el dictamen pericial cuya ponderación le corresponde al final del juicio.

Con la presente disertación, se propuso la necesidad de la capacitación del perito informático, que se tenga al experto como perito y no como testigo técnico; distinción que ha hecho la Corte Suprema de Justicia colombiana y que explica, además, el profesor español Climent Durán, distinguiendo entre testigo técnico o testigo perito del perito testigo; el primero es quien posee conocimientos especiales y observa un hecho con base en aquellos conocimientos y se le cita a audiencia para que haga referencia a cuanto conozca sobre el mismo, la percepción

es antes del proceso; diferenciándose del perito testigo, pues este conoce un hecho nuevo dentro del proceso, es percepción procesal e interviene en su condición de perito al que se le agrega la calidad de testigo para exponer o sustentar su informe.

Hormiga-Rincón (2020) explica que el testigo técnico participa en el proceso como testigo de los hechos que ha percibido personalmente, pero su testimonio se ve enriquecido por los conocimientos especializados que posee, los cuales le permiten interpretar y percibir de manera más detallada los hechos sobre los que declara.

Entonces, no es igual perito a testigo técnico. Éste último actúa como testigo y aparente condición de perito, pues quien se limita a relatar hechos se convierte en testigo y si se limita a dar información especializada se considera perito. Una cosa es relato de los hechos y otra dar información sobre aspectos que conoce como técnico, que dictaminar sobre una ciencia o arte. El testigo técnico es un testigo más, señala el citado profesor, citando a Fenech (1982). es un testigo cuya utilidad puede ser mayor que la de un testigo vulgar, desprovisto de aquellos conocimientos, especializados pero lo vertido por tal persona tiene el carácter y valor de una declaración (No de dictamen).

Sobre el tópico del testigo técnico se ha pronunciado la Corte, *Sentencia del 11 de abril de (2007)* recalcando, que no se puede confundir la distinción entre testigo perito y testigo técnico pues este posee conocimientos especiales sobre una ciencia u arte, que lo hace especial al momento de narrar hechos que se debaten en el proceso, de acuerdo a la teoría de cada parte, mientras que el testigo perito explica no sobre los hechos sino sobre un tema especializado que debe evaluarse dentro del proceso.

En conclusión:

> Por consiguiente, Asiste la razón al impugnante cuando advierte que el Tribunal incurrió en un error de hecho por falso juicio de existencia por suposición, como quiera

> que, se repite, en el juicio, y ni siquiera en las audiencias anteriores, no existe registro de ese supuesto dictamen. (Corte Suprema de Justicia, Rad. 30214, 2008, s/p)

El testigo estará en condiciones de declarar sobre hechos que percibe de manera directa o personal, que percibió, dándose cumplimiento a la regla que las preguntas formuladas a los testigos que deben versar sobre hechos, no sobre opiniones o apreciaciones personales de los hechos percibidos, de lo contrario el juez debe abstenerse de apoderarlas como fundamento probatorio.

El juez rechazará las preguntas que tiendan a provocar conceptos del declarante que no sean necesarios para precisar o aclarar sus percepciones, excepto cuando se trate de una persona especialmente calificada por sus conocimientos técnicos, científicos o artísticos sobre la materia, conocimiento, habilidad, experiencia, entrenamiento o educación, y que puede, en consecuencia, "fundamentar una opinión en hechos o información del caso que ha sido puesto en conocimiento del experto o que ha observado personalmente" (Corte Suprema de Justicia, Rad. 45711, citado en Díaz y Contreras, 2020, p. 24, 28).

Se define legalmente como firma, como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

La Corte Constitucional en sentencia C-662 de 2000, enunció que la firma está compuesta por un juego de claves, y un certificado digital emitido por las entidades autorizadas para el efecto, habida cuenta que el suscriptor del documento lo firma mediante la introducción de una clave privada, la cual activa un algoritmo que en cripta el mensaje -lo hace ininteligible- y lo envía junto con una copia del certificado digital del mismo por la red de comunicaciones; a su vez, el receptor del mismo para

hacerlo comprensible tiene que activar el algoritmo criptográfico, mediante la introducción de la clave pública del firmante, y si ella está asociada a la primera se producirá la desencriptación.

Por esta técnica considera que el valor y procedimiento en cita, evidentemente requiere de los conocimientos del experto. Según García (2015), en el trabajo fin de máster de la Universidad Carlos III de Madrid, titulado 'Informe sobre el Peritaje Informático' reveló, el listado de medios probatorios se ha ampliado por los avances científicos y tecnológicos, entre ellos los sistemas audiovisuales o medios de producción de la palabra, sonido y de la imagen; los medios soportados en la informática o instrumentos que permiten reproducir o archivar datos o cifras. Indica igualmente que, la ley les diferencia de los medios de prueba documentales, atribuyéndoles una valoración por el juez según las reglas de la sana crítica en lugar de su sometimiento a las reglas de la prueba documental.

Se está totalmente de acuerdo con la enseñanza insertada en el artículo, máximas para interrogar al perito, autoría de Fernández (2020) al resaltar en su post las diferentes reglas o principios aplicables al interrogatorio y contra interrogatorio del perito, debido a las múltiples circunstancias que pueden influir en el buen o mal manejo de las preguntas, debiendo el abogado no prescindir de la técnica.

La experiencia del abogado o del perito que lo asesore para formular preguntas a quien como especialista depone en el juicio oral con debate sobre elementos de la informática, requiere en estos momentos cruciales para el convencimiento del juez de la causa, que el abogado puede conocer bien los hechos, saber el tema y el objeto de la prueba, hasta de las técnicas del interrogatorio, pero al momento de formular las preguntas al perito presentado en la audiencia deberá hacer gala de su especialidad en las lides del derecho informático.

Además, la práctica, la confianza, la disciplina son valiosas en estos momentos, sin embargo, el uso de las preguntas, su secuencia, el control del expositor, el esperar las respuestas

deseadas y la adaptación al tema que propuso el interrogado determinan el éxito probatorio. Conociendo bien al deponente y qué puede causar en la mente del juez con su exposición, podría acreditarlo o desacreditarlo, según el rol del interrogador; el aporte pericial va unido a los factores de credibilidad como la forma de presentarse el perito, de comunicarse de trasmitir, y dar a conocer su experiencia para influir en la decisión del juez, que definitivamente es a quien se debe convencer.

La capacitación del abogado y de su eventual asesor o acompañante a la audiencia de debate probatorio para interrogar o contra interrogar al perito, tiene que ver con lo expuesto en párrafos precedentes. Vital es entonces la idoneidad de los profesionales del Derecho y de la Ingeniería en la labor pericial que se ha venido analizando.

En las exigencias de las normas penales, es relevante, los elementos de prueba que sustenten la objetividad del hecho y la autoría por el procesado, con serie que cumplan requisitos por el legislador. Según Cordero (2021), “un juicio de licitud obteniendo garantías procesales y resaltando los derechos fundamentales, sin quebrantarse el art. 11.1 de la LOPJ, de lo contrario, se reputarán nulas”. Por tanto, la prueba del delito informático es sensible y debe tratarse con especial cuidado para evitar su modificación, como lo afirman Novoa y Venegas (2020).

Cordero (2021), indicó que el juicio de fiabilidad es a partir de la autenticidad e integridad de la prueba conservando el contenido original, se puede afirmar, que no se implementaron las técnicas espurias. Por lo tanto, Toledo y Venegas (2020) expresó, la autenticidad de la información que no haya sido modificado a través de la cadena de custodia, sometida al judicial. Según Bañol (2014). La interceptación de comunicaciones o recuperación de información producto o de la transmisión de datos a través de las redes de comunicaciones, el fiscal y ante el juez de control de garantías, realizará la audiencia de revisión de legalidad.

2.1 Del perito informático

Luego de la disquisición argumentativa anterior, se abordó el objeto principal de nuestra ponencia: la preparación necesaria o capacitación continua del perito informático. Izquierdo-Blanco (2011) se pregunta qué titulación debe reunir el perito encargado de practicar la pericia, ¿una licenciatura en informática, en ingeniería o en matemáticas?, en caso de acordarse una pericial informática.

Con referencia a la legislación española, por petición de parte o decretada por el juez, se requiere que el perito esté en posesión de los conocimientos precisos para explicar técnicamente los aspectos científicos o prácticos para valorar hechos o circunstancias relevantes, así se permita actualmente la intervención como peritos que no posean títulos especiales de índole académico, así deseen explicar su experiencia profesional se requerirá de conocimientos científicos en la estructura y sustentación del informe pericial. Todo lo contrario, será la valoración de dictámenes especiales emitidos por expertos con títulos especiales, sus conclusiones técnicas serán fidedignas.

Lo anterior es como fotografía de la vivencia colombiana, se calca la intervención de igual forma como sucede en España, pero esto no deja de causar inquietud académica para relievar la acreditación e idoneidad del perito informático. Lo que se indica con anterioridad sobre la prueba pericial, revive lo concerniente a la pericia proveniente del experto en informática o electrónica y así como el médico legista conoce de la patología, de causas de muerte, de lesiones personales y el ingeniero civil o arquitecto conoce de su especialidad, debe igualmente el perito informático conocer ampliamente todo lo que le corresponde en la ciencia de la Ingeniería de Sistemas o la técnica de la informática para acertar en su informe o dictamen o en su exposición, para la correspondiente valoración que ha de efectuar el juez.

Los instrumentos que permiten su archivo, reproducción (palabras, sonidos, mensajes de datos, cifras, operaciones matemáticas, publicaciones en redes sociales, etc.) en cuanto

a su autenticidad requieren, obviamente, del experto o perito informático.

El periódico colombiano Ámbito Jurídico el 25 de octubre de 2019, denominó su publicación: La importancia de buscar a un experto en informática forense, escrita por el ingeniero Marco-Ramiro Marín-Ace (Senior consultant digital forensics FTI Consulting), apuntado que la modernidad tecnología e informática forense ha atesorado el servicio judicial, para esclarecer o resolver litigios con estas disciplinas en caso de incumplimientos de contratos o asuntos regulados por la ley donde se corre riesgo con comportamientos fraudulentos o de corrupción.

Señaló el profesional que esta especialidad, al seguir metodologías para recabar y resguardar los datos opera cuando los medios electrónicos son la fuente sustancial de información, siendo de natural importancia la búsqueda del experto que aporte conocimientos técnicos con fines jurídicos. Debe apoyarse en medios electrónicos aplicando el principio de intercambio de Locard (1935), propuesto por el científico francés Edmon Locard y que es clave en la informática forense. De acuerdo con él, “siempre que dos objetos están en contacto transfieren parte del material que incorporan al otro objeto” (p.41).

Siguiendo con los datos conservados en los correos electrónicos, en los mensajes de WhatsApp, con comunicaciones por Skype o medio similar, con los archivos de información o datos en los sistemas como Word, Power Point, y Excel o cualquier elemento electrónico, el experto puede ayudar a esclarecer los hechos judicialmente debatidos, sobre todo cuando percibe de los elementos probatorios su modificación, falsificación o alteración en cuanto a los mensajes de datos, por ejemplo, como información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, internet, intercambio electrónico de datos, telegrama, télex etc.

El perito deberá supeditar su labor a los estándares internacionales como la colección, evidencias digitales; la ISO/IEC 27042:2015, Guía para el análisis e interpretación

de evidencia digital. López Delgado (2007) ;Metodología para el análisis forense de las evidencias electrónicas. UNE 71506:2013, documentos que han de ser parte sustancial en la capacitación del perito informático como se recomienda en esta ponencia; siguiendo con prudencia la recolección de las evidencias, sacando las copias correspondientes, embalándolas y asegurándolas mediante la cadena exigida por la ley y luego -con idoneidad- rendir el informe pericial pertinente y sustentarlo en debate probatorio ante el juez. El experto estará en la condición de sustentar los mecanismos de existencia, transmisión y recibido de mensajes de información, de recuperar datos eliminados, ingresar en archivos protegidos con claves, en fin, llevar a cabo su tarea con idoneidad. Como se expuso, la relevancia probatoria se notará cuando el perito declare, sea interrogado o contra interrogado, coadyuvando con la administración de justicia.

Con frecuencia, el análisis exige el conocimiento especializado o técnico para que el perito solvente su trabajo, lo registre en un informe pericial y lo exponga en un estrado judicial cuando se trate de confrontar o desconocer la autenticidad de un correo electrónico.

> Según Pasamar (2011), en el capítulo titulado “La prueba pericial informática frente a la impugnación de la autenticidad de un e-mail” del libro *Luces y sombras de la prueba pericial en la LEC*, editado por Sotelo-Vázquez, A., la importancia del análisis radica en el acceso al correo original, no únicamente a los reenvíos. Este análisis incluye el examen de los contenedores de correos, los registros del servidor, el disco duro del ordenador, de manera técnica, la cabecera de los correos recibidos y los metadatos de los adjuntos.
>
> Además, los servidores registran la fecha, hora y tamaño de la información, lo cual puede compararse con los datos del correo y con terceras fuentes de registro. Por ello, los contenedores de correos y los metadatos de los archivos adjuntos constituyen objetos esenciales de análisis.

> Es necesario verificar el contenido de los archivos, los formatos y los parámetros o indicadores mediante los cuales el perito o experto puede detectar alteraciones o manipulaciones (Pasamar, 2011).

Ha de precisarse el trabajo arduo que debe efectuar el experto para ser real y materialmente auxiliar de la justicia mediante su opinión científica o técnica. Por lo tanto, los informes periciales, la manera de redactarse o elaborarse, constituyen otra necesidad de aprendizaje por el perito informático. La capacitación no debe limitarse al análisis del objeto del peritaje ni al señalamiento de unos resultados, sino a la forma apropiada de elaboración de un informe pericial y a la sustentación en audiencia pública, para que constituya verdadera prueba que es valorada por el juez. La organización empresarial Evidenttia (2020), afirmó que realizan peritajes técnicos y formalizan las evidencias electrónicas en la fase de análisis, en informes periciales claros, sencillos, que pueden ser utilizados como medios de prueba y ser radicados en juicio por parte de nuestros peritos informáticos. Informes que contienen la firma y currículos de los peritos, resumen ejecutivo para una supervisión rápida de contenido y resultados, descripción de las fuentes de información analizadas e inclusión de los datos de la cadena de custodia y depósito.

El peritaje en la audiencia pública es vital para el convencimiento del juez fallador, la credibilidad del perito, la sustentación o dictamen es trascendental para las resultas del juicio en estos tiempos en que las pruebas informáticas se presentan más frecuentes; la intervención del experto en la ratificación de su informe pericial es sumamente importante, es determinante para la parte que lo presenta como para la administración de justicia. La informática legal, habla de la función del perito en la audiencia donde debe contestar a las preguntas del defensor fiscal o juez, íntimamente relacionadas con el informe pericial, entregado con anterioridad a las partes, debiendo el perito contar con habilidades para comunicar sus conocimientos y opiniones cualificadas de manera que comprenda el juez, quien no ilustración correspondiente.

La empresa Aldana Informática, se publicita como un equipo profesional, quienes además de las dotes comunicativas mejoradas por la sucesión de intervenciones en ciertos juicios, es de una importancia enorme la experiencia para mantener las opiniones propias antes de las preguntas parciales de los representantes legales de las partes. Las preguntas al perito en audiencia pueden ser ambiguas conllevando a confundir sus respuestas, por ello debe tener el conocimiento y el manejo del tema tratado, así llevarlo a que sus respuestas sean ciertas y no lleguen a generar duda al juez.

Aspecto sustancial que permite comprender lo expuesto en cuanto a la preparación integral y prolija del perito informático en nuestra competencia judicial. El valor probatorio que contenga la explicación o declaración del perito es vital para la administración eficaz de la justicia. La confrontación como parte especial del derecho de contradicción en los sistemas penales del dicho de cada perito, arrojará la luz y la verdad procesal o probatoria que acogerá el juez en su sana crítica. La especialidad en el peritaje informático hará ver la verdad que contiene cada prueba especializada.

Recovery Labs (2019), trata el tema de las tres fases del informe pericial:

a. Fase de la adquisición de las pruebas,
b. Fase de la investigación,
c. Fase de la elaboración de la memoria.

El proceso de adquisición de las pruebas consiste en la recopilación que debe estructurar el informe pericial, pues el perito informático lleva a cabo el análisis meticuloso de los equipos, especialmente unidades del almacenamiento de datos que se sirvan de prueba o evidencia electrónica y según el resultado de los procesos realizados se conformarán las conclusiones de la investigación y para redactar el informe que se presentará ante los despachos judiciales. Señala la entidad que, se han dado casos donde ante un informe de absoluta credibilidad, la parte contraria ha buscado mecanismos alternativos para solucionar el conflicto.

Asimismo, siguiendo con las enseñanzas de entidades foráneas sobre el peritaje informático, respecto de la adquisición y presentación de un procedimiento judicial de una prueba informática, publicación de fecha 4 de abril de 2017, sentencias selectas STS 300/2015 y la STS 754/2015, donde se confirman la directriz para la incorporación de una prueba informática digital dentro del proceso judicial, mediante la presentación del informe correspondiente; en ellas, se obliga a la práctica de una prueba especializada si se quiere introducir un elemento probatorio informático y se descarta la presentación de pruebas o de medios mediante pantallazos o impresiones.

Así pues, cualquier pantallazo o impresión que se presente, sin prueba pericial que garantice su autenticidad: de un mensaje de correo electrónico, mensajes de WhatsApp, contenidos en redes sociales, etc., podrá ser inmediatamente impugnado.

No existe la profesión de ingeniero informático en España, por lo tanto; en Colombia, los expertos o técnicos deben ser verdaderos peritos informáticos. Lamentablemente, la ingeniería informática no se encuentra reglamentada como en la Unión Europea, situación que ha permitido a profesionales autocalificarse como peritos informáticos, a sabiendas que las leyes de procedimiento exigen ostentación del título oficial para la división de dictámenes en toda prueba pericial.

Situación académica que nos invita a precisar, que no solamente se necesita del perito informático en los estrados judiciales colombianos y otras partes del mundo, sino que, podría implementarse la especialidad de la ingeniería informática como profesión. Necesitamos de la pericia del ingeniero y del abogado experto en derecho informático, y a futuro la creación de colegio que los agrupe como especialistas con reglamentación sobre derechos, deberes, responsabilidades, etc.

Aunque actualmente se apunta que no es menester afiliarse o colegiarse para ejercer como perito informático, se tiene que el Tribunal Supremo exige para formar parte del listado de peritos, contar con el título requerido. Lo que significará para nuestra

invitación, que la capacitación o ilustración académica del perito informático ha de ser fundamental.

Como horizonte académico se plantea la necesidad de capacitaciones continuas para la acreditación de perito informático en Colombia, realización de cursos o diplomados que de manera extensa y profunda aporten al estudioso de la informática conocimientos científicos, técnicos y jurídicos para fungir como peritos informáticos.

Se ha hecho alusión a esta labor en España, pues en Colombia se sigue la línea legalmente generalizada en materia de la prueba pericial, siendo importante -por lo menos- anotar que en España existe la asociación con la especialidad nombrada, en cuanto a la actualización de la certificación de perito informático forense de ANTPJIE, según publicación del 8 de diciembre de 2020, donde requiere la certificación de perito informático, otorgada por la Asociación Nacional de Tasadores y peritos judiciales informáticos, ANTPJI. Es una acreditación profesional de las personas con suficientes conocimientos en el campo de la pericia informática.

Se señaló que, para obtener la certificación de perito informático, es necesario superar un examen presencial donde se verifican los conocimientos para mantenerla actualizada, una vez transcurrido un año desde que se obtuvo por primera vez. Por lo mismo, la propuesta es la acreditación en nuestro país del perito especializado en informática.

La presentación e incorporación de peritaje informático en juicio oral tiene sus lineamientos hasta con intervención de notario digital; en el supuesto que la prueba informática sea etérea o pueda desaparecer como fotografías o videos en redes sociales, la mejor técnica para su presentación y evidencia de juicio, es certificarla a través de funcionario competente; la herramienta más conocida sobre dispositivos móviles es la Cellebrite UFED Touch, así como el software asociado a esta herramienta llamada Physical Analyzer. Existen otros mecanismos como Oxygen, Magnet Axiom, muy usados en el entorno internacional.

El perito, en casos complejos como los ciberataques, cada vez más frecuentes, juega un papel crucial al ser la persona capacitada para determinar si existe algún tipo de infracción. La ciberseguridad desempeña un rol fundamental en cada etapa de los procesos judiciales digitales. Según Rodríguez-Márquez (2021), en cada etapa del proceso judicial digital, los riesgos cibernéticos asociados, las recomendaciones para enfrentarlos y cómo se respetan las funciones del marco de ciberseguridad del *National Institute of Standards and Technology* (NIST) (Rodríguez-Márquez, 2021).

Al afirmar que, Los ciberataques representan una amenaza significativa para países y empresas, afectando los derechos fundamentales, sociales y económicos de las personas. Como se informó el 3 de octubre de 2020, la Unión Europea tomó medidas contundentes al imponer sanciones en respuesta a estos ataques. El Consejo de Seguridad de la UE aplicó medidas privativas contra individuos y entidades responsables de varios incidentes cibernéticos, incluyendo un intento de ciberataque contra la Organización para la Prohibición de las Armas Químicas. Entre los ataques más notorios se encuentran WannaCry, NotPetya y Operation Cloud Hopper, que han dejado una huella impactante en la seguridad digital global.

Se tomaron sanciones como la de la prohibición de viajar y la inmovilización de bienes, prohibiéndose a las entidades de la unidad europea, colocar fondos a disposición de las personas sancionadas.

La Unión Europea ha fortalecido su capacidad de prevención, disuasión y respuesta frente a las amenazas y ataques cibernéticos con el fin de garantizar la seguridad y proteger sus intereses estratégicos. En este marco, el Consejo decidió imponer medidas restrictivas contra seis personas y tres entidades responsables —o implicadas— en diversos ciberataques. Este hecho evidencia el incremento de tales conductas delictivas y la necesidad de proyectar medidas eficaces para su control o eliminación. Asimismo, se contempla el desarrollo integral de todas las fases relacionadas con la recolección de elementos

probatorios, su análisis y la elaboración de los informes correspondientes.

Labores sencillas o de gran connotación que requieren de los peritos, dejar entrever diversidad de fases en sus análisis, elaboración y sustentación del informe pericial y tratándose de mayor complejidad, acarrearán mayores honorarios en pro del experto. Espada (2021) perito informático titulada ¿Cuánto cuesta una prueba pericial informática?, se indica que no hay dos casos similares, cada experticia es única y posee características específicas que el perito debe conocer, verificar y valorar con antelación a su informe o dictamen.

El peritaje informático de grabaciones de audio, para que constituya un elemento material probatorio o prueba, requiere cumplir con ciertos requisitos específicos. No es lo mismo realizar dicho peritaje sobre mensajes de texto de WhatsApp, correos electrónicos o mensajes de datos. Según De la Torre (2022), en el texto titulado *Peritaje Informático de Grabaciones de Audio como Prueba*, publicado por la empresa española Indalics, el uso de grabaciones de audio digital se ha extendido globalmente tanto en el ámbito profesional como en la vida privada. Estas grabaciones pueden incluir conversaciones telefónicas, publicaciones o imágenes en redes sociales, referencias íntimas o familiares, así como declaraciones o manifestaciones relacionadas con investigaciones periodísticas o de detectives públicos y privados. Con la implementación de *smartphones* y sus numerosas aplicaciones de grabación de audio y mensajería instantánea, las grabaciones de audio digital se han convertido en un elemento común en nuestra vida cotidiana (De la Torre, 2022).

Por su condición digital, una grabación de audio es fácilmente manipulable, por eso no basta la sola audición para acreditar su autenticidad u originalidad; estas grabaciones han incursionado en el campo judicial penal, civil, familia y administrativo.

Enseña, además, que debe estudiarse la autenticidad e integridad de cada fichero de audio digital aportado al proceso,

que puede manipularse. El ejemplo más claro son los software de simulación de voz para suplantar la voz de terceras personas. Igualmente, categóricamente se señala que, no es menester la práctica de la prueba pericial si otros medios corroboran o demuestran la autenticidad da la grabación de audio. Así mismo, indica que, se pierden o no se tienen en cuenta determinados peritajes informáticos, siendo la razón que los peritos no están legalmente habilitados para acudir a los estrados judiciales, sin acreditación especializada pertinente.

Según Bassini (2013), en El *perito informático* y la prueba pericial, el experto debe ser idóneo y especializado en la materia, ya que la informática no corresponde a una sola área. Es necesario que el perito esté preparado en sus múltiples disciplinas, que son vastas y cambiantes. Además, es indispensable contar con experiencia tanto en hardware como en software. Por su parte, Indalics (2013) destaca que el perito debe poseer una titulación en el ámbito de la informática que demuestre su competencia en lo que desea peritar, además de estar colegiado, lo cual acredita su titulación oficial y garantiza el visado colegial de su dictamen pericial. En este sentido, se considera que en Colombia estas exigencias deberían ser objeto de legislación especial o reglamentación oficial para el cumplimiento adecuado de la profesión de peritaje informático. Asimismo, el campo de acción del perito es amplio, con diversas áreas y especialidades en las que puede actuar.

Adalid (2021), (La empresa colombiana especializada en los temas abordados en la presente exposición), el 7 de noviembre de 2017 publicó texto sobre la importancia de las pruebas periciales como medios probatorios, destacando que la fase de rendición de un informe requiere del experto, mismo que está obligado a su certificación con la finalidad que su informe pueda ser utilizado como medio de prueba, donde se debe considerar la idoneidad técnica, científica, ética o moral, incluyendo el conocimiento experimentado sobre el tema materia de su concepto, como garantía de su solvencia y capacidad profesional.

Así la situación, Colombia no puede ser ajena a las exigencias que hace la jurisprudencia y la doctrina, cada uno de los expositores o columnistas o académicos que se han citado y trascrito, dirigen la exigencia al profesionalismo, a la titulación, capacitación e idoneidad o especialidad del perito informático. He aquí el objetivo de nuestro clamor, propuesta o ponencia.

Esta conexión, mediante diapositivas utilizadas para dar conferencia sobre la administración de la evidencia digital por intermedio del doctor Echeverry Aristizábal, enseña los estándares como metodologías para el afianzamiento de los procesos mencionando lo siguiente en cuento a estándares: RFC 2350 Guías para la conformación del equipo de respuestas a incidentes, RFC 3227 Guía para la recolección y manejo de evidencia computacional, ISO27002, ISO 18044 y GTC 169 Gestión de los incidentes de la seguridad de la información, IOCE The international organization evidencia, HB 171 Guía para la administración de la evidencia computacional.

Señaló el experto, que un incidente de seguridad se manifiesta por un evento o conjunto de ellos, inesperados y no deseados que tienen una probabilidad significativa de poner en riesgo las operaciones del negocio y amenazar la seguridad de la información; un evento de seguridad de la información es la ocurrencia identificada de un estado del sistema, servicio o red que indica una posible violación a la política de seguridad de la información, una falta de salvaguardia o una situación desconocida que puede ser relevante para la seguridad; un equipo de respuesta a incidentes de seguridad de la información, constituido por miembros de la organización que son de confianza y tienen las habilidades adecuadas para manejar los ciclos durante su ciclo de vida. Dice, se consideran incidentes la pérdida de confiabilidad de la información, compromiso de la integridad de la información, negación del servicio, indebida utilización de servicios, sistemas o información o daños a los sistemas.

La Fiscalía General de la Nación colombiana emitió la Guía interna de informática forense como subproceso de policía judicial con

código FGN 41300 -G – 10, luego de determinadas definiciones, del fundamento teórico, de normatividad y condiciones relevantes en el capítulo de desarrollo, indica las respuestas a los incidentes informáticos, el análisis y/o recuperación de información de medios de almacenamiento tecnológico, de la extracción de encabezados de direccionamiento IP, el análisis a sistemas informáticos y/o telemáticos, páginas web, software y a la asesoría especializada.

