PRUEBAS DIGITALES COMO MEDIO PROBATORIO[1]

María Camila Luján Herrera[2]
Paula Valentina Vásquez Ospina[3]

RESUMEN:

En una sociedad que migra cada vez más hacía lo digital se aprecia la necesidad de indagar acerca de las pruebas digitales como medio probatorio y su valor, ya que contiene datos o informaciones almacenadas en un dispositivo o red de comunicación abierta, o cifrados en sistemas o mensajes de datos. Además, el principal objetivo es establecer cómo se regulan las pruebas electrónicas en nuestro país y cómo se deben presentar para que tengan su debida validez. Por ejemplo, una fuente de prueba digital tan común como lo es WhatsApp que contiene en sí mensajes de texto, notas de voz, videos, contactos, ubicación y SMS que es indispensable recurrir directamente a los dispositivos electrónicos usados para su conversación para encontrar su contenido.

También se presentan conductas por medios electrónicos tan comunes en el siglo XXI, que se necesita enfatizar en ellos y su afectación social y legal con conductas que categorizan la ciberdelincuencia y delimita situaciones particulares de la cotidianidad, por ejemplo: caso concreto de las alteraciones de imagen en redes sociales, que engloban conductas categorizadas en normativas vigentes. Se concluye que se debe adoptar medidas para el cuidado y conservación de la evidencia digital, debido a que su contenido es frágil y de manipulable acceso.

---

[1] Artículo de revisión bibliográfica para optar por el título de Abogado en la Universidad Católica Luis Amigó. Asesor temático: Dany Steven Gómez Agudelo

[2] Estudiante de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó. maria.lujanhe@amigo.edu.co

[3] Estudiante de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó. Paula.vasquezos@amigo.edu.co

PALABRAS CLAVES: Documento electrónico; evidencia digital; internet; medio probatorio; tecnología; ciberdelincuencia.

ABSTRACT:

In a society that is migrating more and more towards the digital, the need to inquire about digital evidence as a means of proof and its value is appreciated, since it contains data or information stored in a device or open communication network, or encrypted in systems or data messages. In addition, the main objective is to establish how electronic evidence is regulated in our country and how it must be presented so that it is valid. For example, a digital evidence source as common as WhatsApp that contains text messages, voice notes, videos, contacts, location and SMS that it is essential to go directly to the electronic devices used for your conversation to find its content.

Behaviors are also presented by electronic means so common in the 21st century, that it is necessary to emphasize them and their social and legal affectation with behaviors that categorize cybercrime and delimit particular situations of everyday life, for example: specific case of image alterations in social networks, which encompass behaviors categorized in current regulations. It is concluded that the care given to digital evidence must be taken into account, due to the fact that its information is fragile and of manipulable access.

KEYWORDS: electronic document; digital evidence; Internet; means of proof; technology; cybercrime.

INTRODUCCIÓN

El constante crecimiento tecnológico que se denota actualmente y su relevancia en la vida cotidiana de la población, incide en el ámbito jurídico directa e indirectamente. La cantidad de material electrónico que circula cada segundo en las diversas redes sociales se convierte en medios probatorios no tradicionales, que actualmente se han involucrado bajo criterios de necesidad en legislaciones nacionales e internacionales en razón a su adaptación al mundo moderno.

La prueba digital actualmente le brinda una verdadera admisibilidad y credibilidad al proceso jurisdiccional. Esta investigación cuenta con un objetivo primordial que consiste en saber el alcance que se le puede dar a la prueba digital, su reconocimiento jurídico y cuál es el requisito para que sea tenido en cuenta siempre y cuando sea accesible a diferentes consultas.

Por consiguiente, es fundamental conocer qué se entiende por prueba, como lo dice López (2002): "prueba constituye el procedimiento de acreditar los hechos afirmados. En tanto, el medio de prueba es el instrumento a través del cual se busca lograr la convicción sobre el acaecimiento de un hecho particular" (p. 323). A pesar de que constantemente se manipule este tipo de evidencia, cuenta como pieza procesal importante al momento de probar. La prueba funge como una actividad procesal de las partes, mediante la que se busca el convencimiento de orden legal, en estos casos la ley 527 de 1999 asigna algunos criterios a los jueces para valorar los mensajes de datos.

Cabe resaltar que el material probatorio puede ser usado como fin o como medio. Como fin la prueba va orientada a demostrar la existencia y el contenido de un hecho del que depende un derecho. Como medio es un conjunto de recursos que pueden utilizarse para obtener dicha demostración, el fin de la prueba. En este orden de ideas, una prueba electrónica se puede entender como una información de valor probatorio contenida o transmitida por un medio electrónico que tiene la capacidad de acreditar los hechos, y entra la tecnología en este ámbito porque acaba siendo medio de manifestación en el contexto.