Otras guías se han publicado por la Fiscalía General de la Nación sobre la labor a seguir por la policía judicial y los fiscales delegados en determinadas investigaciones penales. Aspectos legales que no puede dejar de lado el perito experto en informática al momento de llevar a cabo análisis, elaboración de informes, rendir el dictamen ante los jueces de la República, entre muchas otras labores, para la validez de su tarea especializada.

En la literatura española, se han encontrado ejemplos que ilustran la labor de los peritos informáticos, lo que se ha acogido en la presente ponencia para resaltar la importancia de su función en el sistema judicial. La figura del perito informático es crucial, especialmente en casos donde la tecnología juega un papel fundamental, como en disputas laborales o delitos cibernéticos. Un caso destacado es el dictamen pericial presentado ante un juzgado en Madrid, solicitado por D. en relación con una carta de despido. En este contexto, el perito, especializado en informática forense, no solo aporta su conocimiento técnico, sino que también debe demostrar su capacidad para comunicar sus hallazgos de manera clara y comprensible para el tribunal. El perito presenta un informe detallado que incluye análisis de datos, recuperación de información y evaluación de evidencia digital. Su formación y experiencia son esenciales; por ejemplo, este perito cuenta con cualificaciones que le permiten emitir dictámenes con autoridad. Entre sus méritos se destaca haber dirigido cursos en el Consejo General del Poder Judicial (CGPJ), lo que subraya su compromiso con la actualización constante de sus conocimientos y habilidades.

Obsérvese la manera como al final del informe pericial se daba a conocer el experto Gallardo Ortiz Miguel Ángel, ingeniero informático y criminólogo, perito en tecnología forense, director del curso para jueces y del libro editado por el Consejo General del Poder Judicial.

Gallardo (1996), señala igualmente que ha publicado diversos artículos, ha dado entrevistas y preside desde 1992, la Asociación para la prevención de estudios de delitos, abusos y negligencias en informáticas y comunicaciones avanzadas, APEDANICA. Además, que es autor del libro Seguridad en Unix. Sistemas Abiertos e Internet publicado en 1996, por Editorial Paraninfo (ahora International Thompson Publishing), y también ha dirigido la obra colectiva publicada por el Consejo General del Poder Judicial (CGPJ).

Por último, este perito hace saber al tribunal, y a las partes, que también cuenta con experiencia profesional como consultor-instructor, precisamente, en la migración de sistemas propietario IBM a entornos abiertos cliente-servidor. El tratadista dice que, a entera satisfacción de los clientes, habiendo recibido formación especializada en ORACLE en la empresa Unisys en 1987, actualizando de sus conocimientos hasta la fecha y también habiéndola impartido en diversos clientes basándose en el texto Understanding ORACLE.

Mínimamente pide que en los informes periciales como presentación se coloque -nuestro nombre completo, número de tarjeta profesional, titulación académica, organización profesional en la que estamos colegiados, y nuestra capacitación en el área de periciales y en área que nos ocupa la pericial. Expondremos que se nos contactó por parte del Juzgado tal (si es judicial), o persona tal (si es de parte).

De otra parte y desde la óptica de la preparación o capacitación del perito informático, deberá de igual manera, adquirir la destreza de la controversia, confrontación o contradicción del informe pericial o dictamen emitido por perito de la contraparte; es decir, el experto ha de adquirir conocimientos técnicos para

enfrentar los peritajes entregados por la parte contraria a la que representa.

La falta de experiencia del perito informático en el producto es fundamental para controvertirlo. Poder demostrar que el perito no tiene experiencia o formación acreditada debilita el primer peritaje. Los aspectos simples han de atacarse cuando no conllevan a demostrar el problema en litigio, son claramente contrarrestables. La parcialidad que emana de la pericia confrontada se enfatiza por el nuevo perito para buscar se tenga en cuenta por quién debe tomar la decisión ¿juez o funcionario? dice el articulista, las palabras nunca, siempre, nada, todo, o similares, suelen ser puntos para estudiar. Probar y puntualizar cada evidencia que el primer perito informático reflejó, marca como falla grave cuestiones que son menores y permiten minimizar la evidencia. La evaluación del cumplimiento de las formalidades sustanciales del documento es parte básica de estudio y confrontación. Enseñanzas del académico que debe adquirirse y aplicarse.

Sobre las pruebas modificadas, indica, realmente parece increíble que un perito informático haya entrado en el código fuente de un proyecto y lo haya modificado para probar que sí funciona. Esto me lo he encontrado varias veces. Cabe destacar que el perito es, en el fondo, un observador teniendo absolutamente prohibido basar sus afirmaciones en modificaciones de las pruebas. Si un ERP no muestra un dato adecuadamente de nada sirve, de cara a un juez, entrar en el código y cambiar, aunque sea una única línea de código, pues está alterando la prueba base de la pericial.

En conclusión, se reitera que se requiere de conocimientos técnicos o estratégicos para controvertir las pericias anteriores de la contraparte, la capacitación continua del perito informático es integral y extensa. Además de lo expuesto en párrafo anterior, debe dimensionar la información que le ofrezca el cliente o terceras personas para sustentar el nuevo peritaje, incluyendo en este informe nuevas informaciones que no se incluyeron en el documento anterior, quizá por desconocimiento o

voluntariamente, que es relevante para las resultas del producto en debate.

Se considera en la presente obra que, así sea sencilla o compleja, en la labor del perito informático, su acreditación es sustancialmente importante para ponderación y convicción por parte del juez o autoridad llamada a dilucidar un litigio.

Fernández (2002), al hablar de la prueba pericial, cuando se trate de pericias tendientes a establecer la autenticidad de marcas o aplicaciones de software, así como también las unidades lógicas o elementos electrónicos que integran un procesador y que normalmente caen dentro de la esfera de la incumbencia del perito informático, el dictamen suele ser sencillo, en la medida en que se cuenta con los correspondientes patrones de comparación o indubitables.

Distinto es el caso en que se someta a dictamen el modo de funcionamiento de un dispositivo, la obtención de información borrada o alterada en soportes magnéticos, la determinación de maniobras fraudulentas mediante el uso de aplicaciones informáticas, puertas falsas, contabilidades paralelas, intrusiones no autorizadas a sistemas de redes o bases de datos a través de internet, violación de la correspondencia electrónica.

Las fases de estudio o análisis la que ha de cumplirse en cada trabajo pericial informático, sino que la diversidad de casos sencillos a complejos necesitará del experto; el éxito de un peritaje estará en su credibilidad emanado de su credibilidad en la exposición o sustentación de los productos o resultados y en su experiencia. Los abogados fiscales, jueces o magistrados o defensores o acusadores, deben, al igual que los ingenieros expertos en informática, plantearse la necesidad de la educación continua en estas materias. La administración de justicia de donde proviene la paz o tranquilidad social se logrará con la eficacia y rectitud de los peritos informáticos, cuando se trate de delitos en contra de la información y los datos, o se presenten ciberataques o se debatan hechos o pretensiones que requieran del peritaje especializado en comento.

Colombia según lo reseñado, posee organismos policiales y estatales con dedicación a los delitos y conductas indebidas ejecutadas o consumadas mediante operaciones informáticas, electrónicas o digitales; abarcan labores penales como disciplinarias o de orden fiscal. Se señala la existencia de laboratorios forenses que coadyuvan en estas clases de investigaciones, que han de ser dirigidos y compuestos por personal idóneo y han de conocer prolijamente la pericia informática. La selección debería ser a corto plazo de expertos acreditados en peritaje informático, por cuanto un resultado eficaz y confiable, como se ha venido tratando, corresponderá solamente a los que han cursado capacitación o diplomados o especialización en esta materia.

Mediante Sentencia C-224 de 2019, la Corte Constitucional colombiana declaró que el convenio sobre la ciberdelincuencia se ajusta a la constitucional política, otorgando aval a la Ley 1928 de 2018, por medio de la cual aprueba este convenio adoptado el 3 de noviembre de 2001, en Budapest. Tardía adaptación que demuestra la necesidad de mirar hacia otros países donde desde temprana época acogieron la labor de buscar la seguridad para el Estado, las empresas y las personas en cuanto a la vulneración de soberanía o derechos fundamentales o sustanciales de los ciudadanos. Surge la necesidad de prepararnos y capacitar a los peritos o expertos en todas estas materias en pro del amparo o protección de las garantías constitucionales o bienes jurídicos tutelados por el legislador. La delincuencia es vertiginosa y la ciberdelincuencia no se queda atrás.

Para relievar la importancia del conocimiento de estos temas novedosos, se referencio a Softplan (2020), como pionera hace más de tres décadas en la implementación y consolidación del proceso digital con la Solución de Actualización Judicial (SAJ), quien se repunta como gran aliada de la justicia en los momentos actuales en cuanto a apoyar instituciones judiciales para mejores resultados aún con el trabajo remoto. En su artículo de las nuevas tecnologías y su impacto en la justicia, editado el día 20 de julio del año 2020; expresa que las nuevas tecnologías están presentes en la realidad del ecosistema de la

justicia y que cambiarán la forma como trabajan los magistrados y abogados, creando áreas de actuación nuevas como serán la inteligencia artificial, la operación en nube y las formas de trabajo digitales de la justicia; el uso de inteligencia artificial para construir sus fallos, buscar jurisprudencia de casos similares o producir la decisión magistral a partir de lo que la máquina ha aprendido acerca de su dueño. La máquina podrá buscar bases de datos de manera inmediata.

La operación en la nube permite almacenar grandes volúmenes de datos con una calidad de almacenamiento superior. Actualmente, esto se refleja en cómo la administración de justicia ha tenido que adaptarse al uso de medios virtuales. Como señala Softplan en su artículo Justicia durante la cuarentena (2020), “la justicia no puede parar”. Este contexto ha llevado a la eliminación del expediente físico, lo que implica que ya no se ven carpetas apiladas en los escritorios de los jueces. Además, Softplan resalta la importancia de que fiscalías y procuradurías se integren en este ecosistema digital para garantizar una mayor agilidad en los procesos judiciales.

Este tema se relaciona con la pregunta formulada por Bierrun Abad (2018) en su artículo *¿Va a remplazar la inteligencia artificial a los abogados?*, donde aborda los temores de los abogados en Estados Unidos frente a la implementación de la inteligencia artificial en el ámbito legal. Thomson (2021) señala que la aplicación de la inteligencia artificial en el sector legal requerirá una combinación de experiencia en la materia, contenido anotado y conocimientos técnicos, ya que “no se puede simplemente arrojar inteligencia artificial, datos legales y esperar buenos resultados”.

Tonya (2018) enfatiza que, mientras más abogados comprendan cómo funciona efectivamente la inteligencia artificial, más cómodos se sentirán con su uso. Además, resaltó la importancia de entender cómo los algoritmos procesan los datos y sus posibles consecuencias en el desempeño de este sistema. En este sentido, la inteligencia artificial no reemplazará a los abogados, sino que incrementará su capacidad para realizar su

trabajo, ahorrando tiempo en investigaciones, identificando casos relevantes, sugiriendo artículos o argumentos, y detectando información que pudiera haber pasado desapercibida.

De otra parte, el ciberespacio se ha constituido en un terreno para determinados delincuentes que atacan a las personas, empresas, infraestructuras y soberanía de los estados. Nace entonces, la ciberdefensa, ciberseguridad y la ciberinteligencia, para protegerlos de los comportamientos delictuales en búsqueda de la seguridad de la nación y de los ciudadanos. Temas que tendrían que abordarse en las capacitaciones continuas de los peritos informáticos; ilustración que impedirá la comisión de errores en la prueba pericial. Se presentan errores en los informes periciales, como los siguientes: Cinco errores que arruinan un informe pericial informático, según el siguiente extracto de página web: (a) Usar demasiados tecnicismos informáticos, (b) Dar las cosas por sabidas, (c) No preservar la integridad de las pruebas, (d) Actuar lento a la hora de tomar las pruebas periciales, (e) No tener el perito el título de ingeniero informático.

Las conductas delincuenciales siguen su galopante avance. Su control es difícil, sin que se acaben las distintas formas como operan las organizaciones criminales. Hace pocos meses, Estados Unidos creó un grupo especial de trabajo para combatir delitos informáticos, Erazo (2020). titulada, El Servicio Secreto de EE. UU. crea un grupo de trabajo sobre delitos informáticos relacionados en las finanzas, grupo contra el Fraude Cibernético que tiene como objetivo combatir la tendencia creciente de esta clase de delitos, fusionando el Grupo de Delitos Electrónicos y el Grupo de Trabajo de Delitos Financieros en una sola red. Creado para combatir los delitos cibernéticos relacionados con el sector financiero y combatir ataques de ransomware, (que bloquea los archivos o dispositivos de los usuarios y se exige dinero para restaurarlos), estafas de compromiso de correo electrónico corporativo, robo de tarjetas de crédito en línea, este último cometido a través de la Dark Web y los detalles bancarios de las empresas.

Estados Unidos como país llamado desarrollado, prepara sus grupos de investigación criminal; si los delitos siguen latentes, ¿qué podrá decirse de los menos desarrollados? Que la preparación es mediante el conocimiento que ofrecen las capacitaciones y talleres en estas lides judiciales. Por ejemplo, lo que pueda avecinarse con las transacciones criptomonedas, que puedan utilizarse en tráficos ilegales en línea para las organizaciones lavar sus ganancias ilícitas. Esto se relaciona en el artículo antes mencionado y se puede afirmar que, en estos países latinoamericanos, siquiera se ha pensado en la gigante actividad que pueda revelarse a futuro.

Ameet (2020), señalo que, los delitos financieros y cibernéticos son dos caras, el toque digital y los ataques Magecart (agrupación de peritos informáticos) engruesan los mercados de la Dark Web (es la parte oscura de internet con contenido ilegal), brotan en el mundo como fraude de pagos, perjudicando el sistema financiero. El elemento cibernético y el chive delito tienen elementos tradicionales como el uso de las mulas para retirar y enturbiar el rastro del dinero.

Colombia todavía se encuentra en la protección de la dignidad humana que se afecta por las publicaciones efectuadas en redes sociales (Tema tratado en párrafos precedentes), procurando que se convierta en ley el proyecto 176 de 2019, sobre la regulación de políticas de uso y apropiación de las redes sociales, estableciéndose lineamientos del buen uso de estas en internet para proteger los derechos fundamentales de los ciudadanos colombianos y residentes en nuestro territorio. Debido esto al uso inapropiado de las redes sociales (la tecnología va a delante y la ley sigue sus pasos) con miras a la protección de las víctimas de la extralimitación y vulneración de sus derechos. El proyecto busca, además, acuerdos o convenios con las aplicaciones o redes sociales más comunes como Facebook, Twitter, YouTube, Google, para buscar que ellas asuman responsabilidad en cuanto a eliminar ipso facto expresiones o publicaciones deshonrosas, denigrantes, injuriosas o delictivas que, hoy en día, se minimiza el daño, pero a través de la acción pública de tutela, cuando ya este se ha ocasionado.

A manera de colofón, se puede señalar que, escribir sobre la prueba pericial es un tema amplio, pero de connotaciones jurídicas y técnicas especializadas para comprender que en derecho penal o procedimental penal quien se incline por la informática, como perito debe estudiar y asimilar las normativas sobre esta clase de medio probatorio, leer y entender lo que ha expuesto o enseñado la jurisprudencia y la doctrina sobre la prueba pericial. Con mayor énfasis en tratándose del peritaje informático. Por consiguiente, converge inexorablemente como conclusión entonces, que se necesita de la capacitación o especialización de los peritos informáticos en Colombia.

González et al. (2019) mencionan que la balística forense es una disciplina fundamental dentro de la criminalística, que se encarga del análisis de armas de fuego y proyectiles. Según González et al. (2019) el perito balístico desempeña un papel crucial en la investigación de delitos relacionados con el uso de armas. Este profesional no solo debe entender la física detrás del disparo, sino también las normativas que rigen su trabajo. En el ámbito normativo, el perito debe seguir procedimientos establecidos para garantizar la validez de su análisis. Esto incluye desde la recolección de evidencia hasta la presentación de informes técnicos que puedan ser utilizados en procedimientos judiciales. Además, las actividades que realiza el experto en balística del cuerpo técnico de investigación son vitales para esclarecer los hechos y proporcionar un soporte científico a las investigaciones policiales.

Guzmán (2020) afirmó:

En la práctica, el requisito legal, en el archivo se pueda abrir, ver su contenido como sus metadatos; en segundo que exista una firma electrónica del documento que cumpla con las mejores prácticas internacionales (ISO 27037), obligando la existencia del código hash, con la fecha y hora del recaudo que, se encuentran en el manual de cadena de custodia (p. 1), en la Ley 527 de 1999 y el Decreto 2364 del 2012.

La prueba pericial es un componente esencial en el sistema judicial, ya que permite la inclusión de conocimientos técnicos y especializados en el proceso de valoración de pruebas. Según Vásquez et al. (2019), el estudio de la idoneidad del perito es crucial para garantizar que la práctica de la prueba se realice de manera efectiva, conforme a lo establecido en la Ley 906/2004. En su análisis, los autores argumentan que contar con un experto calificado en esta etapa contribuye significativamente a que las partes interesadas logren un fallo favorable. La idoneidad del perito no solo asegura que se presenten evidencias sólidas, sino que también brinda garantías efectivas al debido proceso, permitiendo que todas las partes involucradas confíen en la validez de las pruebas presentadas. Este enfoque resalta la importancia de seleccionar peritos que no solo posean conocimientos técnicos, sino también una comprensión profunda del marco legal que rige su actuación.

2.2 Procedimiento penal en Colombia

La Ley de Procedimiento Penal colombiana de 2004, de carácter acusatorio, dictada luego de la reforma de la Constitución Política, especialmente en cuanto a la fiscalía general de la Nación, en su artículo 250 y concordantes, obliga a reseñar la importancia de este ente del Estado, para investigar las conductas con carácter de delitos y acusar a sus autores o partícipes. En consecuencia, la Fiscalía, constitucionalmente está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas la posible existencia de este. Lo que significa que debe la Fiscalía poseer los medios de prueba legalmente producidos, allegados o aportados a la actuación penal, para demostrar aquellos hechos o comportamientos, y determinar a sus autores o partícipes. Pruebas legalmente practicadas pues de lo contrario serán inadmitidas, rechazadas o excluidas, como lo sentencia la Ley 906 de (2004), y de conformidad con las previsiones constitucionales.

El Código Penal Colombiano – Ley 599 de 2000 – prevé tipicidad de la lista de conductas punibles que violen los objetos jurídicos tutelados por el legislador, iniciando con los delitos contra la vida e integridad personal y terminando con los delitos que atentan contra el régimen constitucional y legal del Estado, encontrándose un nuevo título dentro de esta codificación, denominado: De la protección de la información y de los datos, tipificándose los comportamientos llamados de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; también agrega el acápite, de los atentados informáticos y otras infracciones, que evidentemente requieren de la prueba para la correspondiente adecuación típica, o sea, es menester que en el proceso penal, en estos eventos de delitos especiales correspondientes al derecho informático, se produzcan, de soliciten, se debatan y se incorporen legalmente, en la actuación penal, especialmente, en la audiencia de juicio oral.

Por consiguiente, labor especializada que exige de la Fiscalía instructora la ayuda de perito experto en estas materias, para poder celebrar las audiencias de formulación de imputación, acusación, preparatoria y de juicio oral, para que los jueces de la República de control de garantías y de conocimiento que tomen las correspondientes dentro de su competencia prevista en la Ley 906 de 2004. Y como son dos partes en el proceso penal que se enfrentan, como acusador el fiscal de un lado y el defensor de confianza o defensor público de otro, debemos reseñar que es necesaria la capacitación o especialización de cada uno de ellos, como también de los intervinientes en el proceso, como es el agente del Ministerio Público en su condición de procurador o personero municipal y los apoderados representantes de víctimas o perjudicados. Sin embargo, operadores y coadyuvadores de justicia que se están viendo compelidos a estudiar estos temas para adquirir el aprendizaje necesario, ejercer el rol que le compete y procurar la impartición de recta y eficaz justicia.

Deberá ser objeto de consideración o de reflexión que, no solo el fiscal debe tener conocimiento de esta materia sino también

su inmediato auxiliar, como es el investigador de policía judicial del cuerpo Técnico de la fiscalía general de la Nación, cuando ejercen funciones permanentes o transitorias dentro de una investigación penal. Deben ser órganos probatorios científicos o técnicos, para la eficacia de las funciones constitucionales citadas en la norma 250 constitucional, al momento de realizar actividades de policía judicial en la indagación e investigación y luego, poder asistir como perito ante el estrado judicial en la audiencia de juicio oral. Especialización que va unida al cumplimiento de las exigencias legales como las de identificar, recolectar, embalar, y custodiar los elementos materiales correspondientes.

Asimismo, el defensor convencional o contratado debe tener a su lado un experto o perito en las materias de informática, de la protección de la información y de los datos, de los atentados informáticos y conductas afines. En el mismo sentido, los procuradores y sus auxiliares, y los abogados representantes de víctimas con su apoyo de perito experto. Todo en aras de la consecución de la verdad y de la obtención de justicia. De lo contrario, ella flaquea o no se aplicará de debida forma. Sin justicia no habrá paz, se dice cotidianamente, cuando se presentan errores judiciales, que por lo general proviene de las pruebas.

De este modo, la labor especializada que menciona debe ir de la mano de la prueba pericial, regulada igualmente por el Código de Procedimiento Penal colombiano, Ley 906 de 2004, luego de establecer o determinar lo que se entiende por elementos materiales probatorios y evidencia física, mediante enumeración, donde se encuentran las huellas, manchas, residuos, armas e instrumentos para la ejecución delictiva, dinero y bienes provenientes del delito, los elementos materiales descubiertos, recogidos y colocados en cadena de custodia, los documentos de toda índole y de suma relevancia para el presente trabajo, los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, ubicados como cámaras de vigilancia, en recinto cerrado o en espacio público, según el artículo 275 de la enunciada ley.

2.3 Elementos probatorios informáticos

Con mayor relevancia en la enumeración de los elementos materiales probatorios, para la finalidad en estudio, se establecen el Código de Procedimiento Penal, 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; materia que más adelante se tratará puntualmente, no sin antes compartir la enseñanza del investigador Cano (2010), vista en su libro “El peritaje informático y la evidencia digital en Colombia”.

Dado que, una labor de arqueología jurídica podría concluir que fue la Ley 8ª de 1970, la pionera en la materia al autorizar en el artículo 7º al presidente de la República para, entre otras, adoptar las medidas necesarias para generalizar el uso del computador electrónico en 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.

Con posterioridad a la Ley 527 de 1999, el marco legal colombiano se viene nutriendo de normas relacionadas con mensajes 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-justicia.

Dos series de elementos o evidencias que encierran material probatorio concerniente al derecho de la información y de las comunicaciones, a la informática en general, qué como producto

o resultado delictivo utilizado o proveniente de la ejecución o consumación de una conducta punible, deberán ser analizados o ponderados por expertos en estas materias.

Iniciándose por los mensajes de datos, pasando por el internet y correos electrónicos, llegando a los elementos que recoge la Fiscalía o la policía judicial, o los peritos del Medicina Legal o de los laboratorios reconocidos por las autoridades colombianas, se debe considerar, científica y técnicamente que, todas las labores que ejecutan los servidores públicos y los peritos, exige de la experiencia, la idoneidad y capacidad profesional del experto para elaborar el informe correspondiente de acuerdo con la Ley 906 de 2004, y en concordancia con las leyes que tratan los delitos informáticos y los reglamentos o resoluciones de la Fiscalía General de la Nación sobre la cadena de custodia y los protocolos dedicados a la recolección, presentación, descubrimiento, contradicción e incorporación de elementos o evidencias enmarcados en la informática.

2.4 La ley y la informática

Se trata en este segmento, en primer lugar, la Ley 527 de1999, para entronizar posteriormente el análisis de los delitos informáticos y continuar con el tema de la prueba pericial en general, descendiendo luego a la prueba por expertos en informática.

Con esto se dice que, la Ley 527 de 1999, por la cual se establece un marco jurídico para el comercio electrónico en Colombia. (1999); Reglamento el acceso y uso de los mensajes de datos del comercio electrónico, las firmas digitales, y se establecieron las entidades de certificación, que se aplica a todo tipo de información como el envío, acopiada por medios electrónicos, ópticos o similares, con el intercambio electrónico de datos (EDI), internet, el correo electrónico, el telegrama, el télex o el telefax, que tiene relación directa con la enumeración que estableció la Ley 906 de 2004, respecto de las evidencias probatorias.

En efecto, a la firma digital el legislador de igual manera le otorga valor probatorio y establece que se entenderá a satisfacción cuándo se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido, cuenta con su aprobación o que el método sea confiable en la generación del mensaje. Son cuestiones técnicas que deben ejercitarse dentro de las actuaciones judiciales de todas las áreas y para el horizonte que lleva esta exposición, en materia penal.

No obstante, los mensajes de datos serán admisibles como medios de prueba, dice la ley, lo que se concatena con los medios probatorios del Código de Procedimiento Penal antes enunciados y hacen notar la transcendencia jurídica de esta clase de documentos y firmas. Por esto, la normativa legal señala para la ponderación de la prueba en estudio que, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas, relacionándose esto con la Ley 906 de 2004 sobre el proceso penal. Conexión que permite la necesidad de analizar en esta parte todo lo relacionado con la prueba pericial.

Las herramientas tecnológicas permitidas por la Ley 2213 del año 2020 conforme a la ley 2213 del 2022: Las autoridades judiciales las implementan y desarrollan las funciones en forma combinada para el cumplimiento" (Ley 2213, 2022, art.4).

De esta manera, las herramientas tecnológicas acogidas por los juzgados en Colombia fueron: TYBA, SAMAI, Tutela en Línea, Consulta de procesos nacionales unificados, Lifesize, correos electrónicos; cuya función es proteger el acceso a la justicia, la igualdad constitucional, el debido proceso y la urgencia en agilizar los procesos judiciales.

Cabe mencionar, la importancia de las herramientas en las diferentes plataformas, entre ellas encontramos:

La ***plataforma TYBA***. Desarrollada por el Consejo Superior de la Judicatura, está diseñada para operar en tiempo real,

ofreciendo a los colombianos transparencia y publicidad al publicar diariamente información de los juzgados. Además, permite buscar expedientes de procesos judiciales ingresando el número de radicado y el número de cédula o NIT de algunas de las partes involucradas en el proceso. Cabe mencionar que algunos procesos pueden estar ocultos o privados, especialmente cuando no han pasado la fase de notificaciones por parte del juez. En este caso, el juez debe pronunciarse mediante autos, memoriales o traslados, los cuales se notifican por correo electrónico. Posteriormente, se inicia la publicación en las plataformas virtuales con la inserción de la providencia, la cual no requiere firmas ni impresiones físicas (Bohórquez, 2024).

Plataforma SAMAI. Son plataformas creadas para agilizar los expedientes digitales de los procesos administrativos o "la sede electrónica de la jurisdicción de lo contencioso administrativo en Colombia" (SAMAI, 2020).

Es relevante la interacción entre los magistrados de la corporación y la oficina de sistemas, con altos componentes de seguridad relacionados con los estándares tecnológicos actuales, su objetivo es proveer la información de cada proceso de la sede administrativa para el acercamiento con la justicia al ciudadano" (SAMAI, 2020), en acceder a información y a su vez descargar el expediente

Tutela en Línea. Cuya función es radicar las acciones de forma virtual, teniendo en cuenta la Constitución Política en el artículo 86 de 1991.

La Consulta de Procesos Nacional Unificada es una herramienta fundamental que permite a los ciudadanos visualizar procesos judiciales en Colombia. A través de esta plataforma, se puede acceder a información detallada utilizando el número de radicado y el nombre del juzgado donde se encuentra el expediente. Aunque no ofrece la opción de descargar documentos, permite a los usuarios visualizar el estado del proceso y recibir información sobre autos y memoriales, lo que refuerza el principio de

publicidad en el sistema judicial. Esta iniciativa busca promover la transparencia y facilitar el acceso a la justicia para todos los colombianos, sin embargo, si se visualiza e informa el proceso si hay un auto o memoriales principio de publicidad Lifesize. En la Ley 2213 del año 2022, en su artículo séptimo se mencionó que “las audiencias con el desarrollo en los medios tecnológicos a disposición de las autoridades judiciales, o los interesados en el proceso deberá proporcionar y admitir la presencia los individuos procesales, en interacción digital o vía celular del parágrafo 2o. del artículo 107 del Código General del Proceso” (Ley 2213,2022. art 7)

> En el que hacer judicial, la plataforma elegida por los juzgados para las audiencias virtuales es Lifesize, siendo una plataforma que integrar y brinda experiencias constantes a través de los diferentes dispositivos e integrando escenarios para reuniones con Skype empresarial, Outlook, Slack, Hipchat, Cisco, Polycom. (Vargas,2020)

Los ***correos electrónicos***. Son un medio directo de comunicación con los juzgados, estipulado por la Ley 2213 de 2022, para el envío de poderes por mensaje de datos sin necesidad de firma. No obstante, el poder debe coincidir con la dirección de correo electrónico inscrita en el Registro Nacional de Abogados. En el caso de una persona jurídica, el correo debe enviarse desde la dirección electrónica registrada en el respectivo registro mercantil (Ley 2213 de 2022).

2.5 Aspectos procesales y probatorios

La prueba pericial en materia penal exige ingredientes fácticos, jurídicos y probatorios, debe estar en consonancia con la Constitución Política de Colombia, con los tratados y convenios internacionales en materia de derecho procesal penal y probatorio, y con los principios rectores y garantías procesales que introdujo la Ley 906 de 2004, Bernal (2012), como sistema penal acusatorio en nuestro país, con base en la prelación de estos instrumentos sobre derechos humanos que prohíban su

limitación durante los estados de excepción, por formar parte del bloque de constitucionalidad y por ser la Constitución norma de normas, que se aplica de preferencia sobre una norma legal o de menor rango.

Concretamente, el descenso en la pirámide seguirá con los principios y garantías procesales y probatorias, siendo obligatorias las disposiciones sobre la dignidad humana, igualdad, imparcialidad, legalidad, presunción de inocencia e *in dubio pro reo*, defensa, oralidad, lealtad, intimidad, contradicción, inmediación, publicidad, cláusula de exclusión, que se establecen para el debido proceso, también de carácter constitucional, donde se encuentra inmersa la materia de la prueba, al preverse que, todo sindicado tiene derecho a pedir pruebas y a controvertir las que se alleguen en su contra, y además, reiterarse que es nula de pleno derecho toda prueba obtenida con violación del debido proceso.

Claramente contiene esta disposición constitucional y legalmente reiterada en los principios o garantías procesales la trascendencia de la prueba y su forma o manera de solicitarse, practicarse, debatirse e incorporarse en el trámite procedimental penal. Las formas propias del juicio se establecen también para la producción y efectos probatorios. Corresponde a la Fiscalía la carga de demostrar la existencia y adecuación típica de la conducta o encuadramiento en una norma penal, y determinar su autor o partícipe. La labor exclusiva de la Fiscalía, junto a sus auxiliares de policía judicial y peritos del Instituto Nacional de Medicina Legal, que ha de reflejar conocimientos sobre la tecnología que ocupa nuestra atención. Por tanto, situación que no menos importante es la defensa del autor o partícipe de un delito. Derecho también fundamental previsto en el artículo 29 constitucional, mediante las previsiones que todo sindicado tiene derecho a designar un defensor de su confianza o en su defecto, uno perteneciente al Sistema Nacional de la Defensoría Pública, adscrita a la Defensoría del Pueblo.

De ahí que, los abogados deben velar por las garantías y derechos de aquellos, que como facultad corresponde de estar el

sindicado asistido y representado por un abogado de confianza o nombrado por el Estado, por esto refleja esta particular situación la real, material o verdadera defensa de un indiciado, imputado o acusado, en el evento de poseer un idóneo o capacitado profesional en informática, cuando se trate la conducta de atentados contra la protección de la información y de los datos, de la confiabilidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, o de atentados informáticos en particular.

Los actos de prueba son diferentes a los actos de investigación sumarial, dice la doctrina, que corresponden por funcionalidad al fiscal investigador y su tarea es manifestar hechos al proceso, soportados para la imputación e imposición de medidas preventivas.

Actos de prueba, de acuerdo con Gimeno (2020), se refieren a la actividad de las partes procesales, dirigidas a ocasionar la evidencia necesaria para obtener convicción del juez o del tribunal sobre los hechos afirmados por ellas, intervenida por el órgano judicial bajo los principios de contradicción, igualdad y de las garantías constitucionales tendientes a asegurar la espontaneidad e introducida en el juicio oral a través de medios lícitos de prueba, según enseña Bernal ¡ (2013).

En otras palabras, la ley procedimental penal prevé el derecho sustancial de poder disponer el proceso para la preparación de la defensa, y esta será solo posible en los casos antes aludidos de delitos informáticos, cuando el defensor convencional o público conoce de esta ciencia o tecnología. De lo contrario, el ejercicio de las prerrogativas a favor del imputado o acusado no podrá calificarse de eficaz. Fallas en la defensa que puede también ocurrir en la acusación si el fiscal o su auxiliar no tienen los conocimientos para esta labor especializada. Y de contera puede señalarse, de igual manera, respecto de los perjudicados o víctimas de esta clase de comportamientos delictivos, cuando el representante legal o el asesor de una empresa afectada o el apoderado de persona lesionada, no conoce de esta especialidad.

En fin, la estructura de este opúsculo va dirigida a que, en Colombia se dicten diplomados, capacitaciones o cursos de especialización a abogados o ingenieros de sistemas o similares, para que puedan fungir como peritos, en las investigaciones penales por los delitos tantas veces mencionados. Abogados en su condición de fiscales o jueces, defensores de confianza o defensores públicos o agentes del ministerio público, procuradores, apoderados de las víctimas o perjudicados. Concretamente, es previsión legal -de la misma manera- a favor de todo sindicado la de solicitar, conocer y controvertir las pruebas. Este ejercicio defensivo tendrá efectos positivos o favorables cuando la controversia proviene del experto, del perito idóneo, que sea acreditado ante el juez o magistrado para la obtención de la verdad y de la justicia.

Acerca del juicio penal, en contra de todo acusado ha de ser oral, contradictorio, concentrado, imparcial, con mediación de las pruebas y sin dilaciones injustificadas, en el cual pueda -si así lo desea- por sí mismo o por conducto de su defensor, interrogar en audiencia a los testigos de cargo y a obtener la comparecencia, de ser necesario, aún por medios coercitivos, de testigos o peritos que puedan arrojar luz sobre los hechos objeto del debate; derecho sustancial frente a la declaración que ha de rendir un testigo técnico o experto o un perito. Condiciones o requisitos que permiten inferir la necesidad del profesionalismo de quien interviene en un juicio criminal donde se debata los comportamientos delictivos informáticos que tipifica el Código Penal colombiano.

La oralidad es importante para que pueda darse la explicación de cada informe pericial o técnico, para que, con los demás principios procesales, afloren el respeto a los derechos fundamentales de las personas que intervienen en la actuación judicial y se logre la eficacia del ejercicio de la justicia. Amparándose sobremanera, la intimidad como garantía constitucional, no solo en cuanto a su persona o domicilio sino para cuando resulte necesaria la búsqueda selectiva de datos computarizadas, mecánicas o de cualquier otra índole, que no sea de libre acceso y cuando fuere necesario interceptar comunicaciones. Previsiones

constitucionales y legalmente insertadas en el código procesal penal, conformando la contradicción el ejercicio probatorio tantas veces comentado en este trabajo, como prerrogativa de las partes – Fiscalía y defensa – de conocer y controvertir las pruebas, así como a intervenir en su formación; garantía que se relieva en el caso de formular la Fiscalía General de la Nación puesto que deberá por conducto del juez de conocimiento, suministrar todos los elementos probatorios e informes de que tenga noticia, inclusive los que sean favorables al procesado.

De modo, se exige por las normas que únicamente se estimará como prueba la que haya sido producida o incorporada en forma pública, oral, concentrada y sujeta a confrontación y contradicción ante el juez del juicio público. El juez percibirá de manera personal y directa todas las pruebas, evidenciándose la imperiosa necesidad de ser también conocedor de la tecnología, la informática, cibercrimen y temas similares, para poder dictar sentencia en un juicio penal por los delitos especiales que más adelante se tratarán de forma detallada.

Con lo expuesto, se comprenderá el principio de legalidad respecto a los elementos probatorios en la cual se recoge o se obtiene. De tal manera, la Constitución Política, en los tratados internacionales de los derechos humanos vigentes en Colombia y en las leyes, prevé la Ley 906 de 2004, que la extiende a la autenticación de las evidencias y sometidos a las reglas de cadena de custodia, pudiéndose aseverar que la prueba pericial informática debe también cumplir las normas utilizadas para la ejecución de los delitos que vulneren la información o los datos en atentados de sistemas tecnológicos como consecuencias a los comportamientos delictuosos.

Considerando que, los elementos que requieren identificación técnica o científica han de ser determinados en cuanto a su naturaleza y características, la cual debe hacerse por expertos en ciencia, técnica o arte, lo que se expone en un informe pericial, como ya señalamos.

2.6 Producción de la prueba pericial

En el siguiente segmento se analizarán específicamente las normas relativas a la aducción de la prueba pericial; a través de la historia se ha considerado que es procedente cuando sea necesario efectuar valoraciones que requieran conocimientos científicos, técnicos, artísticos o especializados. El perito cuando declara en un juicio penal es como un testigo que posee aquellos conocimientos especiales sobre ciencia, arte, técnica o profesión cualificada, como la del que conoce de informática o tecnologías de la información y de los datos, de ataques cibernéticos o similares. De esta manera, el servicio de peritos que en la actuación penal es prestado por los expertos de la policía judicial, del Instituto Nacional de Medicina Legal y Ciencias Forenses, entidades públicas o privadas y particulares especializados en la materia que les corresponda. De ellos se exige rendir siempre informe pericial bajo la gravedad del juramento que se convertirá en prueba en la audiencia de juicio oral luego de ser presentado, controvertido e incorporado legalmente ante el juez fallador.

Para ser perito se requiere que sea persona con título legalmente reconocido en la respectiva ciencia, técnica o arte; en su defecto podrá designarse a persona de reconocido entendimiento en los temas en referencia. No podrán ser nombrados los menores de 18 años a pesar del conocimiento prolijo que poseen algunos jóvenes, ni quienes hayan sido suspendidos en el ejercicio de las respectivas especialidades, tampoco los que hayan sido condenados por algún delito a no ser que procesalmente el juzgado de ejecución de penas mediante providencia haya otorgado la rehabilitación.

Es menester reiterar, que la forma propia del juicio penal permite a las partes solicitar al juez que haga comparecer a los peritos a la audiencia de debate probatorio, debiéndose entender, si no se permite la controversia del informe pericial, no se convertirá en prueba para ser ponderada o valorada por el juez al momento de dictar sentencia. Si las partes, Fiscalía o defensa, omiten citar o hacer comparecer a la audiencia del juicio oral al experto

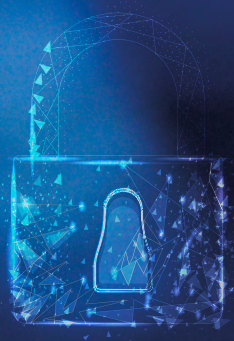
que coadyuvará o sustentará su teoría del caso, acusación o defensa, respectivamente, el elemento probatorio no llegará a estructurarse como prueba, por no estar precedida de la confrontación o contradicción como garantías inviolables, como se ha expuesto.

La base pericial como declaración que hace el perito debe estar precedida de un informe resumido en donde se exprese la base de la opinión solicitada por la parte que propuso la práctica de la prueba. Este informe se presenta en la audiencia preparatoria y deberá ser puesto en conocimiento de las demás partes hasta cinco días antes a la celebración de la audiencia de juicio oral. De no cumplirse esta exigencia legal, no podrá ser aducida o producida la declaración del perito en la audiencia de juicio oral ni convertirse en prueba. Requisitos que deben ser de conocimiento de los fiscales, defensores, apoderados de víctimas u otro sujeto procesal; para la eficacia de la prueba en estos casos que se enuncian en la presente investigación sobre los delitos informáticos. El informe por sí solo será entonces inadmisible como evidencia, si el perito no declara oralmente en el juicio, advierte la ley procedimental penal colombiana, podrán emplearse medios virtuales, sistemas de audio y video u otros mecanismos de reproducción a distancia, a través de los cuales la persona podrá ser interrogada o contrainterrogada.

Es decir, el perito que haya rendido informe o que será interrogado o contra interrogado en la audiencia de debate probatorio o de juicio oral, posee la facultad de conocer o acceder a todos los elementos a que refiere su informe y a los que se haga referencia en el respectivo. Es prerrogativa del experto sustentar o basar su manifestación en otros elementos que sirvan para su labor científica o técnica, por cuanto la controversia puede conducir a restarle credibilidad o desconocerlo como pericia, transformándolo en insuficiente para obtener la convicción del juez. Por esto mismo, el legislador enumeró catálogo de pautas para interrogar al perito, preguntas sobre los antecedentes que lo acrediten como conocedor de la ciencia o técnica pertinente, en el uso de instrumentos, equipos o medios utilizados como experto sobre su práctica o experiencia, principios científicos o

técnicos en los que fundamenta sus verificaciones o constatación pericial, y los métodos empleados en la investigación o análisis.

Esto, máxime cuando se establece en las normas procesales la forma de apreciación de la prueba pericial, exigiéndose del juez - para apreciarla- tener en cuenta la idoneidad técnico científica y moral del experto, la claridad y exactitud de sus respuestas en el interrogatorio y contra interrogatorio, su comportamiento al responderlas, el grado de admisibilidad o aceptación de los principios científicos o especializados en que se apoya el perito, los instrumentos que ha utilizado y la consistencia de la respuestas analizadas en conjunto. Si los temas tratados en la pericia son novedosos, como los referidos a las tecnologías de la información y la comunicación, la protección de datos, los atentados informáticos o similares, es necesario que la opinión del experto y la base científica o técnica satisfagan al menos ciertos criterios: que la teoría subyacente haya sido corroborada o verificada, que la tesis haya sido publicada y recibida con crítica por la comunidad académica, que sea acreditada, y que tenga una escala de confiabilidad de la aceptabilidad de la comunidad. Requisitos que exigen aún más, la preparación o capacitación del perito informático.



CAPÍTULO III
INFORMÁTICA JURÍDICA EN EL DERECHO DE FAMILIA

CAPÍTULO III
INFORMÁTICA JURÍDICA EN EL DERECHO DE FAMILIA

Los procedimientos judiciales concentraron en el Código General del Proceso Ley 1564 de 2012, los trámites de actuación en derecho de familia, civil, comerciales y agrarios en cuanto a la necesidad señalada en el artículo 29 de la Constitución Política. Prerrogativa sustancial como actividad procesal que se relaciona con los principios constitucionales correspondientes a un estado social de derecho fundado en el respeto de la dignidad humana, que en el proceso en derecho de familia y otras áreas corresponde a la prerrogativa de la administración de justicia que se logrará de manera objetiva, real o cierta, si se permite el discurrir del trámite procedimental sin mecanismos de afectación a los derechos humanos o fundamentales.

Este acceso para el ejercicio de los derechos y la defensa de los ciudadanos se ejecutan o se ejercitan mediante la solicitud y práctica de pruebas, por la exigencia o carga para las partes en litigio de demostrar los supuestos de hecho en que fundamentan sus pretensiones. Elementos probatorios que se ventilan en audiencias mediante la inmediación o percepción directa del juez, la concentración de la celebración de audiencias en sesiones continuas y permitiéndose la controversia de todas las pruebas por la parte contraria, en igualdad de condiciones o de oportunidades procesales o probatorias. Igualdad que se traduce en una obligación funcional del juez de conocimiento.

(Reuters et al., 2022). Este nuevo escenario digital en juzgado de familia en la comunicación, por lo tanto, los instrumentos de comunicación y usos sociales se transforman, dando lugar a la "huella digital", que es relevante en los procesos de familia con su objeto procesal y probatoria en hechos que revelan los medios electrónicos (redes sociales, mensajería instantánea, correos electrónicos, páginas web, etc.), así,

evitando riesgos en las fuentes de prueba, para estar previenes en los operadores jurídicos, en la aplicación de estándares de protección y garantías, en resguardar los derechos y libertades fundamentales de los implicados.

3.1 Aspectos procedimentales

La legislación procedimental vigente permite la interpretación de las normas al juez, pero teniendo en cuenta que el objeto de los procedimientos es la efectividad de los derechos reconocidos por la ley sustancial, derechos humanos, fundamentales y sustancialmente reconocidos en el Código General del Proceso. Esta efectividad de garantías también tiene que ver con la solicitud probatoria y su presentación, producción, debate o controversia e incorporación en la audiencia de juzgamiento, para que, con base en ellas, el juez pueda dictar la sentencia justa o adecuada a derecho. Por los mismo, el juez debe buscar la efectividad de las prerrogativas previstas en la ley sustantiva y de ser necesario para lograrlo, deberá aplicar los principios constitucionales y generales del derecho procesal garantizando el debido proceso, el derecho de defensa, la igualdad de las partes y los demás derechos constitucionales fundamentales, como reza en la ley referida antes.

Los principios fundamentales, en el siguiente extracto de la sentencia C-086 de 2016, emanada de la Honorable Corte Constitucional, al decir: En este sentido, el artículo 2º del Código reconoce el derecho que toda persona tiene a la tutela judicial efectiva para el ejercicio de sus derechos y la defensa de sus intereses, con sujeción a un debido proceso de duración razonable, lo que reafirma la competencia del juez para asumir un rol activo en el proceso y lograr la búsqueda de la justicia material. El artículo 4º, consagra el principio de igualdad, según el cual el juez deber hacer uso de los poderes que este código le otorga para lograr la igualdad real de las partes; ello supone abandonar una visión estrictamente formalista de la posición de las partes en el proceso para hacer uso de las facultades oficiosas y restablecer el equilibrio o distribuir las cargas probatorias cuando las circunstancias así lo demanden; el artículo 12 señala

que los actos procesales se realizarán con observancia de los principios constitucionales y los generales del derecho procesal, procurando hacer efectivo el derecho sustancial.

En consecuencia, los redactores del Código General del Proceso ajustaron sus previsiones a la Carta Magna de 1991 y a las codificaciones modernas, por cuanto Colombia hace gala de ser un Estado social de derecho, con el fin de garantizar la participación de todos en las decisiones que los afectan y asegurar la convivencia pacífica y la vigencia de un orden justo; lo que se obtiene con la recta y eficaz toma de las decisiones de la administración de justicia que conforman un bloque necesario concedida a quien corresponde.

En este orden, toda persona o la comunidad en general tiene derecho a la tutela jurisdiccional efectiva para el ejercicio de sus derechos y la defensa de su voluntad o pretensión o de sus intereses, mediante un proceso adelantado dentro de un plazo razonable o sin dilaciones indebidas. Y para este efecto, es menester la necesidad de permitirse a aquellos la producción o el aporte de la prueba para pretender lo demandado por cada parte, demandante o demandado.

(Reuters et al., 2022). El juzgado de familia en el nuevo escenario digital, a través de la comunicación de las nuevas tecnologías con la relación en las pruebas digitales o con las bases de las herramientas informáticas muestran y revelan datos al procedimiento judicial, por producirse en la intimidad familiar. De esta manera se trazan nuevas posibilidades de práctica probatoria en las evidencias.

La prueba digital, se apreciará en función de la confianza y seguridad de quién, cómo se ha obtenido y se ha contribuido al procedimiento para cuidar y no alterar la cadena de custodia de la prueba; siendo un apoyo la tecnología de la información en proporcionar nuevos recursos y herramientas útiles para esclarecer la verdad de los hechos, con objeto de evitar los riesgos en las evidencias para los derechos y libertades fundamentales de los individuos. Ibid. (2022).

3.2 La administración de justicia y el derecho de familia

La administración de justicia es función pública; las decisiones de los jueces son independientes, pero deben estar no solo ajustadas a las normas, sino que su sustento ha de ser la prueba producida legalmente ante él. He aquí entonces, la importancia del amparo judicial eficaz y el respeto por las solicitudes y práctica de pruebas, acordes con los hechos debatidos, que en caso de requerir de la especialización de la técnica o del experto, se produzca con el perito idóneo. No puede comprenderse un debate probatorio de temas o aspectos científicos o técnicos, sin el lleno de requisitos, acreditación y versión jurada del perito, en los casos propuestos, mediante un ingeniero conocedor de la informática. Así se indique en la Constitución que los jueces en sus providencias solo están sometidos al imperio de la ley y que la equidad, jurisprudencia, los principios generales del Derecho y la doctrina son criterios auxiliares de la actividad judicial, se considera que no es menos importante la producción, admisión e incorporación probatoria en cada litigio judicial de competencia de los jueces de familia.

Observando el listado de asuntos que corresponden a los jueces de familia, visible en los artículos 21 y 22 del Código General del Proceso, se pueden seleccionar algunos donde se podrá ventilar tópicos de evidencias virtuales o documentos de internet, informática, información o de datos protegidos por el legislador colombiano.

Podrán señalarse actuaciones judiciales como: (a) procesos de cesación de efectos civiles y divorcios, declaración de unión marital de hecho y su liquidación de la sociedad patrimonial de hecho, (b) custodia y cuidados personales de los niños, niñas y adolescentes, (c) investigación de la paternidad, (d) medidas de protección de la infancia en los casos de violencia intrafamiliar, (e) restablecimiento de derechos de la infancia, (f) revisión de la declaración de adoptabilidad, (g) fijación, aumento, disminución y exoneración de alimentos, (h) filiación natural, (i) indignidad o incapacidad para suceder y del desheredamiento, petición de herencia.

Los artículos 21 y 22 del Código General del Proceso hacen alusión a medios informáticos y respecto de las clases de procesos de derecho de familia, como son: (a) De la protección del nombre de personas naturales, (b) Suspensión y restablecimiento de la vida en común de los cónyuges y la separación de cuerpos y de bienes por mutuo acuerdo, sin perjuicio de la competencia atribuida a los notarios; y otros.

Señala el artículo 22: Competencia de los jueces de familia en primera instancia: (a) De los procesos contenciosos de nulidad, divorcio de matrimonio civil. Cesación de efectos civiles del matrimonio religioso y separación de cuerpos y de bienes, (b) De la investigación e impugnación de la paternidad y maternidad y de los demás asuntos referentes al estado civil, (c) Liquidación de la sociedad conyugal y patrimonial.

Artículo 34: Competencia funcional de los jueces de familia. Corresponde a los jueces de familia conocer en segunda instancia de los procesos de sucesión de menor cuantía atribuidos en primera al juez municipal, de los demás asuntos de familia que tramite en primera instancia el juez municipal, así como del recurso de queja de todos ellos.

3.3 Juez y auxiliar de justicia

La legislación colombiana inscribe los deberes del juez, y entre ellos se encuentra el de emplear los poderes que el Código General del Proceso que le concede en materia de pruebas, para verificar los hechos alegados por las partes. Considerado de buena utilización cuando ante el juez de familia, se debatan aspectos especializados en la materia objeto de la presente investigación. Debiéndose acudir en determinados casos a los auxiliares de la justicia, instituidos como cargos de oficio público ocasionales que deben ser desempeñados por personas idóneas, imparciales, de conducta intachable y excelente reputación. Para cada oficio se requerirá idoneidad y experiencia en la respectiva materia.

Como se requiere del auxiliar de la justicia tener vigente la licencia, matrícula o tarjeta profesional expedida por el órgano

competente que la ley disponga, según la profesión, arte o actividad necesarios en el asunto en que deba actuar, se considera que aquí radica una de las fortalezas legales para cuando se requiera del ingeniero especialista en informática, como tarea que puede ejecutar el juez de familia en los asuntos o procesos que lo necesiten como peritos técnicos. Sin desconocer, naturalmente, que la legislación actual lleva implícita la solicitud de prueba especializada para adjuntar a la correspondiente demanda o su contestación. Principio de la necesidad de la prueba, de la prueba pericial que conllevará a la recta y eficaz administración de justicia en esta área del Derecho.

Así el legislador limite a determinados auxiliares de justicia su designación, no es óbice conforme a los principios constitucionales y legalmente plasmados en el Código General del Proceso, para la tutela jurisdiccional efectiva, buscándose el equilibrio judicial y la garantía de la primacía del derecho sustancial sobre el procedimental; esta designación especial del auxiliar técnico. Obsérvese que la ley 1564 (2012), República de Colombia, Congreso de la República, indica que: Para la designación de los peritos, las partes y el juez acudirán a instituciones especializadas, públicas o privadas, o de profesionales de reconocida trayectoria e idoneidad, sentenciado igualmente la normativa 48. Numeral 2 que: El director o representante legal de la respectiva institución designará la persona o personas que deben rendir el dictamen, quien, en caso de ser citado, deberá acudir a la audiencia.

Es más, las partes, señala la norma, de consuno, podrán en cualquier momento designar al auxiliar de justicia o remplazarlo. Generalidad que permite enfilar nuestra propuesta como válida, para que, en casos de requerirse un experto o peritos para dilucidar aspectos probatorios de la informática, internet, cibernética o de la evidencia digital, se acuda al especialista para una mejor y eficaz administración de la justicia que se exige de un Estado social y de derecho.

3.4 El abogado y la prueba legalmente producida

Tratándose de litigios en derecho de familia, igualmente se considera que es obligación o deber del apoderado -según lo exige la misma ley- realizar las gestiones y diligencias necesarias para lograr la integración del contradictorio, o sea, así como es un derecho el de solicitar pruebas, también es obligación buscar los mecanismos idóneos para ejercitar el contradictorio o la controversia, de lo expuesto o intentado demostrar, por la parte contraria. Si se enfrenta el apoderado de una de las partes a una probanza sobre estos temas de especialidad informática, se considera que su deber es obtener los medios para controvertirlo, naturalmente, acudiendo al perito en las materias antes aludidas. Es más, es una obligación ética la de procurar por los medios legalmente preestablecidos, defender a su poderdante mediante su utilización. Así lo establece en el listado de deberes, la Ley 1123 de 2007 o código disciplinario del abogado, para la administración de justicia.

Otro deber del apoderado en derecho de familia según el Código General del Proceso es, conservar en su poder las pruebas y la información contenida en mensajes de datos que tenga relación con el proceso y exhibirla cuando sea exigida por el juez, de acuerdo con los procedimientos establecidos por este código, que, en determinado momento, requerirá de su autenticación, de ser menester, por los medios propios o protocolarios dictados para esta clase de mensajes de datos.

Es requisito para el contenido de la demanda, la petición de pruebas que se pretenda hacer valer cuando estos medios probatorios sean de índole informática; como prueba pericial tiene formalidades específicas que más adelante veremos. Aquel requisito nos hace reflexionar sobre la importancia de solicitar o de allegar oportunamente junto al libelo de la demanda, el informe pericial elaborado por el experto para luego debatirse en audiencia pública, oral y concentrada. La eficacia de una demanda entonces estará signada por la procedencia, objetividad e incorporación de esta clase de pruebas periciales, depende de la petición probatoria, de los informes o dictámenes

adjuntos y de su mérito probatorio frente a una decisión del juez de familia. Y es notoria en el Código General del Proceso la introducción de mecanismos o medios relativos a la informática o a los medios virtuales o evidencias digitales, por ejemplo, para la presentación de la demanda se alude al mensaje de datos para el archivo del juzgado, mensajes especializados que exigen del conocimiento de los expertos, en el evento de cuestionarse como medio documental. Tema que enseguida se toca para el traslado de la demanda, que se surtirá mediante la entrega (copia de la demanda y sus anexos) o como mensaje de datos. Constituyendo estos elementos de los mensajes de datos, una eximente que depende del juez al señalar el legislador que, atendiendo las circunstancias particulares del caso, podrá excusar al demandante de presentar la demanda mediante mensaje de datos, como lo enuncia el Decreto 806 de 2020, (2020), en su artículo número 6, establece importantes disposiciones sobre la admisibilidad de pruebas en los procesos judiciales. En este sentido, se señala que el demandado tiene el derecho de ejercer la contradicción mediante la solicitud de las pruebas que pretenda hacer valer. Esto es crucial, ya que la efectividad de este derecho está relacionada con los aspectos fácticos que se están tratando en el caso. De manera lógica y prudente, se destaca la necesidad de incluir la prueba pericial, que puede ser fundamental para esclarecer los hechos en disputa.