Conjuntamente conviene reconocer que actualmente muchas personas recurren a los mensajes electrónicos, como pruebas de lo que sucedió o como un medio idóneo, para probar la veracidad de los hechos o argumentos, debido a la alta demanda tecnológica que se presencia termina siendo un aliado procesal.

Esta investigación es desarrollada bajo criterios cualitativos tras la cual se realizan investigaciones históricas, comparativas.

Se utilizó la técnica de la revisión documental, analizando en conjunto las referencias encontradas con antecedentes de investigación, leyes y jurisprudencia vigente que permitieron al artículo clarificar conceptos para evaluar el concepto de la prueba digital como medio probatorio, como proceso metodológico se trabajó en el análisis correspondiente a teorías y herramientas de datos que facultan a los medios procesales y probatorios dentro de los procesos jurisdiccionales.

Se pretende bajo esta investigación recoger los datos que pueda hallarse sobre la prueba digital en una modalidad cualitativa que permita su obtención para posteriormente ser analizados en el presente texto.

I. ASPECTOS HISTÓRICOS.

Para comprender el avance de las telecomunicaciones y de todos los medios informáticos, sería conveniente realizar un símil del derecho antiguo con el derecho moderno, y así tener un mayor entendimiento respecto al tema.

De hecho, se conoce que el derecho debe avanzar progresivamente con la sociedad, ya que este debe atender a sus realidades sociales para mantener un orden social justo; en el siglo XXI, en plena revolución tecnológica, cuando la informática avanza a pasos agigantados, el sistema jurídico debe avanzar progresivamente con esto, en una misma línea de tiempo, para así tener la capacidad de atender todos los problemas jurídico-legislativos, sociales, políticos y económicos de la sociedad actual.

En la antigüedad el derecho era simple, ya que solo existía un mandato y una amenaza con una sanción, y las fuentes de este mismo era la voluntad del gobernante, la divinidad, o las costumbres de esa misma sociedad.

En la era remota se expresaron actuaciones donde ésta forma probatoria era simplemente una idea utópica, aclamada por las personas con el fin de aportar un elemento clave que determinaría su juicio. Aun así, cabe señalar que aparte de la historia, se desea identificar el

nacimiento y desarrollo de dichas pruebas digitales, y desde casos fácticos analizar si el consentimiento de este moderno modo probatorio es una forma más de beneficiar aquellos que puedan, lucrativamente, contratar para manipular pruebas que sirvan como ayuda pertinente en su caso, o si por el contrario, gracias a sus regulaciones y requisitos para que ésta se tome en cuenta ayuden a retomar la esencia de la justicia.

En la sociedad actual, el derecho no solo cuenta con muchas más fuentes, tanto principales y auxiliares, como lo son la doctrina, la jurisprudencia, el precedente judicial, la ley, la costumbre, entre otras; también ha avanzado en materia probatoria en el sistema jurídico, el cual será nuestro tema a tratar. Además, resulta oportuno hacer mención de leyes y jurisprudencias trascendentales en el tratamiento del material electrónico, y conocer los antecedentes históricos del tema.

En la edad antigua, 3500 años A.C, el hombre se comunicaba mediante signos abstractos o dibujos, después se dio el invento y la transformación del telégrafo, en el año 1729 la electricidad pudo ser transmitida, en 1876 se patentó el primer teléfono, en 1936 se fabricó la primera computadora, en 1969 nace el internet, desde el año 1970 se continuó con el avance de redes que ha evolucionado en el almacenamiento de información en dispositivos móviles que ha facilitado en muchos aspectos la vida laboral y personal del ser humano.

Hoy en día, estas herramientas tecnológicas e informáticas podrían servir como medios para facilitar información para la reconstrucción de los hechos sobre determinados casos, y ser utilizadas como pruebas.

Aunque, estos avances tecnológicos traen consecuencias indeseadas, esto genera dificultad en la aceptación de estas herramientas informáticas como medios probatorios, ya que, al tener poco control e investigación sobre la veracidad de esta información, sería pernicioso incorporarlas en el sistema judicial.

II. FUNDAMENTO LEGAL Y JURISPRUDENCIAL.

Actualmente, al referirse al mensaje de datos en la ley 527 de 1999, no se logra dimensionar el amplio espectro que proporciona y su significativa cooperación en la globalización de las

relaciones económicas, el efecto de su transformación, las secuelas que propaga en el tratamiento de los actos y negocios jurídicos, diligenciados de manera pertinente y trae consigo una necesidad que se presencia especialmente en el ámbito jurídico, y es la trascendencia de regular, reglamentar y legalizar jurídicamente su adecuada utilización.