3.5 Código General del Proceso y la tecnología

El uso de las tecnologías de la información y las comunicaciones por el legislador en la sección segunda del Código General del Proceso permite que se asevere sin temor alguno que la modernidad del sistema se debe concebir, aceptar y practicar dentro de los procesos de derecho privado o derecho de familia. Las TIC son necesarias para el procedimiento judicial que se ha convertido obligatorio, al estipularse que, como garantía se trata al principio en esta publicación.

La ley procedimental prescribe que, las actuaciones judiciales se podrán realizar a través de mensajes de datos y registra, a

su vez, la siguiente obligación funcional: La autoridad judicial deberá contar con mecanismos que permitan generar, archivar y comunicar mensajes de datos. Situación que requiere del conocimiento de la materia tratada como necesaria no solo para trámite procesal sino para la presentación y producción probatoria; siendo sumamente importante que la misma normativa en estudio, 103 del Código General del Proceso, remita este contexto a la Ley 527 de 1999 permitiendo su aplicación o las normas que las sustituyan o modifican. Se establece como lo que se ha venido mencionado, el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Normatividad donde se estructura el ámbito jurídico, que autoriza los mensajes de datos en todas las actividades públicas.

Sistema operativo que en estos momentos ha sido aplicado por el gobierno nacional en cuanto a la rama judicial. Por ejemplo, se tiene el Decreto 806 de 2020, mediante el cual se dio inicio a actividades judiciales en los juzgados civiles y de familia, indicándose que ante la eventualidad que hoy en día se vive en el país y en el mundo, es importante resaltar como la rama judicial tuvo que acudir a la normatividad arriba enunciada reforzando la Ley 1564 de 2012, apoyando los medios tecnológicos como WhatsApp, correos electrónicos y otros, valiendo como pruebas éstos dentro de un trámite judicial; es así que conlleva a que la ciencia viene evolucionando, es decir la justicia no se puede quedar corta cuando son asomadas estas clases de pruebas que son de gran aporte y evidencias dentro de los procesos para esclarecer la verdad y que los jueces puedan aplicar bien a través de sus fallos una justicia justa.

Es relevante e importante tener en cuenta que los profesionales del Derecho como los jueces, no estaban preparados para el gran reto de la virtualidad y demostraron no ser inferiores cuando a estos se refiere, como lo fue esta nueva modalidad de justicia, es decir los abogados litigantes se han convertido en abogados virtuales con el nuevo instrumento jurídico como el Decreto 806 de 2020, donde se enuncian las medidas digitales en las actuaciones judiciales, como también hay que tener en cuenta la circular 041 de 2020 emitida por el Ministerio de

Protección Social, que otorgó los lineamientos para el trabajo en casa. Entre otras disposiciones ha incentivado el uso de las tecnologías de la información en el litigio.

Lo anterior, incluyendo el desarrollo de las actividades judiciales como los apoderados desde sus vivencias, en el cumplimiento de los objetivos que no vienen a implicar mayores modificaciones a las obligaciones contractuales de las partes, logrando la búsqueda del equilibrio con la vida familiar, regulación de jornadas y riesgos profesionales sin descuidar a los usuarios.

Hasta hace poco la excusa o lo que no se escuchaba era la falta de regulación, la carencia de iniciativa de la rama judicial para propender por la modernización del litigio y la inoperancia del sistema para asumir la modernidad. Puede decirse que hoy se cuenta con las herramientas para ello, con algunas falencias claro está, pero con el sentido de apropiación con gran responsabilidad para los abogados litigantes como para los funcionarios que imparten justicia. Es un deber de todos los actores continuar con el esfuerzo para que la virtualidad prospere, pero en los litigantes está tomar este reto como una derogatoria de conocimientos o una renovación de estos, adquiriéndose los aprendizajes técnicos que no se habían implementado en la cotidianidad.

Esto hace parte del plan de justicia, integrado por todos los procesos y herramientas de gestión de la actividad jurisdiccional por medios de las tecnologías de la información y las comunicaciones, que permitan formar y gestionar expedientes digitales y el litigio en línea. Se presumen auténticos los memoriales y las comunicaciones cruzadas entre las autoridades judiciales y las partes o sus abogados cuando sean originadas desde el correo electrónico suministrado en la demanda o en cualquier otro acto del proceso, sin embargo, se afirma que cuando se presente alteración, omisión en el envío, desvío o efecto similar, en estos documentos electrónicos se requerirá de la prueba mediante expertos.

El código prevé que cuando refiere al uso de correo electrónico, dirección electrónica, medios magnéticos o medios electrónicos, se entenderá que también podrán utilizarse otros sistemas de envíos, transmisión, acceso o almacenamiento de mensajes de datos, siempre que garanticen la integridad del intercambio o acceso de información. Garantía o prerrogativa que de no cumplirse requerirá naturalmente de la intervención de un perito como se está reclamando de la justicia en derecho de familia, en cuanto a la prueba dentro de los procesos de esta competencia.

Pueden darse muchas situaciones para la intervención de los peritos en estas lides, como, por ejemplo, en las grabaciones de las audiencias que deben hacerse en medios de audio, audiovisuales o en cualquiera otro que ofrezca seguridad para el registro de lo actuado. Circunstancia que traslada el pensamiento a eventuales casos donde no se produzca dicha seguridad, que no grabe el sistema, se manipule o altere, se falsifique de cualquier forma, y que conduce a concluir que ante estas situaciones es menester que un experto o técnico ofrezca la explicación de lo acaecido.

La intervención de las partes es permitida por la ley y por el juez, a través de videoconferencia o teleconferencia o por cualquier otro medio técnico; es sistema que se arraiga en nuestra legislación de civil y familia y que por su especialidad permite escribir que los equipos modernos y tecnológicos deben ser frecuentes en el procedimiento regulado por el código general bajo examen. el cual obliga al despacho judicial a mantener el buzón del correo electrónico con disponibilidad suficiente para recibir los mensajes de datos y permitir que las comunicaciones se lleven a cabo a través de mensajes, al punto que el legislador habla de la justicia digital al anotar sobre la formación de los expedientes.

Entonces, el aserto que proviene de lo anterior es que la tecnología es parte de la operatividad de la justicia. Descendiendo a la práctica de la prueba especial o por medio de expertos, ha de seguir estos lineamientos y los que se registren sobre la prueba pericial. Existe un régimen probatorio, se habla de

la necesidad de la prueba porque toda decisión debe fundarse en las pruebas regular y oportunamente allegadas al proceso y dentro de los medios probatorios, se tiene la declaración de parte, la confesión, el juramento, el testimonio de terceros, el dictamen pericial, entre otros. Este último es el que ocupa nuestra atención en el presente compendio.

Incumbe a las partes probar el supuesto de hecho de las normas que consagran el efecto jurídico que ellas persiguen. Pero esto no obsta para que el juez pueda, según las particularidades del caso, de oficio o a petición de parte, distribuir la carga al decretar las pruebas durante la práctica o antes de emitir la sentencia. Puede exigir el juez la demostración de determinado hecho a la parte que puede hacerlo también, como puede el funcionario equilibrar o distribuir esta carga probatoria que procede de la argumentación en pro de la verdad y la respuesta de la administración de justicia, en espera de la plena convicción de lo acaecido o pretendido mediante la prueba pericial por medio de expertos. Si las pruebas son útiles para la verificación de los hechos relacionados con las alegaciones de las partes, permitiendo en acoger los medios de los peritos en los casos que sean necesarios, y lo es, cuando trate el debate de temas especializados de las TIC.

En cuanto a la apreciación de las pruebas en conjunto y de acuerdo con las reglas de la sana crítica, debe conforme a la ley exigirse al juez el cumplimiento de las exigencias o solemnidades prescritas en la ley sustancial para requisito o validez de ciertos actos; requerimiento de los protocolos que existen por normas legales o manuales oficialmente socializados por el Estado en cuanto a los elementos probatorios que corresponden al derecho informático.

3.6 Código General del Proceso y prueba pericial

La prueba pericial está regulada en el artículo 226 de la obra que se ha venido estudiando in extenso en el presente escrito. Dice la norma que es procedente esta prueba para verificar hechos que interesen al proceso y requieran especiales conocimientos

científicos, técnicos o artísticos. En la propuesta de los peritos en informática podría catalogarse de expertos científicos o técnicos. Se elabora por el perito un dictamen el cual describe el hecho especial que requirió de su intervención; informe pericial sobre hechos y no sobre puntos de derecho que son los que conoce y aplica el juez o magistrado.

Los escritos, llámese informe pericial o dictamen, serán rendidos bajo la gravedad del juramento que se entiende prestado con la imposición de su firma en dicha manifestación escrita. La opinión que expone es independiente y debe corresponder a su convicción profesional. Debe el perito adjuntar a su dictamen o informe los documentos que le sirven de soporte o sustento a su manifestación pericial, igualmente los que demuestren su idoneidad o experiencia. Manifestación que debe ser clara, precisa, exhaustiva y detallada, debiendo explicar los exámenes, métodos, experimentos e investigaciones realizadas, exigiéndose del perito que explique los fundamentos técnicos o científicos de sus conclusiones. En estos requisitos se concentra las exigencias especiales del experto; en el caso de ingeniero o profesional idóneo en materia de la informática, habrá de acreditar y cumplir con la ley y los reglamentos de su profesión o especialidad. Es menester escribir la profesión u oficio, por lo mismo, que se ponderan junto a los documentos idóneos que lo habilitan para ese ejercicio pericial, los títulos académicos y evidencias para demostrar la respectiva experiencia profesional o técnica.

He aquí la importancia de la idoneidad o capacitación o profesionalismo del perito que emita un dictamen dentro de un proceso adelantado por el juzgado de familia, en la casuística arriba enumerada; máxime que la ley pide del perito, la lista de publicaciones relacionadas con la materia del peritaje, si las tuviere. Exigencia que reflejará en el evento de existir dictamen pericial, por la parte contraria ante el juez, cuál es el que se aproxima a la verdad o posee la credibilidad para dar por demostrado un hecho que requiere de conocimientos científicos o técnicos. En toda esta requisitoria saldrá avante la prueba pericial que lleve la convicción al fallador. Cuando la experiencia

del perito es extensa, con mayor razón, y por esto la ley pide que se allegue la lista de los casos en que haya sido designado como perito o en los que haya participado en la elaboración de dictamen pericial en los últimos cuatro años.

En materia del derecho de familia; en las disputas, los conflictos y motivos de demanda ante los estrados judiciales, se presentan situaciones en las que se ofrecen pruebas digitales, mismas que corresponden a publicaciones por las redes sociales, mensajes de WhatsApp, grabaciones de voces o videos tomados por medio de celulares, que se aportan sin los protocolos de la informática. La violencia entre las personas o entre las parejas de casados o en unión marital de hecho, por las redes sociales y por medios del sistema de teléfonos móviles es frecuente y, cuando se presentan como evidencia ante el juez de familia, por ejemplo, para demostrar infidelidad de alguna de las partes, no se cumple con las exigencias del derecho informático.

Esto conforma la violencia digital que campea en la sociedad actual a raíz de la tecnología de la TIC. Son acciones deliberadas que se dirigen hacer daño a otros, como utilizando medios de comunicación y redes sociales; fenómeno que perjudica la convivencia ciudadana.

Cada vez es más común que las víctimas denuncien casos de ciberacoso, hostigamiento, amenazas, insultos, vulneración de datos o información privada, divulgación sin consentimiento de contenido sexual, entre otros. Colombia avanzó en materia legal al contar con la Ley 1620 de 2013, que creó el sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos, en función de combatir el fenómeno de la agresión en las redes hacia los escolares. Al igual que México, que incluyó la Ley General de Acceso a las Mujeres a una vida libre de violencia, incorporando la violencia digital como un tipo de acción hacia las mujeres.

Los derechos humanos que descienden al derecho privado o de familia, entre ellos, los derechos de las mujeres y de los niños han de ser protegidos y cobijados con el amparo judicial, a su

vez, para evitar a futuro la inadmisión, exclusión de medios de prueba en debates ante el juez de familia por no cumplirse con las exigencias legales. Al presentar evidencias sobre esta clase de hechos, debe implementarse o aplicarse los seguidos, por ejemplo, por los jueces penales colombianos a costa y riesgo que en alguna oportunidad procesal se vaya a desconocer pruebas de mensajes de WhatsApp, Cd, donde se traslada una llamada telefónica necesaria para la probanza de un hecho en derecho de familia o un video publicitado por las redes sociales o medios digitales.

Se ha observado en los juzgados de civil y familia, respecto de estos sistemas o tecnologías o evidencias que se han dejado de lado; no se incursiona en las tecnologías desde el punto probatorio del peritaje informático.

Como ejemplo en este terruño, se tiene el proceso ejecutivo hipotecario que se tramitó en Juzgado Civil Municipal, allí, el demandado aportó como elemento probatorio dentro de su contestación de la demanda como defensa, un audio donde corroboraba que el demandante le había cobrado intereses excesivos superando los que había establecido en la escritura de hipoteca; ante esa evidencia el juez dentro de su pronunciamiento, emite que la contestación dio cumplimiento con las formalidades prescritas en la ley; se le dará el valor probatorio en el momento procesal oportuno. Pero con respecto a la prueba del audio es rechazada de plano por ser violatoria al debido proceso (artículo 29 de la Constitución Nacional), argumentando que la aquí demandada tomó esa prueba después que se notificó de la demandada, y más cuando se está violentando el debido proceso; enuncia que la jurisprudencia de la honorable Corte Constitucional ha señalado que el operador judicial incurre en una vía de hecho, por defecto fáctico cuando somete a la valoración probatoria un elemento probatorio ilegal o inconstitucional.

La prueba ilegal es definida por la Corte Constitucional como aquella recaudada, practicada y valorada en contra de las normas propias de cada juicio. Ahora bien, la nulidad de pleno

derecho que, en vigencia del Código de Procedimiento Civil, llamó supralegal por no estar contemplada en la ley y si en norma superior, como ocurría frente a la prueba obtenida con violación al debido proceso; en la actualidad, con la entrada en vigor del nuevo estatuto de ritos civiles (Ley 1564 de 2012), está reglada en el artículo 14 del Código General del Proceso.

Ante el pronunciamiento emitido por el fallador, se genera la duda si es al caso que el mismo está realizando defensa hacia la parte que considera que se le vulneró un derecho constitucional, cuando es deber de su apoderado realizarlo, dejando que el mismo derecho constitucional en su articulado señalado en su artículo 13, nos remite que todas las que personas nacen libres e iguales ante la ley y recibirán la misma protección y trato de las autoridades.

Es evidente que sí se vulnera un derecho a la persona lesionada, constituye situación que se agrava por no existir normatividad clara contenida en este tipo de situaciones.

Una de las consecuencias de la aceleración digital que trajo la pandemia, es que prácticamente todo está alojado en este ecosistema. Esto es procedente también para las pruebas de los delitos pues en la eventualidad, cuando se quieran denunciar situaciones donde exista extorsiones o amenazas enviadas por medios electrónicos, el elemento probatorio será virtual.

De acuerdo entonces con la apreciación que lo anterior ha hecho que cobre cada vez más importancia la certificación de evidencia digital y prueba de esto, es el crecimiento de compañías dedicadas a ello como Adalid, Ratsel, FTI, Forensictic o Investigaciones Estratégicas.

Tema que refuerza nuestra orientación en el sentido de requerir en todo estrado judicial o administrativo para la validez de las evidencias digitales, en este caso de los mensajes de WhatsApp, del experto, o perito informático que posea esta especialidad o capacitación. Por cuanto, no solo es exigencia legal la expedición de la correspondiente certificación, sino que deberá

en determinados casos, el experto declarar en su condición de perito en la audiencia de juzgamiento.

El perito de la parte contraria podrá demostrar que el mensaje escrito, de voz o un video, no son auténticos o que se pudo manipular o alterar, desaprovechándose una pretensión civil o de derecho de familia por esta circunstancia. Existen diferentes programas para editar y modificar todo, por eso, a diferencia de lo que sucede en países como Ecuador, la evidencia en Colombia solamente se admite como prueba directa confirmatoria si hay un análisis pericial que garantice que la huella digital del documento no ha sido alterada y se conserva su autenticidad.

Para cumplir los requisitos de validez jurídica se deben tener las siguientes condiciones: estar escrito, es decir, que se pueda acceder en su formato original y estar firmado.

En la legislación privada o el derecho de familia, el demandante, el demandado o el juez, no podrán desconocer esta exigencia que, en el caso de la evidencia digital, requiere la certificación del experto pues el mensaje de datos aportado como evidencia debe mantenerse original e íntegro, lo que quiere decir que debe estar completamente inalterada la información que contiene. Esto se hace a través de un hash, (ya explicado).

3.7 Decreto 806 de 2020 y su implementación tecnológica

De igual manera, se considera que, por el problema de la pandemia, se incrementó el uso de los medios tecnológicos, sin embargo, con su aplicación no podrá permitirse la vulneración de la Constitución o de la ley sobre el Decreto 806 de 2020, dictado por el gobierno nacional; puede predicarse que este antes mencionado, surgió por la necesidad de que los procesos judiciales siguieran dividiéndose en tres pilares como son:

1. Prácticas relacionadas con el deber y facultad de dar uso a las TIC en sus actuaciones virtuales y presenciales.
2. Disposiciones concernientes con las reglas generales de

ordenamientos en los expedientes, poderes, demanda, audiencias, notificaciones personales, traslados, emplazamientos, comunicaciones, oficios, despachos, aplicación de recursos ya sea autos o sentencias en lo que concierne a la materia civil y familia.

3. En lo que tiene que ver a los trámites en la jurisdicción Contenciosa Administrativa y Jurisdicción laboral.

Se resalta en el marco normativo de este decreto, que, como regla general, todas las actuaciones judiciales se deben tramitar a través de los medios virtuales y casos excepcionales de forma presencial, lo que viene a entenderse, que en todas sus prácticas y disposiciones judiciales se complementan las normas procesales vigentes.

El objeto, uso y deber de los sujetos procesales en relación con la tecnología de la información y las comunicaciones, se deriva de lo enunciado en el artículo 1°, cuyo fin es agilizar el trámite de los procesos judiciales ante la jurisdicción ordinaria civil, familia y laboral.

Es importante resaltar en este compendio, los objetivos centrales del decreto en mención, como es ver la necesidad de las tecnologías en toda actuación judicial, agilizar los trámites judiciales y flexibilizar la atención de los usuarios. Este decreto viene a ser complementario a los estatutos procesales vigentes; dentro de su marco normativo procura por regla general que todas sus actuaciones judiciales se tramiten por los medios virtuales a excepción de manera presencial.

Por lo que es comprensible, este Decreto 806 de 2020, se creó con el fin de lograr mitigar los efectos de la pandemia en la administración de justicia, a efecto de que los abogados entren en comunicación directa con los colaboradores de los despachos judiciales para que puedan encontrar alternativas y soluciones concretas a sus casos.

El Decreto 806 de 2020 hace un señalamiento concreto y determinante en lo que refiere a toda la documentación requerida

establecida en el artículo 82 del Código General del Proceso. Si se aporta en una demanda o en el discurrir del proceso un documento, en primer lugar, él podrá gozar de la presunción de autenticidad, que se infirma o desvirtúa mediante la tacha de falsedad por la parte interesada. Operación que se podrá realizar al momento de la contestación de la demanda o en la audiencia en la que el juez ordene tenerlo como prueba.

La necesidad del dictamen pericial es indefectible. Retomando lo que corresponde a las pruebas periciales en materia civil familia, se cita en alusión el artículo 228 del Código General del Proceso, sobre la contradicción; la parte que lo aporte podrá solicitar que comparezca el perito a la audiencia igualmente, aportar otro o realizar conjuntamente dentro del término de traslado del escrito con el que haya sido aportado o, en su defecto, dentro de los tres (3) días siguientes a la notificación de la providencia que lo ponga en conocimiento.

En virtud de la anterior solicitud o si el juez lo considera necesario, citará al perito a la respectiva audiencia, en la cual el juez y las partes podrán interrogarlo bajo juramento acerca de su idoneidad e imparcialidad y sobre el contenido del dictamen. La contraparte de quien haya aportado el dictamen podrá formular preguntas asertivas e insinuantes. Las partes tendrán derecho, si lo consideran necesario, a interrogar nuevamente al perito en el orden establecido para el testimonio. Si el perito citado no asiste a la audiencia, el dictamen no tendrá valor.

Ante lo expuesto, forzoso es concluir que, el Código General del Proceso regula cómo dar aplicabilidad a ciertas pruebas periciales con su trámite, desarrollo y validez dentro de un proceso judicial. En la actualidad, es de resaltar cómo el gobierno nacional recientemente expidió normatividad, por ejemplo, la Ley 2108 del 29 de julio del 2021, en la que establece que el internet es un servicio público de telecomunicaciones, de manera eficiente, continua y permanente, permitiendo la conectividad de los habitantes del territorio nacional, en especial de la población que, en razón a su condición social o étnica se encuentre en situación de vulnerabilidad o en zonas rurales y apartadas.

Cambios traídos por la Ley 2213 del 2022, el decreto 806, que estipuló la implementación de la TIC en el sistema de justicia en Colombia durante la pandemia a través del Decreto 417 del 2020, para seguir con la virtualidad, siendo el complemento y apoyo en la rama judicial, de esta manera no se elimina la atención presencial dentro de los juzgados.

Lozada (2019) se presentó una situación en la que un celular perteneciente a una señora contenía evidencias que podían comprometer su privacidad. La señora argumentaba que el dispositivo era de su propiedad y se negaba a entregarlo, dado que estaba registrado a nombre de la empresa compartida con su esposo. Sin embargo, gracias a la política de seguridad de la empresa, se logró acceder al celular para realizar un peritaje.

Este caso ilustra el derecho a la intimidad puede entrar en conflicto con el tratamiento de datos personales. En este sentido, el funcionario judicial optó por otorgar pleno valor probatorio a la evidencia digital, considerando los acuerdos previamente establecidos en materia de protección de datos.

3.8 La doctrina y la prueba pericial en materia de derecho civil y familia

La prueba en derecho, según el maestro colombiano Rocha (1967), destacó el sistema probatorio denominado dispositivo y la función y actividad del juez civil en el proceso probatorio, al recalcar que existe una carga para la parte demandante, demandada y su razón de ser. La actividad de la parte, cuando la ley le impone una carga en la instrucción del litigio, le es útil, en primer lugar, a esa parte interesada en la verificación del hecho y, además, asegura el rendimiento del proceso así impulsado, para poner al juez en la condición de proveer o fallar con conocimiento de causa. La actividad del juez no se agota con la demanda y su respuesta, sino que continúa en el proceso de instrucción o verificación de los hechos (término probatorio), y luego en la aducción de las razones de estos hechos relacionadas con el derecho que invocan (término para alegar de bien probado). Los tratadistas señalan que existen

tres cargas: la carga de la razón, la carga de la prueba y la carga del impulso procesal.

El profesor Brichetti (1985), señaló que también el legislador civil en su normativa y modificaciones exigen que hecho determinados para producir rotundas consecuencias, sean evidentes, como cuando permite al padre del menor - en el ejercicio de la patria potestad- realizar actos que excedan de la simple administración sólo por causas de la necesidad o de utilidad evidente y previa autorización del tribunal cuando permite la continuación del ejercicio de establecimiento de comercio o de industria que se encuentre en el patrimonio del menor, cuando exista la evidente utilidad del menor; normativa anterior exigía un grave y evidente motivo de utilidad general de la comunidad, el deudor que quiere hacer restringir una ejecución como excesiva debe, con prueba rápidas y clarísimas justificar el exceso).

El autor nombrado señala igualmente, refiriéndose a los procesos penales y civiles, que hay diferencia de uno al otro; la principal es que no es igual el carácter de la objetividad porque el procedimiento civil comporta distinción del hecho en su exterioridad, con ello evitando lo correspondiente a las personas y sus móviles, mientras que el procedimiento penal refleja su carácter subjetivo, intenta cautivar el hecho en su totalidad centrándose en el aspecto intencional o culposo como valor moral del hecho.

Se ha considerado a través del tiempo, que el juez civil - en nuestro tema- el juez de familia aparentemente desempeña o ejerce una función o rol de relativa inactividad en los litigios que se presentan a su consideración. Es apariencia porque le compete vigilar y dirigir la ordenación del proceso, analizar las peticiones probatorias, admitirlas o no, decretar las pruebas pertinentes y conducentes y que ellas se produzcan o cumplan con los ritos previstos en la ley; en el caso del objeto de este texto argumentativo sería la ritualidad de la prueba pericial, específicamente, el dictamen informático.

La primaria actitud del juez de derecho privado es receptora; es una persona que escucha antes de hablar - la voz es de las partes

y el oído es del juez- como lo decía Carnelutti (1994). Recibe el juez las demandas, las aseveraciones y las demostraciones así sean por los escritos demandatorios, exigiéndose del juez paciencia, vigilancia e imparcialidad. Debiendo considerar con sus limitaciones, en una segunda fase, la verificación de las afirmaciones de las partes con mayor inmediación mediante el contacto con las pruebas, para luego apreciar cada medio probatorio respecto del grado de verdad que ellos muestren. Procedimiento que, por el cúmulo de trabajo en los despachos de los jueces de familia, se tornan en determinadas ocasiones muy fugaz, cuando se considera sencillo lo debatido, a sabiendas que en derecho de las personas lo controvertido es primordial, con tramas o conflictos graves como o cuando se tiene por objeto el amparo de derecho de los niños.

Reconoce que la tarea no es fácil, menos cuando las pruebas son muchas y de variada condición, como cuando se trae al estrado la prueba pericial, la cual se controvierte por la otra parte, requiriéndose de la apreciación de todas las pruebas por separado, contactándolas o relacionándolas unas con otras; de comprobar un orden de deducciones con otro, tener cuenta cuidados de los detalles, escoger con cautela las reglas de la experiencia, vigilar con atención los enlaces de los silogismos. Basta pensar en la apreciación de una prueba testimonial un tanto compleja para comprender dicha dificultad y valor, dice el clásico Carnelutti (1994). mayor complejidad podrá presentarse y debatirse o incorporarse un peritaje informático.

El tratadista español Climent (1999), luego de dar opinión sobre la prueba pericial, indica que “Partiendo de las anteriores definiciones, o de cualquier otra, de similar factura, conviene examinar los aspectos esenciales que definen la actividad pericial. Ha de puntualizarse, de antemano, que tales aspectos son referibles tanto a la pericia civil como a la penal y, en general, a la realizada dentro de cualquier orden jurisdiccional”. La doctrina más prestigiosa viene admitiendo que, salvo peculiaridades accidentales, no existen diferencias entre la pericia civil y la penal. El proceso penal presenta como particularidad diferenciadora digna de mención, la pericia practicada en fase de instrucción

sumarial, que se sujeta a unas reglas muy específicas, pero la prueba pericial practicada en la fase plenaria del proceso penal -esto es durante el juicio oral- no ofrece especialidad ninguna que la diferencie verdaderamente de la pericia practicada en el proceso civil.

La Suprema Corte colombiana en casación penal de abril 22 de 2015, Radicado 45711, con ponencia del doctor Eugenio Fernández Carlier, (2015), diferenció al testigo técnico del perito en materia de derecho de familia que ocupa estos acápites, indicando que el artículo 227 del Decreto 1400 de 1970, reiterado en el 220 de la Ley 1564 de 2012, prevé la práctica del testimonio disponiendo que el juez debe rechazar las preguntas que traten de provocar conceptos de testigo, excepto cuando la persona sea especialmente calificada por sus conocimientos científicos, técnicos o artísticos sobre la materia.

La doctrina especializada como en el espacio del procedimiento civil, escoge esta figura del testigo técnico, se traslada a la jurisdicción penal, definiéndolo como aquello que percibe los hechos materia de investigación y en virtud de su especial cualificación o conocimiento técnico o científico, puede agregar a su declaración en juicio, apreciaciones afines a estos que enriquecen el esclarecimiento para aplicación de justicia. Por consiguiente, este escrito, nos inclina entonces, no solo a distinguir testigo de perito, sino a relievar la necesidad de capacitar a los últimos para el ejercicio científico o técnico en informática.

Puig (2015), enseñó sobre la prueba pericial informática en el procedimiento civil que, respecto a la prueba electrónica se subsistan controversias, especialmente relacionados con los medios de comunicación masiva como son los correos electrónicos, el WhatsApp, redes sociales que no se han contemplado de manera amplia en el derecho privado, debiéndose analizar el origen del hecho electrónico y su concepción científica o técnica, el modo, los medios y el sustento en que se conserva y los dispositivos para su reproducción, entrándose con ello al ámbito jurídico procesal de estos temas electrónicos para allegar a su valoración como prueba pericial.

Pasos o fases que ahora se tratarán de manera similar, al estudiar estos temas ante los estrados judiciales penales y de derecho civil familia.

Se trae a colación el fallo de unificación de la Corte Constitucional colombiana sobre los intermediarios de internet y las plataformas digitales, en la sentencia SU-420 del 2019, donde define a los intermediarios de internet e indica el rol de las plataformas digitales, el pasivo que facilita el proceso de transmisión y difusión no tomando decisiones sobre estas últimas. Por consiguiente, con relación a la honra y al buen nombre en las pagina Web o buscadores de internet, distingue la condición del responsable de la trasgresión delictiva, teniendo en cuenta la plataforma mediante la cual se efectúo la publicación.

Al resolver un recurso de casación en el cual, entre otros asuntos, se debatió la responsabilidad por los comentarios públicos de un blog, la sentencia SC-52382019 del 10 de diciembre del 2019 de la Sala de Casación Civil de la Corte Suprema indicó:

> Que no habrá responsabilidad por los comentarios dejados en un blog, a no ser que resulten humillantes e injuriosos o calumniosos. Los blogs, facilitan el intercambio de comentarios que pueden ser deshonrosos, obligando a los administradores de estos sitios evitar tales publicaciones o eliminarlos si ya fueron difundidos, de lo contrario, se conformaría la responsabilidad civil por culpa probada. (Corte Suprema de Justicia, Sentencia SC-52382019, 2019, s/p)

Responsabilidad compartida que amerita conocimientos precisos ante los eventos de incursionar en eventuales demandas de carácter civil; empero, las vulneraciones que se aluden en estas providencias operan frecuentemente en el campo de las relaciones de familias que pueden desembocar en la necesidad del peritaje informático para la legal y regular demostración del hecho y del perjuicio o daño ocasionado con el comportamiento delictivo o policial o ético.

Se necesita de la administración o impartición de justicia, así se viva en época difícil por la pandemia y la cuarentena obligatoria. La tecnología referida en el Código General del Proceso como sistema o medios aplicables en los procesos civiles y de familia han de ayudar a su tramitación, evitándose la paralización de las actuaciones judiciales. El proceso y el expediente digital fue vislumbrado por el legislador, pudiéndose de manera electrónica hacer realidad lo que no se esperaba.

La tecnología desplaza al expediente en físico o al papel, sistematiza mediante la digitalización la actuación procedimental utilizándose para su seguimiento el computador. Sin embargo, a pesar de estar de acuerdo con esta modernidad, al lado de algunos críticos podemos lanzar la opinión que la presencialidad es necesaria por los factores conocidos del principio de inmediación probatoria.

Se requerirá entonces de un banco de datos, la seguridad en el manejo del recibimiento de demandas, su contestación; haciéndose dificultosa la práctica de pruebas como la especializada de peritaje informático o similares, el trabajo mecanizado en esta clase de medios probatorios no permite clara, científica y sicológicamente la percepción directa mediante el principio material de la inmediación, lo expuesto o declarado por el perito. Como tampoco se tiene a la mano la ponderación de quien rinde un testimonio, cuando la misma ley exige que sea el declarante un perito o experto.

No desconocen que la solución de automatización judicial es posible, solo anota el sentir del clamor general sobre la necesidad de la prueba, pero mediante la percepción del juez, que pueda observar del perito, palpar su experiencia o credibilidad.

Es cierto que el sistema digital o electrónico permite que se llegue pronto al despacho judicial con una demanda o su contestación, como primera fase ya tratado en párrafos anteriores, pero la verificación por parte del juez, la práctica de las pruebas, su contradicción o confrontación, su incorporación y oposición, exige del administrador de justicia la connotada y universal prerrogativa de la inmediación.

El trámite frío y de alguna manera mecanizado, alcanzará sus bondades. Se desea que, de ser beneficioso para la administración de justicia, se lleve a cabo, preparándose los operadores judiciales y sus coadyuvadores, más si se tiene en cuenta que la ley procedimental civil alude a la prueba pericial por cuestiones científicas o técnicas.

Enumera enseñanza relevante que, algunas de las nuevas tecnologías que tendrán un gran impacto en la justicia durante los próximos años serán, la inteligencia artificial en la justicia, la operación en la nube y los trabajos digitales que más adelante se tratarán. Significa entonces la anotación anterior que, se requerirá con mayor capacitación o idoneidad de la informática o del derecho informático, no solo para los debates probatorios, sino para que los jueces y los funcionarios de la rama judicial, apliquen la ley con el cabal cumplimiento de las avanzadas tecnologías enumeradas.

Analizado el expediente, dice el profesional, “observamos que el Juzgado de Familia le admitió a la excónyuge un informe oficial de nuestro cliente, sin Certificado Forense de Origen, pues siempre se debe establecer el origen, su legalidad, integridad y autenticidad”. Señala que el juez de familia tenía que exigírselo si se tiene en cuenta que la naturaleza del documento es digital, en razón a que fue descargado de la plataforma electrónica de la @PoliciaColombia, mecanismo.

El juez en la etapa de descubrimiento de pruebas, como en los casos del uso máximo de elementos electrónicos para su producción, su deber es preguntar por su origen para detectar si es ilegal o ilícita su obtención. En este caso el apoderado de la excónyuge debió acreditar los ingresos de la parte contraria y debió haber requerido del despacho que oficiara a la institución policiva la certificación correspondiente.

Debió primar la orden constitucional sobre toda apreciación judicial de carácter probatorio, aplicando lo previsto en la parte final del artículo 29 de la carta magna colombiana: “Es nula, de pleno derecho, la prueba obtenida con violación del debido

proceso. Sabiéndose que el debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas".

Como secuela de lo precedente, se concluye que no existe desface cuando se insinúa, en derecho de familia, en las controversias adelantadas ante los jueces de esta área, debe existir la especialización o la capacitación continua en derecho informático. El perito idóneo dará luz a la justicia; llevará convicción al juez para obtener la certeza , la evidencia y seguridad a su decisión, especialmente la final denominada fallo o sentencia. En la audiencia correspondiente cuando sea citado el perito como prueba de alguna o de las dos partes o por el juez de oficio, al exponer sus puntos de vista o su opinión profesional, contiene su escrito, emana una de las pruebas, por su cientificidad o tecnicismo, despejan cualquier duda frente a la diversidad de pretensiones. De oficio, como hemos visto, podrá el juez ordenar esta clase de pruebas, indicando la ley que, para la designación deberá acudir preferiblemente a instituciones especializadas o privadas de reconocida trayectoria o idoneidad. Acudir a entes del Estado o de particulares, que no podrán actuar si no poseen las cualidades o condiciones del código exige y enumerado en párrafos anteriores. Es de recalcar, el juez podrá decretar de oficio los servicios de entidades o dependencias oficiales para la obtención de dictamen pericial. El juez es experimentado, sin embargo, existirán casos, como la especialidad de la informática o de las TIC, entre otras, requerirá del experto, en ciertos eventos.

La prueba que ha de decretar de oficio el juez cuando tenga la necesidad de aclarar o precisar hechos que requiere de conocimientos especiales para su práctica, basta con el cuestionario que el perito debe absolver, a quien se le podrá sufragar honorarios, sin embargo, el legislador va más allá y dice que si no se hiciere la consignación el juez podrá ordenar al perito que rinda el dictamen si lo estima indispensable. Es la necesidad de la prueba pericial lo que llevará al juez a buscar herramientas para la eficaz administración de justicia. Es la misma ley la que ofrece todos estos mecanismos o ayudas al juez y por esto mismo en casos de comportamientos informáticos,

debería acudir a ellos. Ya que con estas pruebas proporcionan una herramienta para esclarecer la verdad y así el juez puede aplicar como herramienta la hermenéutica jurídica que conlleva a emitir un fallo en justicia.

Por otra parte, los abogados litigantes podrán tener un resultado más rápido en los procesos y no como antes que duraban años para que los jueces fallaran. Por lo contrario, cuando se demandó la normatividad del Código General del Proceso sobre la carga probatoria y la facultad del juez para aliviarla o determinarla, la Corte Constitucional señaló que una de las principales cargas procesales, cuando se acude a la administración de justicia en general y a la jurisdicción civil, en particular, es la concerniente a la prueba de los hechos que se alegan. La carga de la prueba es un elemento característico de los sistemas procesales de tendencia dispositiva. Se conoce como principio onus probandi, el cual indica que por regla general corresponde a cada parte acreditar los hechos que invoca, tanto los que sirven de base para la demanda como los que sustentan las excepciones, de tal manera que deben asumir las consecuencias negativas en caso de no hacerlo.

La corte guardiana de nuestra constitución política acoge la jurisprudencia de la Corte Suprema de Justicia, en este aspecto de la contienda o controversia entre las partes en un proceso civil o de familia, al reseñar cómo en el sistema procesal se exige- en mayor o menor grado- que cada uno de los contendientes debe contribuir con el juez al esclarecimiento de la verdad, cada una de las partes se presenta ante el juez con su teoría sobre los hechos, haciendo una manifestación detallada sobre ellos y buscando el convencimiento para lograr una decisión favorable; por lo mismo, al juez no le es suficiente la sola enunciación de las partes o la presentación de un argumento convincente, por cuanto debe traer al juicio la prueba oportuna y regularmente producida y aportada al proceso.

En el estudio de los aspectos referidos, se recuerda el objeto de demanda analizado y definido por la Corte Constitucional en la sentencia citada C- 086 de 2016, respecto de la previsión sobre

la carga de la prueba: en cuanto incumbe a las partes probar el supuesto de hecho de las normas que consagra el efecto jurídico que ellas persiguen, señalando; en cada caso el juez de oficio o a petición de parte, referirá al decretar las pruebas la correspondiente carga durante su práctica o en transcurso del proceso antes de emitir fallo; carga impuesta a la parte en mejor condición para aportar la evidencia y esclarecer los hechos.

Para esta disquisición o ponderación es importante el objeto de la prueba por circunstancias técnicas especiales, que conducen a la informática resaltada en esta exposición para concluir que, en materia de la prueba pericial de expertos en ingeniería de sistemas o de derecho informático, no ingresa a los estrados judiciales, no opera la prueba pericial en los juzgados de familia de este circuito judicial, no se produce legal y técnicamente esta clase de prueba en litigios que la requiere. Porque en las controversias, como las que corresponden a ciertos procesos de familia como el divorcio, cesación de efectos civiles, custodia y cuidados personales, restablecimiento del derecho del niño, niña y adolescentes puede ser menester utilizar la prueba pericial informática en aras de proteger a la familia. Esta establecido en la normatividad constitucional y Decreto 1098 de 2006, Código de la Infancia y Adolescencia, el Código Civil, no se producen estos medios de prueba en esta clase de estrados judiciales.

La prueba pericial vendría a ser un medio de gran aporte para esclarecer hechos que muchas veces los abogados litigantes no logran esclarecerlos a la hora de tramitar un proceso, es decir vendría a convertirse en un medio para aclarar la verdad en un proceso, para que con ello los falladores operen oportunamente y fallen con resultados de justicia.

Cuando el documento tachado de falso haya sido copia, el juez podrá exigir que se presente el original. Al impugnar un medio probatorio digital, es fundamental considerar lo dispuesto en el Código General del Proceso (Ley 1564 de 2012). El artículo establece que quien alegue la falsedad de un documento debe especificar en qué consiste dicha falsedad y solicitar las pruebas necesarias para su demostración. Además, si el documento

impugnado es una copia, el juez tiene la facultad de exigir la presentación del original.

Así que, se puede corroborar que necesariamente se exige el documento original para verificar la autenticidad o demostrar la falsedad denunciada. Ante una de las situaciones en que se requieren la aportación física del documento, puede hacerse a través de una audiencia de exhibición de documentos como enuncia el artículo 266 del Código General del Proceso. Sobre trámite de la exhibición, quien la pida debe expresar los hechos que pretende demostrar y acerva que el documento se encuentra en poder de la persona requerida y la relación documental con los hechos. El juez, ordenará este descubrimiento.

Se presentan o se pueden producir elementos probatorios que converjan en los comportamientos delictivos previstos en cuanto a la vulneración de la información o de los datos o que requieran de una prueba especializada, como cuando se traen al debate evidencias digitales o documentos publicitados por las redes sociales o internet, entre otros como WhatsApp, videos, audio etc.

En estos últimos tiempos se requiere constantemente de un perito informático para que entre a dictaminar sobre la autenticidad de qué tan real son las conversaciones realizadas a través de las aplicaciones para el caso de los teléfonos móviles, WhatsApp, Lines, Telegram etc.

Es importante profundizar en la parte técnica para corroborar que no ha preexistido manejo de los mensajes, bien sean estos enviados o recibidos y que nadie los ha colocado intencionalmente en el teléfono móvil; maniobrando el mismo sería necesario la realización de un examen informático forense, bien en el teléfono emisor o bien en el receptor, es decir, en función de donde encuentren los mensajes que se requieran autenticar o si es el caso, en ambos.

Se busca con la técnica autenticar los mensajes recibidos; que del examen informático forense en el teléfono receptor se

evidencie como deducción que no existió manipulación en el mismo.

El juez debe procurar el equilibrio y el cumplimiento de las cargas procesales asumiendo las partes; que la eficacia en la composición de la litis proporcione la iniciativa de las partes para la solución justa y eficiente del debate.

Los principios y los fines plasmados en el Código General del Proceso poseen fuerza vinculante y el juez como director del debate judicial, es garante del derecho y vigilante del cumplimiento normativo en nuestro estado social y democrático del derecho.

Como epílogo, en este segmento sobre la necesidad del experto puede decirse que, he aquí la importancia de los peritajes informáticos elaborados por conocedores de la ciencia y la tecnología, para que en los juzgados de familia se apliquen en los procesos arriba indicados, con la finalidad de las garantías y derechos de las partes, de la ciudadanía en general que acude a la administración de justicia, necesaria en todo estado de derecho. La afirmación registrada en este artículo sobre la necesidad de dar capacitaciones en las TIC se ratifica y se amplía, al detectar que, en este ámbito jurisdiccional de competencia de los señores jueces de familia no campea el peritaje informático; no se presentan estas oportunidades probatorias a pesar de tenerse ante la justicia elementos de prueba que requieren de la especialidad en los temas enunciados y enseñados en la academia especializada.

Ahora bien, es de suma importancia para conocer el desarrollo del proceso colombiano y la intervención de los peritos en la actuación judicial, la normatividad vigente sobre la prueba pericial. En ella se regula no solo la procedencia de este especial medio de conocimiento, los requisitos que deben cumplir los peritos, la presentación de informes y señalamiento de la base pericial sino, además, se reglamenta la rendición del informe pericial, el momento procesal para su presentación por alguna de las partes, Fiscalía o defensa - y especialmente, su tramitación dentro de la audiencia del juicio oral o de debate probatorio.

El informe pericial corresponde a estudios o análisis hechos por expertos que ha de suscribir dicho informe. Dice la norma que las investigaciones o los análisis se realizarán por el perito o los peritos, según el caso. Ha de concluirse entonces que el perito debe ser verdadero experto en la materia, en este caso, de la tecnología de la informática, la información y los datos, en el momento en que funja como experto a favor de las pretensiones de la Fiscalía o de la defensa, demandante o demandado. El éxito o prosperidad de un asunto adelantado por la Fiscalía o controvertido por la defensa depende de los medios probatorios presentados, debatidos, incorporados y valorados por el juez en la sentencia de carácter absolutorio o condenatorio.

El perito es el vehículo para llegar ante el juez, lograr su convencimiento sobre los hechos materia de análisis sustentando la base de su opinión pericial y estar preparado para cuando sea contra interrogado por la parte contraria, siendo necesaria su capacitación y certificación.

Con el creciente nivel de complejidad en las tareas relacionadas con esta especialidad, la certificación del perito sobre la autenticidad de los medios probatorios se vuelve esencial. Esta certificación no solo valida la integridad y veracidad de los documentos digitales, sino que también proporciona un respaldo legal crucial en los procesos judiciales. La intervención de un experto asegura que todos los procedimientos empleados para la obtención y análisis de la evidencia se realicen conforme a las normativas vigentes, fortaleciendo así la confianza en los resultados presentados ante el juez. Por si sola la acreditación de ser auténtico un mensaje, no servirá para soportar una sentencia de condena por lo expuesto; más aún, cuando no se ha obtenido siquiera la certificación por un perito informático sobre la autenticidad.

Las posibilidades son muchas y lo más adecuado es siempre valorar la prueba pericial informática del envío o recepción de mensajes a través de WhatsApp u otras aplicaciones de mensajería, en relación con el resto de las pruebas.

En esta exposición se continúa con el tema de la prueba pericial, aplicable a los peritajes informáticos como sustento de nuestro llamado para la capacitación de expertos en esta materia. El aspecto doctrinal expuesto por la Suprema Corte alude al seguimiento de esta línea por parte de la sala de casación penal, al estampar la siguiente consideración: “Por supuesto, la prueba pericial ha de tener lugar en el juicio oral, donde las partes pueden intervenir en el interrogatorio cruzado, sin más limitaciones que las derivadas de la constitución y la ley”.

No puede perderse de vista por los mencionados entes y particulares, que la prueba pericial informática debe seguir el curso reglamentado por la ley procesal penal colombiana para darle el mérito correspondiente; el juez es ante todo un científico, toda vez que, su función está ligada a la valoración de si la tesis o la teoría del caso expuesta por la Fiscalía alcanza el nivel de certeza, por el ofrecimiento de elementos probatorios exhibidos y demostrados por el ente acusador, basado el juez, en la confiabilidad probatoria.

Los tratadistas de Derecho consignan su opinión sobre los temas contenidos en los códigos Penal y de Procedimiento Penal, que tiene repercusión en otras áreas como civil y familia. Para el presente estudio se extraen apuntes importantes sobre el tema, sobre el desarrollo y profundización de la prueba pericial que conduce al peritaje informático en lo referido a su presentación, descubrimiento, enunciación, solicitud probatoria, decreto de la práctica de la prueba, su producción e incorporación o introducción como prueba en la audiencia del juicio oral, y por último, la valoración del juez en la sentencia para absolver o condenar al acusado por un delito informático o por otra conducta punible donde intervenga el experto o perito en informática.

Si bien, el peritaje como prueba reclama siempre de la presencia de un experto en la audiencia de juicio oral (por regla general el mismo que realizó el informe), porque así lo demanda la ley y la naturaleza misma de lo obligado referir ante el juez y las partes, para que explique los hallazgos, exámenes, técnicas y conclusiones a las que se llega; resultando inane la sola

presentación del informe, es posible, por vía excepcional, que el perito no sea necesariamente aquel encargado de ejecutar directamente el examen y elaborar el consecuente informe, pues, en determinados eventos como lo expone Chiesa (2020). Cuando se advierte que lo consignado en el documento hace parte del tipo de información que el experto utiliza para su trabajo, nada obsta para que persona distinta acuda a la audiencia de juicio oral en aras de soportar conclusiones pertinentes para el objeto del proceso.

El testigo únicamente podrá declarar sobre aspectos que en forma directa y personal hubiese tenido la ocasión de observar o percibir; adicionalmente, el artículo 392 del Código de Procedimiento Penal prescribe que, en el desarrollo del interrogatorio de los testigos, toda pregunta versará sobre hechos. Debido a lo anterior, es inadmisible en principio, que el deponente presente apreciaciones u opiniones sobre los hechos aprehendidos; en caso de hacerlo, el funcionario judicial tiene el deber de omitirlas y abstenerse de valorarlas como fundamento probatorio del fallo[1].

Lógico es concluir de lo inmediatamente anterior, que la necesidad de los peritos informáticos se acentúa ante los litigios judiciales referidos a lo largo de esta connotación; no es un testigo técnico sino el experto acreditado quien debe coadyuvar en las investigaciones penales en el ente acusador o en la parte de la defensa, o en cada parte demandante o demandado en los litigios ante los jueces de familia.

Tema igualmente trajinado en materia de derecho informático que podría presentarse como debate en los estrados judiciales es el de la firma electrónica, sobre todo en los títulos valores que deben tener la correspondiente firma digital del facturador; exigiéndose condiciones técnicas y tecnológicas para garantizar su autenticidad, integridad y no refutación, de acuerdo con el concepto 1230 del 10 de julio del 2020, de la Dirección de Impuestos y Aduanas Nacionales.

1 En ese sentido, CSJ AP, 25 mar 2015, rad. 45.374.

3.9 Capacitación del perito

Se requiere que el perito esté en posesión de los conocimientos precisos para sustentar y explicar técnicamente los aspectos científicos, técnicos y ponderar circunstancias fácticas en el asunto materia de estudio y obtener certeza sobre lo mismo, sin que se le exija grado de licenciado o especialización alguna; es así como la jurisprudencia admitía la intervención de los peritos sin poseer títulos académicos, daban su opinión con base en su experiencia de los conocimientos que poseía técnica o científicamente, que se reflejaban en la mayor o menor credibilidad del dictamen; siendo distinto el dictamen elaborado por expertos con título oficial, con valoración de las conclusiones sustentadas en la ciencia o técnica.

Es igualmente trascendental, para efectos periciales, la cabecera del correo electrónico. Detectar alteraciones en su contenido, así como la adulteración de la cuenta del correo, los servidores involucrados, nombres, fechas, horas, tamaño del mensaje e identificadores, entre otros elementos, resulta fundamental para garantizar la integridad y autenticidad de la evidencia. Tarea útil al contrastar la información de los datos con la cabecera y las fuentes de registro, que pueden estar asociados a sus prestadores, gozando de credibilidad.

Lo más significativo, el perito debe contar con la habilidad de comunicar sus opiniones cualificadas de manera comprensible para quienes no cuentan con la formación pertinente. El perito informático realiza un análisis exhaustivo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos en búsqueda de todos aquellos elementos que puedan constituir evidencia electrónica, el resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando, extraer las conclusiones de la investigación para redactar el informe que se presentará ante los despachos judiciales.

Aunque en reciente publicación en España, octubre 8 de 2020, se apunta que no es necesario colegiarse para ejercer como perito informático; el único requisito establecido por el Tribunal

Supremo para formar parte de una lista de peritos es contar con la titulación requerida, sin necesidad de estar colegiado. Lo que significa para esta disertación, que la ilustración académica, es fundamental.

En caso que la prueba informática sea volátil, es decir, que pueda desaparecer a partir de una acción humana ejecutada en cualquier instante del tiempo (como, por ejemplo, unos comentarios o fotografías en Facebook, un mensaje en Twitter, una entrada en un blog, un comentario en un foro de internet, una noticia, etc.),la mejor opción para presentarla en un juicio es certificarla a través de un notario digital o, en caso de que la tecnología no lo permita, auxiliarse de un notario clásico, en ambos casos, siempre dirigido por las indicaciones del perito informático.

Por su parte, es importante la idoneidad cuando se presenten ataques, el asesor, aconsejara las precauciones frente a un software espía que facilite la fuga de información, impidiéndose los riesgos en las entidades o de las personas y mantener los mecanismos de seguridad informática.

El mecanismo de una grabación de audio digital puede versar sobre elementos de toda índole: conversaciones telefónicas, publicaciones en redes sociales, situaciones de la vida íntima o familiar, declaraciones sobre hechos diversos, investigaciones periodísticas o de detectives privados.

Las grabaciones de audio digital están tomando cada vez un mayor peso en todo tipo de procedimientos judiciales, correspondientes a las materias de derecho penal, civil, familia, comercial y administrativo.

Bassini (2013) categóricamente aseveró que, un perito informático debe ser un profesional del peritaje informático, no un experto en una sola área de la informática; es decir, un experto preparado, idóneo en varias disciplinas y sobre todo, eficaz perito en la materia. Igualmente, el profesional debe contar su especialidad, como sucede en todas las profesiones

es importante la especialización dado que la materia informática es extensa y cambiante.

En Colombia existen escuelas de seguridad informática que ofrecen instrucción en esta especialidad, como la de Palmira (Valle del Cauca). Lasso (2017), en su obra *Estado del peritaje informático de la evidencia digital en el marco de la administración de justicia en Colombia*, autoría de la Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnológicas e Ingeniería, especialista en seguridad informática, señaló que en nuestro país el estudio informático comenzó con reflexiones sobre la evidencia en otros países, especialmente en Estados Unidos. En 2004, apareció en el ordenamiento jurídico colombiano la denominación de expertos en informática forense, tal como lo establece el artículo 236 del Código de Procedimiento Penal, que prevé la recuperación de información dejada al navegar por Internet u otros medios tecnológicos que produzcan efectos equivalentes.

En este mismo año, apareció por primera vez la informática forense como una ciencia de apoyo para las investigaciones judiciales que realiza la Policía Nacional, pues debido al incremento de los delitos informáticos, evidenciado en los problemas de seguridad informática de las empresas y las pérdidas financieras del sector privado, surge el Gabinete de Informática Forense, conocido actualmente como la Dirección de Investigación Criminal e Interpol (DIJÍN), con el fin de brindar apoyo a las labores investigativas, desarrolladas por la Policía, dedicadas específicamente a los medios informáticos. Sin embargo, durante este año no solo se fundó la DIJIN sino la Contraloría delegada para investigaciones, juicios fiscales y jurisdicción coactiva, que decidió crear su propio laboratorio de informática forense con el propósito de investigar las acciones cometidas contra el patrimonio del Estado, convirtiéndose así en la primera entidad latinoamericana que contaba con estos instrumentos de investigación elevando su nivel para emular las tareas de CIA, el FBI, la INTERPOL.

Forensictic, como empresa colombiana especializada en los temas abordados con anterioridad, ha publicado en varias redes sociales, LinkedIn entre ellas frecuentemente, se pregunta, ¿para qué certificar un correo electrónico?, para comprobar y certificar que el correo electrónico llegó a su destinatario. Esta certificación, cuenta con validez jurídica, técnica y probatoria; ¿por qué certificar una página web?, para comprobar el contenido de una página concreta o de toda una sección de navegación, su procedencia real, presencia en la Web y que su contenido no se alteró; ¿para qué certificar una fotografía?, para firmar digitalmente quién, cuándo, cómo y dónde se capturó una fotografía; recomienda no corre riesgos y proteger su información con los expertos en seguridad.