Para empezar, a partir de 1996 fue aprobada por la resolución 51/162 Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, el 16 de diciembre de 1996 de la comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI)/ United Nations Commission for the Unification of International Trade Law (UNCITRAL), que constituye una de las fuentes del derecho uniforme del comercio electrónico. En efecto, esta ley consagra una serie de principios sobre los cuales se inspira el derecho del comercio o contratación electrónica y su ámbito de aplicación corresponde a todo tipo de información en forma de mensaje de datos utilizada en el contexto de actividades comerciales.

Una de las cuestiones que motivó la elaboración de esta ley fueron los inconvenientes que en el tráfico jurídico internacional se podían presentar con la utilización de los medios informáticos, cabe anotar que también era evidente la ausencia de criterios para examinar registros informáticos como prueba en los procesos judiciales. Esta ley constituye un punto de partida para la regulación de la contratación electrónica y la eficacia probatoria del documento electrónico en los ordenamientos jurídicos internos de los Estados (Cruz Tejada, 2015).

Dado lo anterior, esta resolución de la ONU fue incorporada a la legislación interna colombiana por medio de la Ley 527 de 1999, por la cual se regula el acceso y el debido uso de los mensajes de datos, comercio electrónico y firmas digitales, bajo las cuales las entidades deben otorgar certificaciones. Esta ley trajo el principio de equivalente funcional, según el cual el documento electrónico tendrá el mismo valor probatorio que el documento en papel, siempre y cuando se cumplan los requisitos de originalidad, firma y posibilidad de acceso posterior.

En un principio fue aplicable al campo de las transacciones comerciales que se hacían por medios electrónicos, para que esos mensajes de datos tuviesen fuerza obligatoria, pero hoy en día es una ley transversal que se aplica a distintas áreas del Derecho, concediendo un reconocimiento y valor probatorio a los documentos electrónicos.

Por consiguiente, incluye aspectos como el ámbito de aplicación, definiciones de interés, requisitos jurídicos a los mensajes de datos y su alcance probatorio y las firmas digitales. También crea las autoridades de certificación y contiene un capítulo especial en materia de transporte de mercancía, en el artículo número 5, la ley establece que no se negarán los efectos jurídicos, validez o fuerza obligatoria a la información que esté en la forma de datos. Trata también lo referente a la integridad de un mensaje de datos, admisibilidad y fuerza probatoria de los mensajes, aborda lo relacionado con los escritos, firma y el original. La ley 527 de 1999 en su artículo 10, reconoce valor probatorio al documento electrónico, estableciendo:

> En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original (Ley 527, 1999, art. 10).

Continuamente, el Código General del Proceso hizo referencia a documentos de tipo físico y electrónico que pueden ser originales o reproducidos. Un documento que se creó electrónicamente y luego se imprime, esta impresión se convierte en una copia física de un original electrónico que también es tenido en cuenta como medio probatorio. Sobre el particular, el legislador indicó:

> Distintas clases de documentos: Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares (Ley 1564, 2012, art. 243).

Por otro lado, los documentos son públicos o privados. Documento público es el otorgado por el funcionario público en ejercicio de sus funciones o con su intervención. Así mismo, es público el documento otorgado por un particular en ejercicio de funciones públicas o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es autorizado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública.

En esa línea legislativa, el artículo 120 de la ley 1395 de 2010 en la cual se adoptan medidas en materia de descongestión judicial, permitió la notificación por medios electrónicos. Así mismo, la ley 1437 de 2011 específicamente en el artículo 216, se admitió la utilización de medios electrónicos para efectos probatorios, en los artículos 53 al 64 también se estipulan diferentes procedimientos y trámites en los cuales es válido la utilización de medios electrónicos para ello.

La sentencia C-662 de 2000 menciona la libertad informática en los siguientes términos:

> 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 le cumplan requisitos técnicos y jurídicos plasmados en la ley (Corte Constitucional, Sentencia C 662, 2000).

En esta sentencia se pretendía interponer la acción de inconstitucionalidad en contra de la ley 527 de 1999, la cual resuelve declarar exequibles las disposiciones demandadas.