¿Puede usar las conversaciones de WhatsApp y otros chats como prueba de juicio?, en Colombia se puede solo si se cumple con lo siguiente: Debe existir un informe emitido con un perito informático certificado que asegure la autenticidad del contenido de la conversación y, el dispositivo móvil en cuestión debe quedar a disposición total del caso y debe ser llevado al juicio como prueba, junto con el material impreso que soporte el mismo contenido de las conversaciones presentes en el teléfono celular; ¿sabes qué es un Ransomware?, es un programa de software malicioso que infecta tu computadora y muestra mensaje que exigen el pago de dinero, para restablecer el funcionamiento en el sistema; ¿sabes qué es un perito digital?, es una especialidad de perito judicial, que en su carácter de auxiliar de la justicia tiene como tarea primordial la de asesorar al juez respecto a temas relacionados con la informática; la función del perito informático consiste en el análisis de elementos informáticos, en busca de aquellos datos que puedan constituir una prueba o indicio útil para el litigio jurídico al que ha sido asignado. La protección debe abarcar a las víctimas del ciberacoso, la seguridad digital a los menores de edad.

CAPÍTULO IV

LAS TIC COMO APOYO EN LOS MECANISMOS DE INTERVENCIÓN DE LOS PERITOS INFORMÁTICOS EN LAS PRUEBAS FORENSES

CAPÍTULO IV

LAS TIC COMO APOYO EN LOS MECANISMOS DE INTERVENCIÓN DE LOS PERITOS INFORMÁTICOS EN LAS PRUEBAS FORENSES

Los procesos digitalizados exigen un cambio de mentalidad, comprometiendo los valores y principios, especialmente la honestidad y lealtad para la consecución de la verdad en la intervención del perito informático con el juzgado (juez, magistrado) para trabajar en equipo.

Por este motivo, la implementación de las TIC en los procesos judiciales sirve para agilizar los procedimientos en los juzgados; que trae grandes retos. De esta manera, los jueces y magistrados deberán fungir como orientadores del proceso digitalizado, inmediatamente, se deberán establecer estándares mínimos de seguridad para conformar el expediente digital, en un tercer orden garantizar la probidad de la información. Por consiguiente, el juez y las partes deberán asumir la responsabilidad en la verificación de los traslados virtuales de pruebas el derecho de contradicción, también se deberán orientar la recepción de memoriales y notificación de los autos para hacerle seguimiento y así, velar por el debido proceso.

A continuación, los procesos deberán agilizarse y tramitarse en tiempos casi inmediatos. Para garantizar el acceso del proceso a la administración de justicia se pueden estar llevando a cabo actuaciones dolosas, donde el juez procederá a trasladar a las autoridades competentes para que investiguen los delitos de invalidez de las pruebas.

Meneses-Obando (2019), el autor expresó la importancia de contar con un estándar en informática forense, para garantizar la recepción de la evidencia digital en el procedimiento penal o civil.

Ahora bien, en Colombia los delitos informáticos son sancionados siguiendo lo establecido en la Ley 1273 del año 2009, siendo indispensable el desarrollo y el establecimiento con mecanismos que desarrollen marcos, regulados, controlados y así analizar el caso forense.

Los avances tecnológicos en la informática forense conllevan a la reorganización de la realidad de personas, estados, entidades y empresas; origen en relaciones y hechos electrónicos, siendo el eje principal de una prueba.

Los peritos informáticos “son trascendentes en los procesos judiciales, razón por la cual se recomienda que las instituciones judiciales desarrollen un plan de acción para habilitar espacios para funcionarios especializados en la temática, incluyendo la política pública en la formación especializada” (Lasso-Vivas, 2017).

Corrales y Osorio (2015), manifestaron el crecimiento inmoderado de las TIC. Se da a la tarea, capacitar integralmente el área de sistemas de las herramientas informáticas forenses para adquirir la pericia de saber cómo investigar, cómo utilizar las herramientas; en obtener la información en cada caso para darle una solución en la trayectoria del análisis desde que inicia, a partir de apoyos como evidencias, finalizando en los resultados de los delitos informáticos; es relevante la prevención en la ejecución de auditorías en los sistemas, en los errores que se presenten, incluyendo políticas de seguridad.

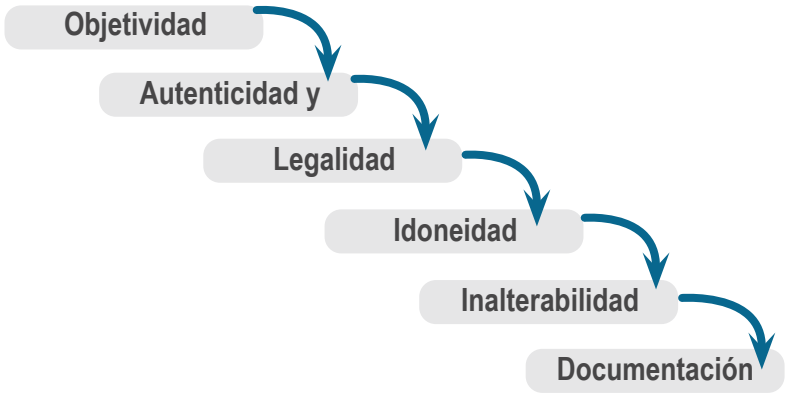
Grijalva y Loarte (2017), determinaron la eficacia de la metodología UNE 71506:2013, en la integridad en el manejo de la evidencia digital, partiendo como referencia: “ a E : es de aplicación a cualquier organización con independencia de su voluntad o tamaño, así como oratorios o entornos de análisis forense de evidencias electrónicas E”, también en la metodología contiene el uso de interfaces hápticas y entornos virtuales para garantizar la admisibilidad en los tribunales y no tener una objeción de descalificación del informe pericial.

4.1 Principios del peritaje

Se debe tener en cuenta los principios del peritaje y su cumplimiento por todos los peritos involucrados, que garanticen la autenticidad e integridad de dichas evidencias. Por lo tanto, la informática forense es recobrar registros y mensajes de datos existentes dentro de un equipo, que toda la información digital pueda ser utilizadas posteriormente ante un tribunal.

Figura 1

Principios del peritaje.



Fuente: Elaboración propia.

Ver figura 1. Principios del Peritaje. (a) La Objetividad: el perito debe observar los códigos de ética profesional. (b) Autenticidad y Conservación: durante la investigación se debe conservar la autenticidad e integridad de los medios probatorios dentro de la cadena de custodia. (c) Legalidad: el perito debe ser preciso en sus observaciones, opiniones y resultados de los hallazgos. Debe conocer la normatividad respecto a la actividad pericial y el cumplimiento de los requerimientos establecidos por la legislación. (d)Idoneidad: Los medios de prueba deben ser fidedignos, relevantes, suficientes y tener mérito probatorio para el caso. (e) Inalterabilidad: existe una cadena de custodia debidamente asegurada que demuestre que los medios no han

sido modificados. (f) Documentación: se debe establecer por escrito los hallazgos dados en el procedimiento pericial, según Acurio (2020).

Este último gran segmento del presente escrito nos lleva a concluir que, el peritaje informático es necesario para determinar la existencia de uno o varios delitos especialmente tipificados en el título VII bis del Código Penal; importante o trascendental es que los expertos que acudan a la investigación o al juicio oral para adecuar los hechos, la Fiscalía como acusadora o la defensa para desvirtuarlos o informarlos, indefectiblemente tiene que asistir a la audiencia de debate probatorio el experto en derecho informático. Ciencia y Derecho van de la mano para la administración eficaz de la justicia.

De hecho, en el circuito judicial muy pocos casos se han ventilado de estos novedosos comportamientos delictivos, pero esto no es óbice para afirmar que solo uno o dos ingenieros en sistemas con conocimiento de tecnologías computarizadas o de la informática, han pasado por los estrados judiciales como peritos. Por lo que se sostiene que, para la recta impartición de justicia penal en esta región del país, es menester cristalizar nuestra propuesta inicial que podrá llevarse a final término, con la creación de un programa de especialización o por lo menos un diplomado, para la capacitación de abogados y/o ingenieros para fungir en las audiencias como peritos.

4.2 De la necesidad del perito informático

En estos últimos tiempos se requiere constantemente de un perito informático para que ingrese a dictaminar sobre la autenticidad de conversaciones, por ejemplo, realizadas a través de las aplicaciones en teléfono móviles, de WhatsApp, entre otras. Es importante ahondar en la parte técnica para corroborar la preexistencia o no de los mensajes; ya fueren enviados o recibidos o que nadie haya maniobrado el artefacto, emisor o receptor, todo esto requiere de la autenticación.

Se debe procurar el equilibrio entre la función del juez y la carga procesal de la parte correspondiente; el equilibrio entre la

iniciativa de las partes como poder dispositivo y el poder oficioso del juez como poder inquisitivo, son facultades o prerrogativas distintas que buscan un solo fin como es la solución justa en una *litis*.

Es menester precisar que las disposiciones deben ser interpretadas conforme a los fines y principios plasmados en el Código General del Proceso, sin olvidar que tienen fuerza vinculante. El juez, como director del proceso debe estar atento en todo su trámite para cumplir con su misión como protagonista en un estado social y democrático de derecho, debiendo acudir de ser necesario, a las atribuciones oficiosas en la producción y práctica de pruebas o para razonablemente distribuir la carga probatoria según la condición en la que se encuentre las partes. Para el caso, todo en aras de validar las pruebas informáticas en pleno auge de la normatividad en la jurisdicción de familia, constitucionalmente, internacionalmente, Código de la Infancia y Adolescencia y Código General del Proceso.

Al contrario, con el uso incorrecto de las TIC o de las plataformas virtuales se pueden generar debilidades, las cuales se pueden detectar como inexperiencias de los operadores judiciales en la administración de justicia; a su vez, las dudas e inquietudes con relación al rol del juez y de las partes. El incorrecto manejo del expediente digitalizado promueve reticencia de las partes a cumplir las nuevas cargas, tales como allegar digitalizadas las piezas procesales que tengan los intervinientes en su poder o la de escanear expedientes.

Por otro lado, se menciona el principio de neutralidad en los procesos jurídicos, los cuales son aquellas personas que no tienen la facilidad o no cuentan con las TIC, podrán hacerlo de manera presencial, manifestando las razones por las cuales no tienen los medios informáticos. Es relevante, mencionar otra herramienta de las TIC, una de ellas, es la firma electrónica en la cuál es importante para la seguridad digital en los procesos jurídicos; por tal motivo la Sala Administrativa del Consejo Superior de la Judicatura implementó un aplicativo de firma electrónica de documentos para los jueces, basado en

credenciales, usuario y contraseña, cuenta además con un link para verificar la veracidad de la firma a través de los módulos de validación.

No obstante, los apoderados de los casos deberán colaborar en la digitalización de los expedientes, en la preparación de sus testigos y peritos para que puedan comparecer a través del aplicativo TEAMS, a la audiencia de pruebas; teniendo en cuenta que en los juzgados se hace necesario el perito informático como apoyo al juez y al magistrado. Por tal razón, la controversia suscitada en los estrados judiciales con la presencia activa de un perito o experto en derecho informático viene a revelarse en los últimos años mediante las investigaciones por la violación de los datos personales cuando se sube a las redes sociales fotografías y videos que quebrantan el derecho a la intimidad. Por cuanto, la técnica corresponde a los protocolos de la Fiscalía y la ciencia informática.

Como sustento importante para hacer ver la significación del perito informático en los procesos judiciales, debe mencionarse la decisión del Tribunal Superior de Medellín, con ponencia del magistrado John Jairo Gómez Jiménez del 4 de agosto de 2021, dictada dentro del radicado acusatorio ordinario 2014-40631, donde se confirma la sentencia absolutoria de primera instancia, por no haber probado la Fiscalía su teoría del caso, máxime cuando dejó de presentar prueba pericial, sabiéndose que la conducta trataba de acceso abusivo a un sistema informático, previsto en el artículo 269A del Código Penal colombiano.

El caso refiere a fraude millonario en perjuicio de connotado banco de la ciudad de Medellín, donde se utilizó firma que presta apoyo a la corporación bancaria, a sus usuarios, en lo atinente al desbloqueo y cambios de claves, pudiendo acceder a la red del banco. El resultado conllevó al cambio de nombre del usuario y clave de funcionario de la empresa de apoyo del banco; sin embargo, el usuario podía acceder a la plataforma y estaba autorizado para cambios de contraseña, por tres medios: chat interno, correo electrónico o llamada telefónica y además se requería que fuera directamente por la persona a quien se

le asignó el usuario y con el aval del jefe inmediato. Ocurre que el titular de la cuenta nunca solicitó el cambio de contraseña y tampoco tuvo origen en los otros medios autorizados por la mesa de trabajo. Afirmándose entonces, que el responsable del cambio de la contraseña fue el usuario que tenía conocimiento de un caso anterior en esta entidad.

El juez de la causa absolvió al acusado, señala la sentencia del Tribunal Superior de Medellín, por considerar que no se logró demostrar la modificación de la contraseña de acceso a la plataforma principal del banco, ya que no se trajo al juicio un disco duro, copia forense, una copia espejo, un peritaje y otra prueba técnica o pericial, que permitiera apreciar con antelación que efectivamente existió el cambio de contraseña que tenía el usuario. Inclusive este disco fue extraviado o desaparecido y, de contera, la Fiscalía desistió del perito que daría cuenta sobre la copia forense o espejo, supuestamente tomada del disco duro para establecer la mismidad y lo derivado de allí, como la dirección IP, la contraseña inicial y final, si realmente existió el acceso y si el usuario había sido bloqueado o deshabilitado, en el primer caso el usuario tendría facultades para reanudar su funcionamiento, en el segundo evento solo podría darle vigencia el banco.

En la decisión judicial se señala de manera puntual que, pese a que no hay tarifa legal de pruebas para este asunto, en este caso se requería una prueba técnica o informática; las pruebas testimoniales son inocuas ya que no provienen de técnicos en la materia.

Elemental es concluir, que esta doctrina es reflejo claro de la necesidad de los peritos informáticos en los debates probatorios que correspondan a temas relacionados con la informática.

Corrales y Osorio (2015), manifestaron que debido al crecimiento desmesurado de las tecnologías, se hace necesario capacitar a los ingenieros de sistemas en el manejo de las herramientas informáticas forenses, dando la pericia de saber cómo investigar, cómo utilizar las herramientas, cómo obtener la información

necesaria para con ello resolver cada caso que debe ser sometido a procesos preventivos mediante la ejecución de auditorías en los sistemas, corrección de errores y desde esta perspectiva plantear políticas de seguridad.

Guijarro et al., (2016), traen la temática de la informática forense en el punto de vista de seguridad; la seguridad informática, en el hardware y software y en el factor humano, capacitarlo de manera adecuada, prevenirlo y brindarle las herramientas necesarias para que pueda implementar protección a nivel de aplicaciones, concientizándolo de los riesgos potenciales que suponen los ataques informáticos y las metodologías aplicadas para mitigar el mismo, convirtiendo al factor humano en un representante más de la seguridad informática. A continuación, la normatividad en Colombia sobre aspectos informáticos.

4.3 Normatividad en Colombia sobre aspectos informáticos

Tabla 2
Normatividad.

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Ley de derechos de autor, ley 23 de 1982.	Derecho de autor y derecho conexo en Colombia.	Protege a las obras literarias, científicas y artísticas, productores de fonogramas organismo de radiodifusión, libro, folletos, conferencias, obras dramáticas, composiciones musicales, videos, pintura, escultura, grabados.
Ley de Comercio electrónico. Ley 527 de 1999.	Reglamenta el uso de mensajes de datos, del comercio electrónico y de las firmas digitales y se establece las entidades de certificación.	*Integridad de información como mensaje de datos.*

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Ley modificatoria de comunicaciones, derechos de autor y propiedad industrial. Ley 1032 de 2006.	Artículo 306 del C.P usurpación de derecho propiedad industrial.	Nombre comercial, enseña, marca, patente de invención, modelo de utilidad, diseño de industrial, derechos de obtentor de variedad vegetal.
Ley de delitos informáticos. Ley 1273 de 2009.	Protección de la información y de los datos.	Protección total de los sistemas de acceso abusivo a un sistema informático. Ingreso al correo electrónico, Facebook, WhatsApp, conectarse a una red inalámbrica, sin autorización de instalación de un Keylogger. Instalación de software sniffer un software espía Suplantación de sitios web para capturar datos personales.
Ley de Teletrabajo.	Promueve y regula el teletrabajo.	Generación de empleo, autoempleo. Trabajo utilizando los soportes técnicos de labor remunerada.
Ley de habeas data. Ley 1266 de 2008.	Derecho de las personas a conocer, actualizar y rectificar las informaciones en los bancos de datos.	Seguridad, bancos de datos, cámara de comercio.
Ley de protección de datos personales. Ley 1581 de 2012.	Datos sensibles, afectan la intimidad del titular el propietario de los datos.	Titular. Orígenes étnicos, racial, orientación política clero, filosofías sindicatos, organizaciones sociales, derechos humanos.
Reglamentación ley de protección de datos personales. Decreto 1377 de 2013.	Autorización por parte de los responsables del tratamiento de datos personales, que permita obtener la autorización de los titulares.	Autorización del titular cumpliendo los requisitos cuando se manifieste por: escrito de forma oral, mediante conductas inequívocas del titular, que permita de forma razonable dar a entender que otorga la autorización.

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Ley de regulación del sector de las TIC. Ley 1341 de 2009.	Regirán el sector de las tecnologías de la información y las comunicaciones.	Ordenamiento general, régimen de competencia, protección del usuario, cobertura, calidad del servicio, promoción de la inversión en el sector y el desarrollo de estas tecnologías, su eficiencia en las redes y del espectro radioeléctrico, formación de personal.
Decreto regulatorio de la firma electrónica. Decreto 2364 de 2012.	La firma electrónica es un medio de identificación electrónica flexible y tecnológicamente neutro que se adecua a la necesidad de la sociedad y que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación.	Reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos, facilitar y promover el uso masivo de la firma electrónica en todo tipo de transacciones.
Ley contra *cyberbullying*. Ley 1620 de 2013.	Creándose el sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos.	Coordina la creación de mecanismos de denuncia y seguimiento en Internet, redes sociales y demás tecnologías de información. Responsabilidad de la secretaria de educación y formación en los derechos humanos.
Ley de transparencia y el derecho de acceso a la información pública nacional. Ley 1712 de 2014.	Regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la Publicidad de información.	Las personas deben adoptar un programa de gestión documental en el cual establezca los procedimientos y lineamientos necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos integrándose con las funciones administrativas del sujeto obligado.

CÓDIGO PENAL	NOMBRE DE LA LEY	CONCEPTO
Lineamientos generales de las estrategias de gobierno en línea. Decreto 2573 de 2014.	Define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones para contribuir con la construcción de un estado abierto, eficiente, transparente, participativo para prestar el servicio a la sociedad.	TIC para servicios, gobierno abierto, gestión, seguridad y privacidad de la información.
Decreto estructural de la factura electrónica. Decreto 2242 de 2015.	Utilizar formato electrónico de generación XML estándar establecido por la DIAN, llevar numeración consecutiva autorizada por la DIAN condiciones que esta señale artículo 617, incluir la firma digital o electrónica para el Control fiscal.	Artículo 12: Autorizar de proveedores tecnológicos, sin perjuicio de la expedición de la factura electrónica directamente por el obligado a facturar electrónicamente, este podrá para tal efecto contratar los servicios de los proveedores tecnológicos autorizados por la DIAN. XML: Extensible Makup Language, es el formato para WEB que permite manejar datos para luego ser usados por otros programas.

Fuente: Castaño, 2018.

CAPÍTULO V
HALLAZGOS DE LA INVESTIGACIÓN

CAPÍTULO V
HALLAZGOS DE LA INVESTIGACIÓN

5.1 Metodología de la investigación

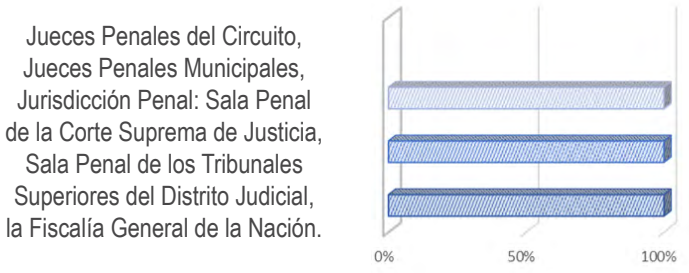
El estudio se desarrolló desde el enfoque cuantitativo, Hernández, Fernández y Baptista (2018). Usando, un diseño explicativo y muestreo intencional, con muestra no probabilística depende de las características de la investigación (Hernández et al., 2014).

5.2 Resultados del análisis cuantitativo de la encuesta

5.2.1 ¿Qué entidades investigadoras, fiscales, tienen experiencia en delitos informáticos (actividades delictivas contra las computadoras o la información computarizada, o el uso de computadoras como medio para cometer un delito)?

Figura 2

¿Qué entidades investigadoras, fiscales, tienen experiencia en delitos informáticos?



Fuente: Elaboración propia.

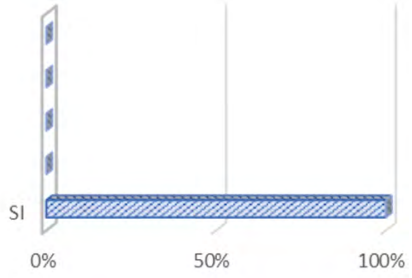
Un 100% respondió: en la jurisdicción penal, se tiene experiencia en la Sala de Casación Penal de la Corte Suprema de Justicia, sala penal de los tribunales superiores del distrito

judicial, los jueces penales del circuito, jueces penales municipales y la Fiscalía.

5.2.2 ¿Se ha cometido alguna vez o es común que se cometan en el país delitos informáticos?

Figura 3

Delitos informáticos cometidos.



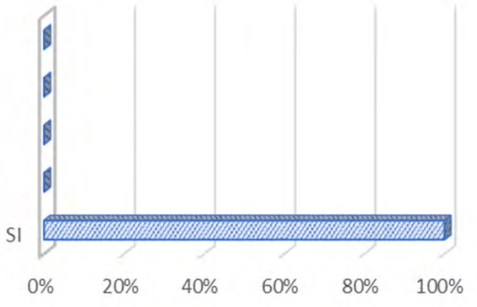
Fuente: Elaboración propia.

Un 100% da respuesta: sí; se han cometido los delitos informáticos en el país.

5.2.3 ¿Sanciona la legislación penal la destrucción, modificación, alteración, acceso, uso o interferencia similar de un sistema o programa de computadora?

Figura 4

Sanciones en la legislación penal.



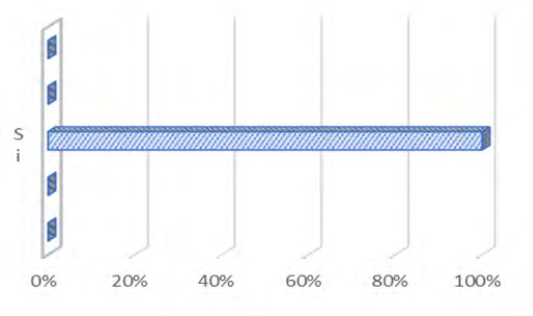
Fuente: Elaboración propia.

Un 100% respondieron que: sí; la ley penal sanciona.

5.2.4 ¿Se llevan estadísticas del número de los delitos informáticos a) denunciados por las víctimas, b) denunciados por la Policía Inc.) de los procesados por la justicia?

Figura 5

Estadística de delitos informáticos.



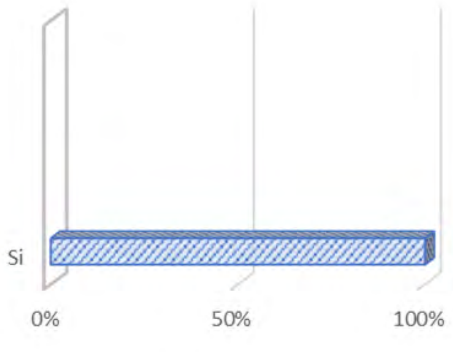
Fuente: Elaboración propia.

Un 100 % responde: sí; llevan la estadística en la temática de los delitos informáticos.

5.2.5¿Ofrecen las instituciones estatales programas de capacitación en delincuencia cibernética a: a) la Policía; b) las procuradurías) Fiscalía; d) la rama judicial?

Figura 6

Ofrece la institución capacitación de delincuencia cibernética.



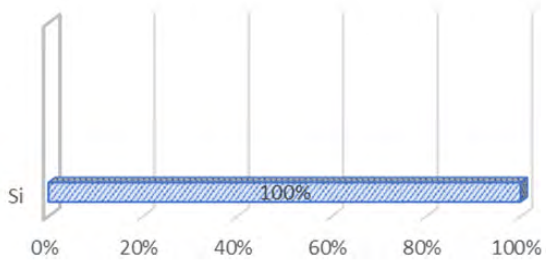
Fuente: Elaboración propia.

Un 100 % responde: sí, ofrecen las instituciones estatales programas de capacitación en delincuencia cibernética.

5.2.6 ¿Existen mecanismos de cooperación técnica en materia de delitos informáticos?

Figura 7

Mecanismos de cooperación técnica en materia de delitos informáticos.



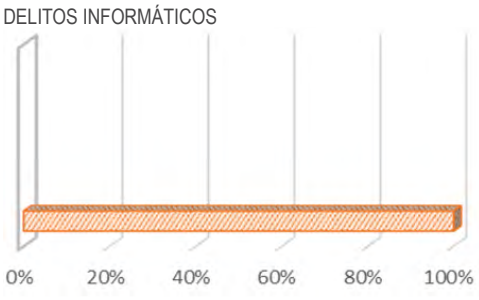
Fuente: Elaboración propia.

Un 100% respondieron que sí hay cooperación de los Estados Unidos.

5.2.7¿De qué forma ha evolucionado la jurisprudencia en el derecho penal en lo concerniente a la prueba pericial forense frente a los delitos informáticos en los diferentes procesos?

Figura 8

Evolución de la jurisprudencia en el derecho penal.



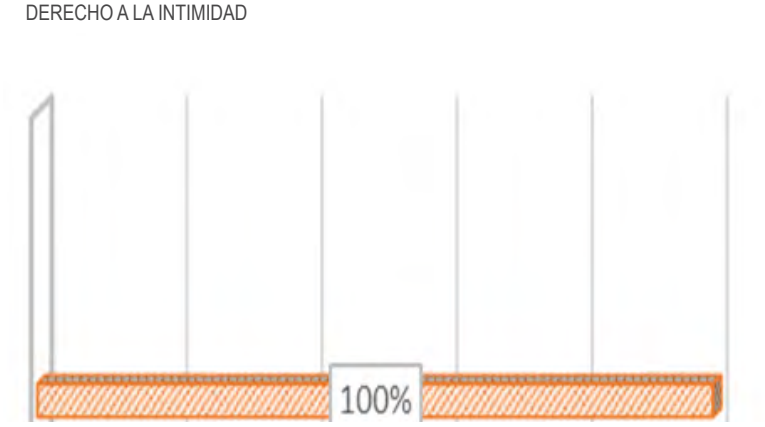
Fuente: Elaboración propia.

Un 100 % responden: la jurisprudencia analiza y precisa la adecuación típica de los delitos informáticos, lo cual ha determinado que el peritaje informático sea una herramienta indispensable, aludiendo a las leyes 1437 de 2011 y 1273 de 2009, que modifican el Código Penal.

5.2.8¿Qué garantías existen con la aplicación de la Ley 527 de 1999, por la cual se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, respecto de la prueba pericial en los delitos informáticos?

Figura 9

Garantías con la aplicación de la Ley 527 del 1999.



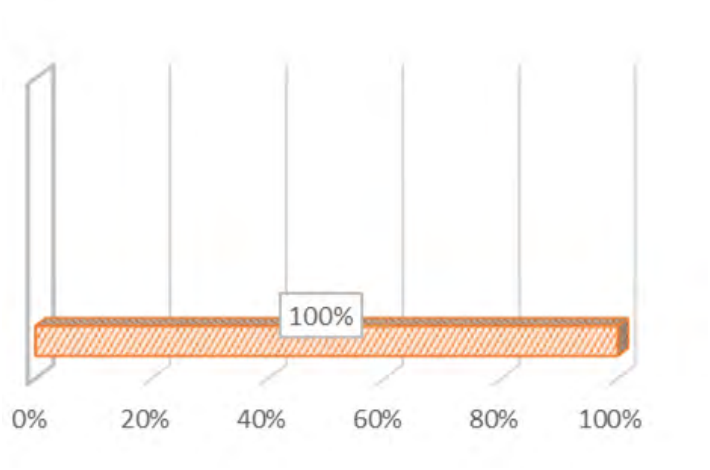
Fuente: Elaboración propia.