De la misma manera, la ley 1564 de 2012 o Código General del Proceso expedido el 12 de julio de 2012 en su artículo 103 y sus posteriores parágrafos, estipula el uso de las tecnologías de la información y de las comunicaciones para proporcionar y agilizar el acceso a la justicia. Es pertinente que las autoridades judiciales cuenten con lo necesario para generar, archivar y comunicar mensajes de datos, el plan de justicia digital que permita expedientes digitales y litigio en línea. Cuando se refiere a uso de correo electrónico o semejante deben garantizar autenticidad e integridad del intercambio o acceso de información.

Igualmente, el artículo 244 inciso quinto presume la autenticidad de los documentos presentados por mensaje de datos. Adicionalmente, lo hace el artículo 247 del mismo código hablando de la valoración de mensajes de datos desde donde fueron generados, enviados o recibidos o en un medio que lo demuestre con exactitud, también se valorará la impresión.

De la misma manera, con relación al plan de justicia digital es preciso hablar de la ley 2213 de 2022 bajo la cual se establece la permanencia de precisiones procesales del uso de la virtualidad, con premisas frente a los planteamientos digitales de los procesos jurisdiccionales, estos procesos virtuales están a medida para garantizar a los portadores de la justicia agilidad y celeridad para la celebración adecuada de los mismos. Por ello se deja claridad que en el año 2022 la virtualidad

será la regla general en el desarrollo procesal, una excepción de ello, será: las audiencias sólo serán presenciales las audiencias y diligencias destinadas a la práctica de pruebas, por ejemplo, en la jurisdicción penal, donde el juez requerirá la práctica presencial de verlo necesario y lo dispondrá si alguna de las partes lo solicite incluso sin motivar la petición.

Los documentos electrónicos procesales se manejan bajo mensajes de datos y cada uno de ellos forja canales digitales para la efectividad del proceso, de la misma manera se implementan los medios tecnológicos determinados para la ejecución de audiencias y demás trámites que lo requieren, de igual manera se fijan virtualmente en las web autorizadas los estados y demás avisos que integren el proceso.

Por consiguiente, el documento electrónico debe contar con tres principios básicos, integridad en cuanto se usa una técnica de la criptografía denominada firma digital que permite verificarla, autenticidad con la firma digital que permita su verificación, finalmente su confidencialidad, para esta se utiliza una técnica denominada cifrado o encriptado (Reyes Sinisterra, C.A, 2013).

Así las cosas, todo medio tecnológico es manipulable y por ende debe cumplir con el principio de lealtad y veracidad de la prueba, que indica que la prueba no sea utilizada para deformar u ocultar la realidad y que también acuda al principio de la necesidad de la prueba. Con los avances de la modernidad, es factible recurrir a la tecnología para resolver inconvenientes jurídicos.

De otro lado, haciendo una línea de tiempo se presencia una constante evolución de los elementos materiales probatorios. En 2003, se consideraban desktops y laptops: CD, DVD, USB, DISCOS EXTERNOS. En 2005, se añaden los teléfonos móviles a los elementos probatorios como Smartphone, Sim Cards, Memorias SD. En 2008, se añaden dispositivos móviles como el iPad, iPhone, iCloud. Finalmente, en 2015, los vestibles como I Watch, I Glass y dispositivos médicos.

Seguidamente, el dispositivo debe quedar a disposición total del caso y llevarlo a juicio como prueba que soporte el mismo contenido, esto es un procedimiento que inicia con la incautación o aporte del dispositivo al facultado, el mismo entrega a disposición de las autoridades competentes para ejercer la adecuada cadena de custodia a criterio se exponga en la legislación nacional para

posterior, extraer la información probatoria o lo necesario del dispositivo móvil aportado como material probatorio.

A continuación se mencionan la consistencia del ejercicio de la cadena, iniciará por la observación, el análisis y la valoración del lugar o elemento probatorio, este se fijará y documentará en el momento; para posterior a ello, a lo que se consiga efectuar la recolección, embalaje y rotulado de los EMP y EF, para que sean entregados y enviados a los almacenes de evidencias para ser valorados por expertos.

También es de anotar en concordancia con fundamentos legales, la veracidad de las lagunas y vacíos legales que disuaden el propósito de la investigación y ello se desarrollará de la siguiente manera, mencionando los documentos CONPES que dirigen su enfoque en llenar ciertos espacios, se definen bajo el siguiente concepto:

> "El documento Conpes es la sigla que hace referencia al Consejo Nacional de Política Económica y Social. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país". (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

Pero, ¿para qué realizar un documento Conpes sobre Seguridad Digital? A continuación se responde a este interrogante, en Colombia se deben realizar controles de riesgos respecto a la seguridad digital bajo la razón de tener que promover un entorno digital que garantice beneficios económicos y sociales a los ciudadanos, dando competitividad ante la producción de los sectores económicos.