Un 100% responden: la garantía como derecho a la intimidad. La prueba pericial debe ser reglamentada, su producción e incorporación.

5.2.9 Si la información que se encuentra en los mensajes de datos tiene efectos jurídicos, validez o fuerza obligatoria, según el artículo 6 de la ley 527 de 1999, ¿por qué su contenido no es válido como prueba en algunos procesos de penales?

Figura 10

Los mensajes de datos tienen efectos jurídicos.

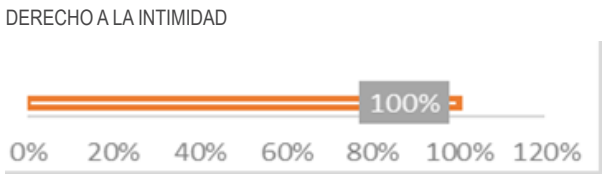


Fuente: Elaboración propia.

Un 100% dicen: la invalidez de la prueba proviene de su ilicitud o ilegalidad por vulnerar los derechos humanos y por no ser solicitada, decretada, producida e incorporada conforme al procedimiento penal; producirá efectos jurídicos de invalidez de la información contenida en el mensaje. La Corte Constitucional mediante sentencia C-831/2001 con ponencia del doctor Álvaro Tafur Galvis, declaró la asequibilidad de la norma mencionada, su contenido, no afecta el derecho a la libertad personal o la inviolabilidad del domicilio; la supuesta violación del artículo 28 y 152 de la Constitución Nacional, no aplica para la reserva de la ley estatutaria aludida por el demandante.

5.2.10¿En los despachos judiciales, se utilizan los mensajes de datos para dar o recibir cualquier información o dejar constancia en los procesos que se adelantan?

Figura 11
Evidencias.

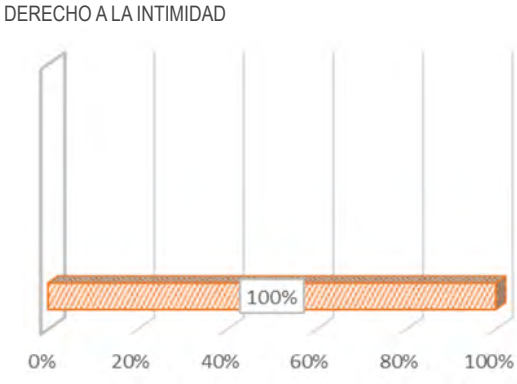


Fuente: Elaboración propia.

Un 100% mencionaron: que existen evidencias de los mensajes de datos recibidos y enviados por los despachos judiciales.

5.2.11 ¿Qué métodos se utilizan en su despacho judicial para la validación de las firmas digitales como prueba en las actuaciones penales que adelantan?

Figura 12
Validación de firmas



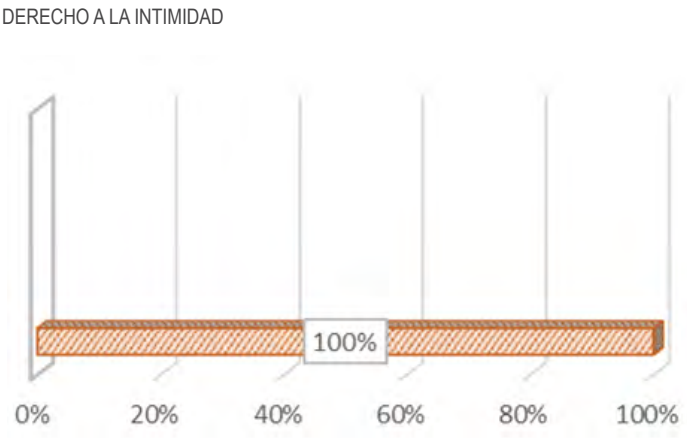
Fuente: Elaboración propia.

Un 100% respondieron: los jueces avalan y certifican firmas digitales, siempre que se garantice su legibilidad, inalterabilidad y perdurabilidad.

5.2.12 ¿En los despachos judiciales que procedimiento se utiliza para la incorporación de la prueba pericial frente a los delitos informáticos?

Figura 13

Incorporación de la prueba pericial.



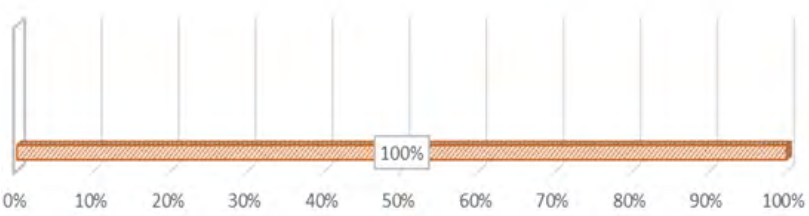
Fuente: Elaboración propia.

Un 100% dijeron: En el sistema penal acusatorio existen precisiones concretas sobre la solicitud y decreto de la prueba en la audiencia preparatoria, que será presentada, debatida y controvertida en la audiencia del juicio oral para proceder a su incorporación.

5.2.13 ¿Qué diferencia existe entre los procesos donde se aplica la prueba pericial forense y en los que no se presenta, debate e incorporan?

Figura 14

Procesos donde se aplica la prueba pericial forense.



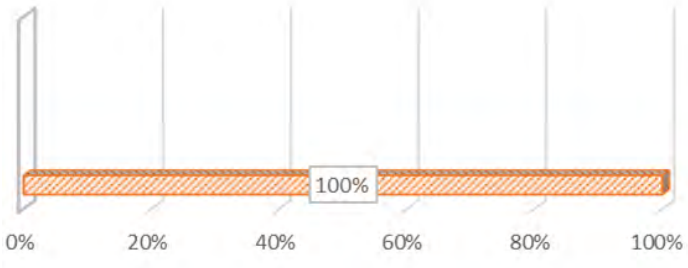
Fuente: Elaboración propia.

Un 100 % mencionó: que la diferencia no se establece al no existir la tarifa legal probatoria; se determina por la eficacia de la prueba pericial para lograr la convicción del juez y obtener la decisión que se pretende.

5.2.14 ¿Qué eficacia tiene el peritaje forense en la actuación judicial por delitos informáticos?

Figura 15

Peritaje forense en la actuación judicial.



Fuente: Elaboración propia.

Un 100 % de los colaboradores indicaron: el perito forense elabora el dictamen para dar luces o aclaración a los hechos debatidos para que el juez emita ajustada a derecho.

La investigación se apoyó en antecedentes internacionales, nacionales y regionales, por consiguiente, se presentan a continuación.

Acosta et al. (2020) destacaron que los delitos informáticos y el uso inadecuado de la tecnología afectan la privacidad de los cibernautas, al acceder a los sistemas operativos y extraer datos de servidores privados o empresariales. En su estudio, concluyeron que estas acciones representan delitos antijurídicos cometidos a través de medios cibernéticos, con el propósito de destruir, desprestigiar o extorsionar al cibernauta mediante herramientas digitales en Internet.

“Aspectos legales al utilizar las principales redes sociales en Colombia”. Se analizaron los aspectos legales al utilizar las redes sociales como el Facebook y Twitter encendrándose resultados del uso y conexión responsable de los usuarios y la trasgresión de la normatividad colombiana sobre el mundo virtual, en la protección de la información y los datos, injuria, calumnia y ciberacoso. Notándose el incorrecto uso de las TIC que conllevan a un delito cibernético en el ámbito judicial (Alvarado, 2017)

“Realidad sobre la privacidad de los datos personales en Costa Rica”, relacionada con la información personal como son el nombre, identificación, domicilio, fotografías, videos, correos electrónicos entre otros, que al ingresar de manera ilícita trae consecuencias penales, civiles, sanciones administrativas y disciplinarias. Toda persona debe conocer la legislación que existe para su protección y ampararse en la Ley 8968 sobre protección de la persona frente al tratamiento de sus datos personales de orden público y garantiza el respeto hacia sus derechos ya sea como persona natural o jurídica (Rivera, 2019).

Rodríguez et al. (2017) investigaron el ciberdelito a nivel mundial, enfocándose en la detección de perjuicios por hackeo y acoso online. Los resultados varían en la victimización cibernética, tanto en el campo experimental como en el técnico o teórico.

Estrada et al. (2020). “Práctica de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolivar (Tuluá, Colombia)”. El uso de los tipos de tecnología es cada vez más frecuente; se tomó la decisión de analizar su enfoque desde el punto de vista de la seguridad informática conformado por cinco variables sobre fortalezas y debilidades; vislumbrándose la necesidad de implementar programas de capacitación continúas sobre estas prácticas.

Sánchez et al. (2017). “La significativa evolución en seguridad de la información para la Policía Nacional de Colombia”. Los autores establecieron una contextualización cronológica sobre los procesos y alcances relacionados con la seguridad de la información; se contextualiza los estándares instaurados por la institución y sus efectos en la comunidad, se señalan acciones normativas y comportamentales para la formación de los policiales y el control de dicha información.

Blanco (2020) abordó la comprensión significativa de las TIC, su relevancia en las organizaciones, su ámbito legislativo y las debilidades presentadas, con miras a establecer el desarrollo en la nación en áreas como salud, educación, medio ambiente, seguridad del agro y la alimentación.

Lanzillotti y Korman (2020). “¿Qué informa la prensa Argentina acerca del fenómeno de ciberbullying?”, los medios de comunicación mencionan los términos técnicos de bullying y ciberbullying, sus características consecuencias y tratamiento de estas conductas que permitirán observar la socialización de la información el tema u orientación empleado y el sentido de mensaje a la colectividad.

Jiménez y Meneses (2017). El internet: su naturaleza más allá de las fronteras, ámbito geográfico, de amplia cobertura, de fácil reproducción y colectividad son el horizonte de un nuevo derecho; internet y derecho como temas para análisis cualitativo mediante el uso de fuentes y técnicas que se desarrollen en la academia y en la administración de justicia como tecnología virtual.

Martínez (2019). “El uso de efectivo y tarjetas débito como instrumentos de pago en Colombia”, equivalentes a las transacciones de dinero en efectivo, créditos y depósitos, como la compra de bienes, requiriéndose de la tecnología que faciliten el ingreso a los servicios financieros, en corporaciones bancarias, cajeros automáticos, comunicaciones por internet y datafonos.

Camaño y Gil (2020). “Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional”, donde se identificaron los riesgos de seguridad mediante ataques cibernéticos; se pauta estrategia para descubrir a los responsables evaluar métodos de apoyo y control, siendo importante el análisis de las capacidades humanas, la gestión del conocimiento y los correspondientes perfiles para la autoría forense.

Meléndrez (2018). “Logística del Comercio electrónico; cross docking, merge in transit, shipping ylick andcollect”. Su importancia para controlar el tránsito de información desde el punto original hasta el destino, especialmente en internet. Los intercambiadores logísticos son necesarios para controlar la recepción y solicitud de elementos materiales, su gestión y archivo, su uso trascendencia y aplicación en las empresas.

Luz (2018) analizó la mediación en entornos electrónicos dentro de las relaciones multiculturales, donde se propician conflictos y se aplican mecanismos alternativos de solución. En un ambiente cambiante, donde los procedimientos judiciales no siempre son suficientes para una solución rápida, se recurre a la mediación, conciliación y transacción para evitar demoras, ineficiencias, altos costos y el desánimo de quienes acuden a la justicia.

Patiño (2019). “El sistema internacional cibernético: elementos de análisis”, en cuanto al debate de aspectos cibernéticos y su relación con las nuevas técnicas de seguridad internacional, debiéndose adoptar métodos de disciplina internacional para estudiar estos asuntos globalmente.

Ovalle et al. (2019) mencionan que la delincuencia informática y su evolución en Colombia son temas relevantes. Los delitos informáticos descritos en la Ley 1273 de 5 de enero de 2009, que regula la protección de la información y los datos, están alineados con lo establecido en el artículo 15 de la Constitución Política, el cual enfatiza que las personas tienen derecho a su intimidad personal, social, económica y educativa, asegurando la protección de sus datos personales y su respeto frente a los delincuentes informáticos.

Mayer (2019). La información y los datos para preservar integralmente los sistemas utilizados con las TIC, reconociéndose la incidencia en el sustento lógico de estos sistemas y el uso de las redes de computación; sabiéndose de la afectación del derecho al libre desarrollo de la personalidad y de las instituciones de un estado democrático de derecho.

Rico (2013). “Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos”. Las TIC y el sistema de internet dieron paso a comportamientos delictivos como el de la utilización ilícita de medios electrónicos de pago, debiéndose revisar cada conducta para no incurrir en la impunidad, buscándose solución para la prevención, investigación y sanción de todos los delitos o fraudes informáticos en España.

Rojas (2016). “Análisis de la penalización del cibercrimen en países de habla hispana”. Ante el incremento de la criminalidad informática internacional para precisar la legislación en cuanto a la tipicidad de las conductas en los países hispanos, al carecer del estudio sobre las categorías y localización de estos delitos, sin que aparezca la capacidad preventiva e investigativa en los países que sufren estas situaciones.

Bolaños y Gómez (2015). “Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador”. De los pasos utilizados por los expertos de la policía nacional frente a la ejecución de casos informáticos con evidencia digital como son el disco duro, los correos electrónicos, las redes sociales

y la base de datos, faltando la regulación de otros elementos materiales como son los documentos de ofimática, imágenes digitales, ficheros de registro y la memoria volátil.

Vuanello (2012). “La interpretación de docentes sobre la seguridad de los jóvenes en el uso de las TICs”. Perspectivas en Psicología: En la sociedad cambiante con el apoyo digital, se ha reconocido el beneficio y el perjuicio que las TIC aporta en el mundo social. Entre el beneficio se tiene la agilidad y rapidez en que se llegan las comunicaciones para interactuar los pares, la escuela, universidades, la familia y la economía. Otros casos como el perjuicio al buen nombre de una persona y a una empresa, quienes son víctimas de estafas, hurto y ciberbullying; sobre todo se presentan amenazas a la población joven que afecta su seguridad psicológica y social. Por tal motivo, la digitalización educativa de la provincia buscó reducir el acceso a los medios informáticos a través de la provisión de conectividad inalámbrica gratuita y el equipamiento de computadoras a los estudiantes, ese fácil acceso conlleva a la poca orientación en los educandos para evitar los peligros en las redes sociales.

CONCLUSIONES

En Colombia los delitos informáticos son sancionados con lo establecido en la Ley 1273 del año 2009, por lo tanto, se hace indispensable establecer y desarrollar mecanismos para el análisis forense, permitiendo que se desplieguen dentro de los marcos procedimentales las pautas que se deben seguir para la aplicación de la cadena de custodia en las pruebas periciales. Es relevante tener el apoyo de las herramientas que garanticen los procesos judiciales y a su vez, se recomienda establecer una bitácora funcional a nivel de cada caso.

Como consecuencia del aislamiento social del COVID-19, la administración jurídica entra con modalidad hibrida en la utilización de las herramientas virtuales con plataformas permitidas por la Ley 2213 del año 2020; entre ellas se tienen las siguientes:

TYBA, SAMAI, Tutela en línea, Consulta de procesos nacionales unificados, Life size, correos electrónicos, desde la creación de estas en el apoyo de los procesos, civiles, administrativos, penales para agilizar y visualizar el expediente digitalizado del proceso. El desarrollo en la administración de justicia fue avanzando y organizando los expedientes de los usuarios, litigantes, jueces y magistrados para el beneficio del colombiano y de la justicia; ya que, antes de la pandemia se utilizaba el correo electrónico institucional basado en Exchange Online de Office 365 con recepción y envío de mensajes a través de correo electrónico, programar reuniones, OneDrive, Forms y SharePoint, entre otros.

Los avances tecnológicos, las tendencias en las herramientas de informática forense en los litigios, son de gran apoyo, así mismo en la reorganización de las pruebas periciales, en el entorno de personas, estados, entidades y empresas. Para ello, el uso de estas herramientas licenciadas garantiza los procesos, siendo vital dentro de los trámites judiciales, razón

por la cual se recomienda una acción que brinde capacitación a los funcionarios especializados para atender un procedimiento penal, civil – familia, con el fin de certificar la calidad en los resultados.

Se resaltó la acción del perito informático sobre todo en la época de la pandemia del 2020; quien desempeña un papel en la administración de justicia, por lo tanto, su perfil debe estar ligado más allá de la experticia, profesionalismo y técnicas aplicadas a su desarrollo laboral, propendiendo a darle reconocimiento a su actuación frente a la ley.

Como consecuencia del COVID 19, los juzgados se dieron a la ocupación de llevar a cabo los procesos a través del mundo virtual. Por consiguiente, la Corte Constitucional en sentencia C-662/2.000 y las normas de la Ley 527 de 1999, señaló que con la entrada de esta ley en Colombia se establece la tendencia al derecho privado, con los documentos electrónicos están en capacidad de brindar similares niveles de seguridad, dando un mayor grado de confiabilidad, agilidad o rapidez en los procesos judiciales.

De tal manera, se resaltó la Ley 1437 de 2011 (CPACA), la cual dio el paso al rompimiento de los paradigmas con la aplicación de los medios electrónicos en el funcionamiento como recurso estatal, siendo esto una revolución tecnológica de la mano de la eficacia y eficiencia en Colombia a través de un marco normativo, el cual permite realizar los procedimientos y trámites administrativos con los medios electrónicos para facilitarle al ciudadano recibir y enviar notificaciones o expedientes electrónicos que corresponden a un procedimiento virtual administrativo al que tiene derecho las personas (art. 54 y 59 CPACA).

La UNESCO ha declarado que el uso de la Inteligencia Artificial está siendo estudiado por poderes judiciales y fiscalías alrededor del mundo. En el campo de la justicia criminal, el uso de esta tecnología para apoyar servicios de investigación y toma de decisiones, ya es una realidad en varios países.

Es de mayor significancia que se empiezan a crear las nuevas plataformas para ser utilizadas en los juzgado en el tiempo del COVID-19; siendo motivo del aislamiento social y a su vez, se toma la decisión en desarrollar plataformas poniendo en práctica las herramientas digitales, los medios desarrollados por el legislador, que han demostrado su beneficio para el funcionamiento de la administración de justicia en función de recopilar los expedientes y pruebas de la investigación en el mundo digital como: Life size, TYBA, SAMAI y Consulta nacional unificada de los procesos, correos electrónicos, que fortalecen y agilizan los avances en audiencias a través de las notificaciones electrónicas, decisiones judiciales, medios expeditos y a su vez, ayudan a visualizar el caso en la publicación del proceso por la virtualidad para los interesados en la resolución del conflicto, en respuesta del caso expuesto.

Es indispensable, realizar capacitaciones a los colaboradores de la justicia para el manejo de las plataformas, con el objetivo de acelerar en forma eficaz las decisiones de la administración de justicia, y a su vez, se informa o se orienta al personal litigante en hacer uso correcto de las herramientas virtuales. Se recomienda que el Consejo Superior de la Judicatura destine rubros para las capacitaciones en su correcto manejo de los aplicativos que se encuentran en forma digital.

Por último, es importante destacar que las adaptaciones que se puedan realizar a la aplicación y el papel que juega la administración de justicia es clave en la permanencia de un estado social de derecho, siendo un factor determinante para la constitución de derechos y garantías de los ciudadanos.

El papel que tiene actualmente la Ley 2213 del año 2022 es fundamental y de relevancia, ya que se mira el impacto de la historia en el antes y después de la pandemia del COVID-19; por este motivo, se facilita el paso a la virtualidad para buscar la eficiencia, la eficacia en los procesos judiciales con funciones de agilizar los trámites, actuaciones y así mismo, el ciudadano accede a la plataforma de la jurisprudencia.

Sin embargo, si la tecnología se desarrolla con seguimiento en base a las normas éticas y estándares universales y utiliza valores basados en los derechos humanos, puede ayudar a resolver problemas complejos como el reconocimiento de patrones de conducta y la detección de decisiones parciales.

Así que tomando en cuenta el desarrollo acelerado de tecnologías como el aprendizaje automático y profundo, como el reconocimiento de voz e imágenes, la utilización de la inteligencia artificial para automatizar las decisiones y veredictos en la corte.

REFERENCIAS BIBLIOGRÁFICAS

Abel, X. (2019). La impugnación de la prueba tecnológica. En Agudelo, D, Pabón, L, Toro, L, Bustamante, M & Vargas, O. La prueba: teoría y práctica (pp. 559 – 595). Medellín: Universidad de Medellín.

Acosta, M., Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89), 351-368.

Acurio, S. (2020). *Manual de Manejo de Evidencias Digitales y Entornos Informáticos*. https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Acurio, S. (s,f). *Delitos Informáticos: Generalidades*. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Adalid. (2021). *Security, Legal & Forensic Corporation*. https://www.adalid.com/nosotros/

Alexy, R. (2017). Teoría de los derechos fundamentales. Madrid: Centro de Estudios Políticos y Constitucionales.

Alhippio, I. (2001). *Elementos de Derecho Civil*. Ediciones Doctrina y Ley Ltda.

Alvarado, M. (2017). Aspectos legales al utilizar las principales redes sociales en Colombia. *Revista Logos, Ciencia & Tecnología*, 8(2), 211-220. https://www.redalyc.org/articulo.oa?id=5177/517752177019

Akhgar, B., & Brewster, B. (Eds.). (2016). Combatting cybercrime and cyberterrorism. Challenges, trends and priorities. Springer International Publishing Switzerland. https://doi.org/10.1007/978-3-319-38930-1

Baila M. (2015). *Procedimientos Periciales*. https://docplayer.es/57959048 Procedimientos-periciales.html

Balmaceda, G. (2009). *El delito de Estafa Informática*. Edicciones Jurídicas.

Bañol, J. M. (2014). “Reconocimiento de las principales audiencias preliminares en el marco de la Ley 906 de 2004.

Baptista, M., Fernández, C. y Hernández, R. (2010). *Metodología de la Investigación*. http://www.esup.edu.pe/descargas/dep_investi-

gacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf

Bassin, Andrés Eduardo. (2013). "*El perito informático y la prueba pericial*". https://derechopenalonline.com/el-perito-informatico-y-la-prueba-pericial/

Barreto Ardila, Hernando. Universidad Externado de Colombia. Magistrado auxiliar de la Sala de Casación Penal de la Corte Suprema de Justicia. https://revistas.uexternado.edu.co/index.php/derpen/article/view/1093/1036

Barrios Hernández,Tahí . (1985) Revista L 'Ane, le magazine Freudien núm. 22.

Bernal, A. (2013). *Las reformas procesales penales en Colombia*. Universidad Santo Tomás.

Bernal, J. y Montealegre, E. (2013). *El Proceso Penal.* Universidad Externado de Colombia.

Blanco, L. (2020). Perspectiva cronológica de las TIC en las organizaciones públicas venezolanas. *Educere, 24*(78), 337-349. https://www.redalyc.org/articulo.oa?id=356/35663284012

Bohórquez Taboada, Juan Carlos. (2024). Herramientas integradas por la ley 2213 de 2022 que lograron el funcionamiento de la justicia en Colombia en época de COVID 19. Universidad Libre de Colombia. Especialización Derecho Procesal. Colombia. file:///C:/Users/PC/OneDrive/Escritorio/articulo%20personali/articulo%20investigativo%20fernando%20bohorquez.pdf

Bolaños, F. y Gómez, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *Recibe. Revista electrónica de Computación, Informática, Biomédica y Electrónica, 4*(3), 1-12. https://www.redalyc.org/articulo.oa?id=5122/512251503001.

Biurrun Abad; Fernando J. (2018). Localización: *Actualidad jurídica Aranzadi,* ISSN 1132-0257, Nº 943.

Brichetti, Giovanni. (1973). *La evidencia en el Derecho Procesal Penal*. Jurídica Europa- América.

Cadavid, G. (2004). Cadena de custodia. *Instituto Nacional de Medicina Legal y Ciencias forenses.* https://www.medellin.gov.co/irj/go/km/docs/pccdesign/Subportaldel Ciudadano_2/PlandeDesarrollo_0_19/Publicaciones/Shared%20Content/Memorias%20y%20eventos/VI%20curso%20de%20vigilancia/Cadena%20de%20custodia%20-%20Dr%20 Dadavid.pdf

Camaño, E. y Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. *Revista de Ciencias Sociales Aplicadas,* I(10),61-80. https://www.redalyc.org/articulo.oa?id=5713/571361695004.

Canales, M. (2006). *Metodologías de investigación social*. Lom.

Cano, Juan. (2010). El peritaje informático y la evidencia digital en Colombia. Universidad de Los Andes.

Cano, M. y Jeimy, J. (2010). El peritaje informático y la evidencia digital en Colombia, *Conceptos, retos y propuestas*. [tesis de grado, Universidad de los Andes]. Repositorio institucional UNA.

Calvete León, Ivanna; Garcés Vásquez, Jorge Iván El paradigma del derecho en Colombia: la constitucionalización del derecho penal Nuevo Derecho, vol. 15, núm. 24, enero-junio, 2019, pp. 37-54. Institución Universitaria de Envigado.

Castañeda García, D. D. J. (2017). "La Culpabilidad Por La Vulnerabilidad Como Medida de la Pena: Una Revisión Al Concepto De Culpabilidad". ISSN-e 2500-672X, ISSN 2011-4540, Vol. 13, Nº 21 Revista Nuevo Derecho, 13 (21), 2017 Institución Universitaria de Envigado, Facultad de Ciencias Jurídicas y Políticas.

Castaño Galviz, W. (2018). *Derecho informático al alcance de todos* (1ª ed.). Editores Javier Hoyos Angulo. ISBN: 978-965-99887-7-8.

Caro John, J. A. (2021). Revisión Crítica de la Teoría del Dominio del Hecho

Caro John, J. A. (2006). Sobre la autoría en el delito de infracción de deber. Derecho penal y criminología (Vol. 27). Bogotá. Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/995

Carnelutti, F. (1944). *Sistema de derecho procesal civil* (Vol. 3). (N. A.-Z. Castillo, Ed.) Editorial Hispano Americana.

Carnelutti, F. (s.f.). *La Prueba Civil*. (N. A.-Z. Castillo, Trad.) Buenos Aires, Argentina: Ediciones ARAYÚ.

Chacón, Francisco. (2007). Sistemas informáticos: estructura y funciones, Madrid. https://www.preparadores.eu/te-mamuestra/PTecnicos/PComerciales.pdf

Chiesa, E. (2005). *Tratado de Derecho Probatorio.* Publicaciones JTS.

Climent, A. (1999). *La prueba pericial*. Tirant lo Blanch.

Climent Duran, Carlos, (1999). La Prueba Penal, Tiran, lo Blanch, Valencia,

Cobo, José Carlos. (2022) Digitalización de la justicia: prevención, investigación y enjuiciamiento. Printed in Spain. Impreso en España, Primera edición. ISBN: 978-84-1124-527-2 DL NA 571

Colombia. Asamblea Nacional Constituyente. (1991). Constitución política de Colombia. Bogotá: Gaceta Constitucional No. 116 de 20 de junio de 1991.

Colombia. Congreso de la República de Colombia. (2002). *Acto Legislativo 3 de 2002*. Diario Oficial No. 45.040.

Colombia. Congreso de la República. (2004). Ley 906, Por la cual se expide el Código de Procedimiento Penal. Bogotá: Diario Oficial No. 45.658 de 1 de septiembre de 2004.

Colombia. Corte Constitucional. (1992). Sentencia T-406 de 5 de junio de 1992. Magistrado Ponente: Ciro Angarita Barón. Bogotá: Corte Constitucional.

Congreso de la República de Colombia. (1974, 18 de diciembre). L*ey 20. Por la cual se aprueba El Concordato y Protocolo Final entre la República de Colombia y la Santa Sede*. Diario oficial. No 34234.

Congreso de la República de Colombia. (1999, 18 de agosto). Ley 527. *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* Diario oficial. No 23.435.

Congreso de la República de Colombia. (2004, 31 de agosto). Ley 906. *Por la cual se expide el Código de Procedimiento Penal.* Diario Oficial No. 45.658

Congreso de la República de Colombia. (2004, 31 de agosto). Ley 906. *Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004)*. Diario Oficial No. 45.658.

Congreso de la República de Colombia. (2009, 05 de enero). Ley 1273. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Diario Oficial. No 47223. 5

Congreso de la República de Colombia. (2009, 5 de enero). Ley 1273. *Por medio de la cual se módica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos "y se preservan integralmente los sistemas que utilicen las tecnologías de la Información y las comunicaciones, entre otras disposiciones*. Diario oficial. No 47.223.

Congreso de Colombia. (12 de julio de 2012) Artículo 247 [Titulo XI]. Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. [1564 de 2012]. DO: 48.489. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

Congreso de Colombia. (17 de agosto de 1999) Artículo 2 [Título I]. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [Ley 527 de 1999]. DO: 43.673. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso de Colombia. (17 de octubre de 212) Por la cual se dictan disposiciones generales para la protección de datos personales. [Ley 1581 de 2012]. DO:48.587. Recuperado en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de Colombia. (31 de agosto de 2004). Por la cual se expide el Código de Procedimiento Penal. [Ley 906 de 2004]. DO: 45.658. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a.htm

Congreso de Colombia. (5 de enero de 2009). Artículo 269F [Título I]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [Ley 1273 de 2009]. DO: 47.223. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de Colombia. (17 de diciembre de 1992). Artículo 6 [Título I]. Por la cual se desarrollan los incisos 9, 10, 11, 12 y 13 del artículo 42 de la Constitución Política y se modifica el Código Civil. [Ley 25 de 1992]. DO: 40.693. Recuperado en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0025_1992.html

Congreso de Colombia. (7 de marzo de 1996) Ley Estatutaria de Administración de Justicia. [Ley 270 de 1996]. DO: 42.745. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0270_1996.html

Congreso de Colombia. (18 de enero de 2011). Artículo 216. [Título IX]. Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. [Ley 1437 de 2011]. DO: 47.956. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011_pr005.html

Consejo de Estado, Sección Tercera. (13 de diciembre de 2017) Sentencia 2000-00082. [MP Stella Conto Díaz del Castillo] Recuperado de http://legal.legis.com.co/document/Index?obra=jurcol&document=jurcol_3738b5fb93a84fb6862262d58331e65b

Constitución Política de Colombia [Const.] (1991) Artículo 250 [Titulo VIII]. 2da Ed. Legis. Constitución Política de Colombia [Const.] (1991) Artículo 29 [Titulo II]. 2da Ed. Legis.

Corte Constitucional, Sala Octava. (10 de febrero de 2020) Sentencia T 043 de 2020. [MP José Fernando Reyes Cuartas] Recuperado de https://www.corteconstitucional.gov.co/Relatoria/2020/T-043-20.htm

Corte Constitucional, Sala Plena. (14 de marzo de 2018). Sentencia C 014 de 2018. [MP Diana Fajardo] Recuperado de https://www.corteconstitucional.gov.co/relatoria/2018/C-014-18.htm

Corte Suprema de Justicia. Sala de Casación Penal. Sentencia del 17 de septiembre de 2008. Radicación 30.214.

Corte Constitucional, Sala Plena. (19 de noviembre de 2014). Sentencia C 881 de 2014. [MP Jorge Ignacio Pretelt] Recuperado de https://www.corteconstitucional.gov.co/relatoria/2014/C-881-14.htm

Corte Constitucional, Sala Plena. (2 de noviembre de 2016) Sentencia C 604. [MP Luis Ernesto Vargas] Recuperado de https://www.corteconstitucional.gov.co/relatoria/2016/C-604-16.htm

Congreso de la República de Colombia. (2012, 12 de junio). Ley 1564. Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Diario Oficial No. 48.489.

Congreso de la República de Colombia. (2022). Ley 2213 de 2022. Por medio de la cual se establece la vigencia permanente del Decreto Legislativo 806 de 2020 y se adoptan medidas para imple-

mentar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia y se dictan otras disposiciones.

Cordero Ruiz, N. F. (2021). La ciberdelincuencia. Obtenido de Ebuah: https://ebuah.uah.es/dspace/handle/10017/49563

Corrales, M. y Osorio, M. (2015). *Diseño de la metodología para el manejo de incidentes T.I. mediante forénsica digital*. [tesis de grado, Corporación Universitaria Minuto de Dios]. Repositorio institucional UMD. https://repository.uniminuto.edu/bitstream/handle/10656/3659/TEPRO_CorralesMargarita_2015.pdf?sequence=1&isAllowed=y

Corte Suprema de Justicia. (2000, 8 de junio). Sentencia C-662/00. (Fabio Morón Díaz, M. P.). https://www.corteconstitucional.gov.co/relatoria/2000/C-662-00.htm

Corte Suprema de Justicia. (2007, 11 de abril). Sentencia C-128/07 (Jorge Enrique Gómez Ángel, M. P.). https://www.ramajudicial.gov.co/documents/9533918/21745755/1.+ACCESO+CARNAL+-VIOLENTO%20Valoraci%C3%B3n+probatoria+del+testimonio+-de+la+menor+v%C3%ADctima.+S2015-0089.pdf/80bac569-4981-4f1e-bab4-37abffb82c8d

Corte Suprema de Justicia. (2007, 21 de febrero). Casación No. 25920. (Julio Alberto Triviño Cruz, M. P.). https://webcache.googleusercontent.com/search?q=cache:kMD0dAef2tkJ:https://cortesuprema.gov.co/corte/wpcontent/uploads/relatorias/pe/spa/audiencia%2520preparatoria/evidencia%2520fisica%2520pertinencia%2520y%2520autenticacion/25920(21-02-07).doc+&cd=12&hl=es-419&ct=clnk&gl=co

Corte Suprema de Justicia. (2008, 17 de septiembre). Rad. 30214. (Sigifredo Espinosa Pérez, M. P.). https://www.redjurista.com/Documents/corte_suprema_de_justicia,_sala_de_casacion_penal_e._no._30214_de_2008.aspx#/

Corte Suprema de Justicia. (2012, 13 de junio). Rad.36562. (José Leónidas Bustos Martínez, M. P.). https://webcache.googleusercontent.com/search?q=cache:7-qKV2_hAaAJ:https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/spa/PRUEBA/CLAUSULA%2520DE%2520EXCLUSION/TEORIA%-2520DEL%2520ARBOL%2520ENVENENADO/36562(13-06-12).doc+&cd=2&hl=es-419&ct=clnk&gl=co

Corte Suprema de Justicia. (2012, 8 de agosto). Acta Nº 289. (Julio Enrique Socha Salamanca, M. P.). https://webcache.googleusercontent.com/search?q=cache:kMD0dAef2tkJ:https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/spa/AUDIENCIA%2520PREPARATORIA/EVIDENCIA%2520FISICA%2520PERTINENCIA%2520Y%2520AUTENTICACION/25920(21-02-07).doc+&cd=12&hl=es-419&ct=clnk&gl=co

Corte Suprema de Justicia. (2015, 22 de abril). Rad.45711. (Eugenio Fernández Carlier, M. P.). https://webcache.googleusercontent.com/search?q=cache:oEhTo0bCPeQJ:https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1may2015/AP2020-2015(45711).doc+&cd=1&hl=es-419&ct=clnk&gl=co

Corte Suprema de Justicia. (2017, 25 de septiembre). Sentencia T-263/10. (Carlos Bernal Pulido, M. P.). https://www.corteconstitucional.gov.co/relatoria/2017/t-593-17.htm

Corte Suprema de Justicia. (2017, 28 de abril). Sentencia T-276/17. (Aquiles Arrieta Gómez, M. P.). https://www.corteconstitucional.gov.co/relatoria/2017/t-276-17.htm

Corte Suprema de Justicia. (2017, 3 de febrero). Sentencia T-063A/17. (Jorge Iván Palacio, M. P.). https://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm

Corte Suprema de Justicia. (2017, 8 de agosto). AP965, tomo IV. (Julio Enrique Socha Salamanca, M. P.). https://webcache.googleusercontent.com/search?q=cache:kMD0dAef-2tkJ:https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/spa/AUDIENCIA%2520PREPARATORIA/EVIDENCIA%2520FISICA%2520PERTINENCIA%2520Y%2520AUTENTICACION/25920(21-02-07).doc+&cd=12&hl=es-419&ct=clnk&gl=-co

Corte Suprema de Justicia. (2018, 7 de marzo). Rad. 51882. (Patricia Salazar Cuéllar, M. P.). http://webcache.googleusercontent.com/search?q=cache:h5YwZpi0k5QJ:www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1abr2018/AP948-2018(51882).doc+&cd=11&hl=es-419&ct=clnk&gl=co

Corte Suprema de Justicia. (2019, 10 de diciembre). Sentencia SC-52382019. (Luis Armando Tolos A Villabona, M. P.). https://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm

Corte Suprema de Justicia. (2020, 4 de junio). Rad. 57143. (Patricia Salazar Cuéllar, M. P.). https://cortesuprema.gov.co/corte/wp-content/uploads/2020/07/SP2073-2020.pdf

Chicharro Lázaro, Alicia. 2013. “La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo”. En La Sociedad Ruido/ Entre el dato y el grito, editado por Javier Herrero et al, 80-81. La Laguna (Tenerife): Sociedad Latina de Comunicación Social.

Choi, K. S., & Toro-Álvarez, M. M. (2017). Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Seguridad Digital. Fondo Editorial Universidad Antonio Nariño.

Cruz Palmera, R., (2021). Fernando Velazquez Velazquez, Fundamentos de Derecho Penal. Parte General, Bogotá, Tirant lo Blanch, 2020, 957 páginas. Díkaion, 30(1), 192-195. https://doi.org/10.5294/dika.2021.30.1.7

Delgado, J. (2018). Investigación tecnológica y prueba digital en todas las jurisdicciones. Madrid, España: Wolters Kluwer.

Díaz, L. y Contreras, C. (2020). El testimonio técnico y su relación con el debido proceso: conceptualización y aspectos procesales. [tesis de grado, Universidad Cooperativa de Colombia]. Repositorio institucional UCC. https://repository.ucc.edu.co/bitstream/20.500.12494/33582/1/2020_testimonio_tecnico.pdf

Dodge, C., & Burruss, G. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. In Leukfeldt, R., & Holt, T.J. (Eds.). The human factor of cybercrime (pp. 339-358). Routledge

Escobar, E. (2016). Las excepciones y las nulidades en el código general del proceso. Librería Jurídica.

Estrada, R., Unás, J. y Flórez, O. (2020). Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolívar (Tuluá, Colombia). Revista Logos, Ciencia & Tecnología, 12(1),121-131. ISSN: 2145-549X. Disponible en: https://www.redalyc.org/articulo.oa?id=5177/517762281011

Espada Bueno. Pablo. (2021). Perito Informático Judicial. https://blog.peritotecnologico.net/

Erazo, F. (2020). El Servicio Secreto de EE. UU. crea un grupo de trabajo sobre delitos informáticos relacionados en las finanzas.

Evidentia Digital S.L.U. (2020). *Reglamento general de protección de datos) y con la Ley de la Sociedad de Servicios de la Información y Comercio Electrónico,* Ley 34/2002, de 11 de julio. http://www.evidentia.es/

Fernández, C. (2002). *Al hablar de la prueba pericial.* https://indalics.com/serviciosperitaje-informático/grabaciones-de-audio-digital. https://oscarleon.es/maximas-interrogar-al-perito-i/

Fernández, J. (2018). La prueba tecnológica en la era digital. Recuperado de https://www.youtube.com/watch?v=IR6ATRSCsN4

Ferrajoli, L. (2012). Constitucionalismo principialista y constitucionalismo garantista. En debate sobre el constitucionalismo. Madrid: Marcial Pons.

Ferrajoli, L. (2014). La democracia a través de los derechos. El constitucionalismo Garantista como modelo teórico y político. Madrid: Editorial Trotta

Forensictic. (2021). *Company*. https; //www.linkedin.com/company/65617140/admin/Gacetas de la Asamblea Nacional Constituyente. (1991). *Informe de ponencia Asamblea Nacional Constituyente, Constitución Política de Colombia.* Gaceta Oficial no. 68.

Gallardo, M. (1996). Ámbito Jurídico de las tecnologías de la información. Cuaderno de Derecho Judicial, 11(2), 1-1. https://biblioteca.ief.es/cgi-bin/koha/opac-detail.pl?biblionumber=56161&shelfbrowse_itemnumber=64456

García, J. (2015). *Peritaje Informático*. Audiovisual y Sociedad de la Información.

Gómez-Agudelo, Dany Steven. (2020). Implicaciones jurídicas de la evidencia digital. Universidad Autónoma Latinoamericana. pp. 220-240, editores UNAULA Medellín-Colombia. DOI: 10.24142/raju.v15n30a11, Revista Ratio Juris Vol. 15 N.º 30 • UNAULA ISSN 1794-6638 eISSN: 2619-4066 DOI: 10.24142/raju

González, J. (2020). “La responsabilidad de los llamados “intermediarios tecnológicos” está definida -por lo menos normativamente- desde el año 2000, en la Directiva Europea y, desde el 2002, en la normativa española denominada Ley de Servicios de la Sociedad de la Información.” https://www.cepal.org/sites/default/files/publication/files/13309/S2010986_es.pdf

González Castellanos, José Andrés y Torrado Pérez, Oscar Duvan. (2019). La balística forense, un estudio a cargo de la fiscalía general de la nación. Recuperado de: https://hdl.handle.net/10901/19125.

González Cussac, José L. (2015). Cuadernos de Derecho Penal, Derecho penal de la Universidad de Valencia, España. ISSN: 2027-1743.

Guijarro, A., Cevallos, L. y Cárdenas, D. (2016). Análisis, incidencias y mitigación de un ataque basado en diccionario. Journal of Innovation and Applied Studies, 17(3), 872-883. http://www.ijias.issr-journals.org/abstract.php?article=IJIAS-16-

Guzmán, A. (2020). Procesalistas estudian el valor probatorio de los "pantallazos" de WhatsApp. Ámbito Jurídico. [Archivo de Video]. https://www.ambitojuridico.com/noticias/general/procesal-y- disciplinario/procesalistas-estudian-el-valor-probatorio-

Gimeno Sendra, José Vicente. (2020). La actividad procesal y la prueba en el derecho penal. Editorial Jurídica. ISBN: 9788413086293

Guimaraes, D. (2019). La prueba digital. En Agudelo, D, Pabón, L, Toro, L,

Bustamante, M & Vargas, O. La prueba: teoría y práctica (pp. 521 – 539). Medellín: Universidad de Medellín.

Grijalva, J. y Loarte, B. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador. CienciAmérica, 6 (3), 1-7. https://dialnet.unirioja.es/servlet/articulo?codigo=6163708

Hernández, R; Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación*. McGraw Hill.

Hernández, R; Fernández, C. y Baptista, P. (2018). *Metodología de la Investigación*. McGraw Hill.

Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge. https://doi.org/10.4324/9781315775944

Hormiga Rincón, Jenifer (2020). Diferencias entre la prueba pericial y el testigo técnico, su valoración judicial en el proceso contencioso administrativo, Facultad de Derecho y Ciencias Políticas de la Universidad de Antioquia.

Izquierdo Blanco, P., (2011). Pericial informática. De acordarse una pericial informática, ¿qué titulación debe reunir el perito encargado de practicar la pericia, Colección de Formación Continua Facultad de Derecho ESADE, J. M. Bosch editor, pp. 403-409. ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. [en línea]. Disponible: https://www.iso.org/standard/44406.html

Jaramillo, A. (2015). *Práctica de Familia*. Ediciones Doctrina y Ley Ltda. Jaramillo, A. (2015). Procedimiento Civil Aplicado. Doctrina y Ley Ltda.

Jiménez, W. y Meneses, O. (2017). Derecho e internet: introducción a un campo emergente para la investigación y práctica jurídicas. *Prolegómenos. Derechos Y Valores, 20*(40),43-61. https://www.redalyc.org/articulo.oa?id=876/87652654004

Fenech, Miguel. Derecho procesal. T. I 2da edición, Barcelona Editorial Labor S.A, Pag. 857.

Lanzillotti, A. y Korman, G. (2020). ¿Qué informa la prensa escrita argentina acerca del fenómeno de cyberbullying? Interdisciplinaria, 37(1), 0325-8203. https://www.redalyc.org/articulo.oa?id=180/18062047003

Locard, E. (1935). *Manual de Técnica Policiaca*. SECCIF.

López, H. (2009). *Instituciones del Derecho Procesal Civil Colombiano*. Dupre.

López Soria, Y. La teoría del delito: revisión crítica del elemento culpabilidad [en línea]. Tesis Doctoral. Pontificia Universidad Católica Argentina, 2020. Disponible en: https://repositorio.uca.edu.ar/handle/123456789/11122

López Delgado Miguel. (2007). Análisis Forense Digital Segunda Edición, revisada y adaptada para su publicación en CriptoRed. pp. 10.

Lozada, A. (2019,). [Entrevista con Ángela Lozada, ingeniera de sistemas y abogada. Miembro de un laboratorio forense digital].

Luz Clara, Bibiana Beatriz. (2018). La mediación en entornos electrónicos. Revista IUS, 12(41), 343-358. Recuperado en 23 de septiembre de 2024, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100343&lng=es&tlng=es

Luz, B. (2018). La mediación en entornos electrónicos. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C., 12*(41), 343-358. https://www.redalyc.org/articulo.oa?id=2932/293258387018

Martínez, C. (2019). El uso de efectivo y tarjetas débito como instrumentos de pago en Colombia. *Lecturas de Economía, (90),*71-95: https://www.redalyc.org/articulo.oa?id=1552/155258871003

Mayer, L. (2019). El bien jurídico protegido en los delitos informáticos. Revista Chilena de Derecho, 44(1), 235-260. https://doi.org/10.4067/S0718-34372017000100011

Meléndrez, V. (2018). Logística del Comercio Electrónico: cross docking, merge in transit, drop shipping y click and collect. *Científica*, 22(2), 105-112. https://www.redalyc.org/articulo.oa?id=614/61458109003

Meneses Obando, O. (2019). Informática forense desde el recurso humano y tecnológico, en las instituciones judiciales que cuentan con el servicio especializado de peritaje informático en Colombia. Bogotá: Universidad Externado de Colombia

Meza, H. R. (2017). La iniciativa judicial probatoria. La prueba de oficio en el proceso contencioso administrativo. Bogotá, Colombia: Leyer.

Ministerio de Justicia y del derecho. (2020). Decreto 806 de 2020. *Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de Emergencia Económica, Social y Ecológica*. El Ministerio.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (17 de mayo de 2018). Guía número 13 sobre seguridad y privacidad de la información. [Fotografía]. https://www.mintic.gov.co/gestionti/615/articles 5482_G13_Evidencia_Digital.pdf

Nadolna, M., & Rudenko, A. (2021). Interpol activities to coordinate cooperation to fight cybercrime. Topical issues of humanities. Technical and Natural Sciences, 299-302. https://jti.donnu.edu.ua/article/view/12014

Naik, A. (2020). La intersección de los delitos financieros y cibernéticos en la era digital. Revista de Criminología y Seguridad.

Novoa Toledo, I. y Venegas Cruz, L. (2020-07). Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. Disponible en https://repositorio.uchile.cl/handle/2250/176344

Organización de los Estados Americanos. (1961). Convención de Viena sobre relaciones diplomáticas. http://www.oas.org/legal/spanish/documentos/convencionviena.htm

Ovalle, T., Coronel, D., Contreras, R. y Cabrera, A. (2019). Impacto sobre la seguridad personal frente a la regulación de la ciberdelincuencia en la Universidad de Pamplona, sede de Villa del Rosario. Respuestas, 24(3), 14-25. https://doi.org/10.22463/0122820X.1845.

Pabón, P. (2010). Manual de Derecho Penal Tomo II - Parte Especial ha sido registrado con el ISBN 978-958-676-494-0 en la Agencia Colombiana del ISBN. Ediciones Doctrina y Ley.

Parra, J. (2018). *Derecho de Familia*. Temis S.A.

Pasamar, Abraham. (2011). La prueba pericial informática frente a la impugnación de la autenticidad de un e-mail-Sotelo Vázquez. Aurora. (2011). *Luces y Sombras de la prueba pericial en la LEC*.

Patiño, G. (2019). El sistema internacional cibernético: elementos de análisis. OASIS, (30),163-186. https://www.redalyc.org/articulo.oa?id=531/53163845010

Pons Gamón Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Universidad Nacional de Educación a Distancia (UNED), España. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, pp. 80-93, 2017. Facultad Latinoamericana de Ciencias Sociales.

Puig, S. (2015). La prueba electrónica: sus implicaciones en la seguridad de la empresa. https://www.tdx.cat/bitstream/handle/10803/285237/TESI%20DOCTORAL%20S%C3%92 NIA%20 PUIG%20FAURA.pdf?sequence=1.

Quiroz, A. (2007). Sociedad Conyugal y Patrimonial de Derecho. Doctrina y Ley Ltda. Reuters Thomson, Llorente Sánchez, Mercedes, Arjona. Calaza López, Sonia, Muinelo.

República de Colombia. (1991). *Constitución Política de Colombia de 1991*. https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

Reuters. (2018). Nuevo tipo de programas de inteligencia artificial llevarán ciberdelitos a otro nivel. *El Financiero*. Recuperado de https://www.elfinanciero.com.mx/tech/nuevo-tipo-de-programas-de-inteligencia-artificial-llevaran-ciberdelitos-a-otro-nivel.

República de Colombia, Congreso de la República, Ley 1564 de 2012, Diario Oficial No. 48.489 de 12 de julio de 2012, “Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones”.

Reuters, Thomson, Llorente Sánchez, Mercedes, Arjona. Calaza López, Sonia, Muinelo Cobo, José Carlos. (2022). Editorial Aranzadi, S.A.U. Camino de Galar, 1531190 Cizur Menor (Navarra). ISBN: 978-84-1124-527-2 DL NA 571-2022, Printed in Spain. Impreso en España Fotocomposición: Editorial Aranzadi, S.A.U. Impresión: Rodona Industria Gráfica, SL Polígono Agustinos, Calle A, Nave D-1131013 – Pamplona

Reuters Thomson, Custis, Tonya (2018). Los temores que los despachos de abogados americanos tienen con la implantación de la Inteligencia Artificial en el ámbito legal. Tonya dirige un equipo de científicos que realizan investigación aplicada en tecnologías de Inteligencia Artificial (IA). Recientemente, fue panelista en Legaltech (parte de Legalweek New York de ALM

Reyes, L. (2006). *Código de la Infancia y la Adolescencia.* Ediciones Doctrina y Ley Ltda.

Rico, M. (2017). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C.,* 7(31), 207-222. https://www.redalyc.org/articulo.oa?id=2932/293227561011 [17].

Rivera, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. *Revista e-Ciencias de la Información, 9*(2), 68-81. https://www.redalyc.org/articulo.oa?id=4768/476862530004.

Rocha, A. (1967). De la prueba en Derecho. Lerner.

Rodríguez-Márquez, Maribel Patricia. (2021) “Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano,” Rev. UISIng., vol. 20, no. 3, pp. 19-46, doi: 10.18273/revuin.v20n3-2021002 Rodríguez, J., Oduber, J. y Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20),63-79. https://www.redalyc.org/articulo.oa?id=5526/552656641006

De la Torre, Rodríguez, P .(2022). Marco normativo de la actividad de perito informático, España: Madrid

Rojas, J. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. *Revista Logos, Ciencia & Tecnología*, 8(1), 220-231. en:https://www.redalyc.org/articulo.oa?id=5177/517754055021

Roxin, C. (2003). Strafrecht Allgemeiner Teil Band II: Besondere Erscheinungsformen der Straftat. München: C. H. Beck.

Roxin, C. (2015). Täterschaft un Tatherrschaft. Berlin

Rubio, J. (2014). Peritaje informático de conversaciones de WhatsApp o aplicaciones similares. https://peritoinformaticocolegiado.es/blog/peritaje-informatico-de-conversaciones-de-whatsapp-o-aplicaciones-similares/

Ruiz Díaz, Joaquín. 2016. “Ciberamenazas: ¿el terrorismo del futuro?”, http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Sánchez, N., Pulido, B. y Camacho, J. (2017). La significativa evolución en seguridad de la información para la Policía Nacional de Colombia. Revista Logos, Ciencia & Tecnología, 9(1), 230-234. https://www.redalyc.org/articulo.oa?id=5177/517752178018

Suarez Fonseca, M. (2021). “El delito de interceptación de datos informáticos en el ordenamiento jurídico colombiano: inconvenientes en su tipificación y aplicación. especialización en derecho penal y procesal penal. universidad Santo Tomas, seccional Tunja.

Silogismo. (2012). Universidad de Guadalajara, México. Recuperado de: http://www.objetos.unam.mx/logica/silogismos

Suárez, R. (1999). *Derecho de Familia*. Temis S.A.

Shick, K. y Toro, M. (2017). Cibercriminología. Guía para la investigación del cibercrimen y las mejores prácticas en seguridad digital. Bogotá, Colombia: Antonio Nariño.

Steinmetz, K. F., & Yar, M. (2019). Cybercrime and society. Cybercrime and Society. SAGE Publications

Strasburger, V. C., Zimmerman, H., Temple, J. R., & Madigan, S. (2019). Teenagers, sexting, and the law. Pediatrics, 143(5), e20183183. https://doi.org/10.1542/peds.2018-3183

Tiedemann, K. (1985). Criminalidad mediante computadoras. *Revista Nuevo Penal*, 4(30), 1-15.

Toro-Álvarez, M. M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. Revista Logos Ciencia & Tecnología, 15(2), 162-173. https://doi.org/10.22335/rlct.v15i2.1768

Tribunal Superior de Medellín. (2016, 25 mayo). Rad. 2012-19107. (Sala de Decisión Penal). https://vlex.com.co/vid/670303621

Urueña Centeno, F. J. (2015). *Ciberataques, la mayor amenaza actual.* Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

Vargas, A. V. *Paso a paso de cómo usar Lifesize.* Rama Judicial. Recuperado de https://www.ramajudicial.gov.co/documents/10056457/35883012/Manual+LifeSize+para+Abogados-Intervinientes.pdf/77b317d7-de334b13-b8c4 58a110eecf0a#:~:text=Administrativo%20de%20Caldas,1.,a%20tu%20flujo%20de%20tra bajo

Vásquez Peña Ilse Gabriela y Claudia Yaneth Ardila Angarita (2019). *Prueba Pericial: estudio de la idoneidad del perito para el desarrollo de la práctica de la prueba,* Ley 906/2004. Recuperado de: https://hdl.handle.net/10901/1549

UNE 71506/2013. Metodología para el análisis forense de las evidencias electrónicas. [en línea]. Disponible: https://peritosinformaticos.es/une-71506-perito-informatico/

Velásquez V., F. (2009). Derecho Penal, Parte General (4a ed.). Bogotá, D.C.: Comlibros.

Vita, L. (2020). Cómo certificar un chat de WhatsApp para que funcione como prueba en un proceso judicial. https://www.asuntoslegales.com.co/consumidor/como-certificar-un-chat-de-whatsapp-para-que-funcione-como-prueba-en-un-proceso-judicial-3094511

Vuanello, R. (2012). La interpretación de docentes sobre la seguridad de los jóvenes en el uso de las TICs. Perspectivas en Psicología: *Revista de Psicología y Ciencias Afines, 9*(3),24-30. https://www.redalyc.org/articulo.oa?id=4835/483549016004.

SELLO EDITORIAL

UNIVERSIDAD
DE PAMPLONA

ISBN (Digital): 978-628-7656-61-1