Ya con una apreciación clara sobre esto, se proseguirá con el contenido del CONPES 3701, el cual manifiesta que uno de los principios de la seguridad digital: siendo esta una situación donde se da cumplimiento a uno de los fines del estado consistente en otorgar a la ciudadanía un equilibrio y tranquilidad respecto al desarrollo del entorno digital, garantizando gestiones de riesgo a nivel nacional es la interacción activa de las partes interesadas, esto lo que hace es establecer que el Estado tiene la responsabilidad de realizar políticas en ciberseguridad y ciberdefensa a nivel nacional como internacional, pero las entidades privadas y los mismos actores de la sociedad

involucrados en el área de la informática, deben garantizar una seguridad digital para ellos mismos, y los demás usuarios.

En el CONPES 3701, anteriormente mencionado, se hace mucho énfasis en maximizar los beneficios a nivel económico y social a los ciudadanos, lo cual es sustancial tanto para el Estado como para los ciudadanos, no obstante, deja de lado a los ataques cibernéticos, *"los cuales aumentaron un 28% durante el 2017"* (Revista semana, 2017), generando más inseguridad cibernética a los ciudadanos, poniendo en peligro su integridad física y emocional, y afectando considerablemente la economía del país.

Para mencionar algunas de las lagunas jurídicas en la legislación colombiana respecto a temas informáticos, se encuentra la ley 527 del año 1999, la cual en su artículo 28, habla sobre los atributos jurídicos de una firma digital; esto jurídica y fácticamente es posible, pero se considera que esto genera una posibilidad de falsificación de huella, suplantación de identidad, la suplantación de correos corporativos, y demás delitos, y así facilitando aún más las conductas inescrupulosas de los delincuentes, y poniendo en riesgo la seguridad de ciudadanos y usuarios de redes informáticas.

Además, no se tiene certeza alguna que demuestre que la persona a través de estos medios digitales, esté realizando el acto consciente y/o voluntariamente.

Pero, si el derecho debe avanzar junto a la tecnología, ¿de qué manera se podrían disminuir estos delitos informáticos?, y ¿de qué forma se pueden esclarecer los hechos de determinados casos que involucren las TIC si aún no han sido incorporadas en el sistema jurídico?

En contextos como lo es Colombia, donde ya se ha regulado el comportamiento y se han establecido parámetros de uso para las herramientas digitales, como se refleja en los CONPES y en el código penal, es más complejo llevar a cabo el tema de estas faltas morales en el uso de las herramientas digitales, ya que para nuestro ordenamiento jurídico no son solo faltas morales, estas acciones están consideradas como delitos; pero entonces si las persona no acatan lo estipulado en la ley y cometiera estos delitos, ¿qué pasaría con ellos? Sencillamente se les aplicaría una sanción en caso de ser necesario; aun así, se seguirán cometiendo delitos que afectan el orden público y por ende a todos los ciudadanos.

Ante esto se atiende que una clara solución para esto es la regulación de las mismas plataformas digitales, pues como se afirma en el trabajo de la abogada Lucia Camacho: Más allá de los casos, debemos pensar en cómo evitar abusos y proteger derechos en redes sociales. La autorregulación -de las plataformas y de las personas- no parece ser suficiente. Por eso, se discute cómo regular a plataformas, redes sociales o buscadores (Gómez, 2019)

Actualmente es trascendental conocer al respecto del tema que se viene tocando, cómo funciona en casos recientes y controversiales; por ejemplo, en el caso concreto Santrich en el cual los magistrados se pronunciaron para ofrecer la garantía de no extradición por las pocas pruebas que llegaron a sus manos, Néstor Humberto Martínez comentó al respecto, y dio a entender que existía una "copiosa prueba que da cuenta de estos delitos de narcotráfico, evidencia electrónica, pruebas documentales, videos" (Martínez, 2018).

Las únicas pruebas con las que contó la sección de revisión para determinar el supuesto delito fueron 12 audios de interceptación de comunicaciones que se recaudaron en indagaciones aventajadas por la fiscalía en contra de Marlon Marín familiar de Iván Márquez, que trabaja como agente encubierto en Estados Unidos, en donde reside el material probatorio del cual se habla. En esos audios se mencionan aparentes actividades ilícitas de Santrich.

En la sentencia que se profirió del caso dice "las intercepciones telefónicas no corresponden al descargue original que se realiza de manera directa del sistema de intervención, sino al copiado que realizó algún funcionario en un medio magnético determinado (USB)" (Corte Suprema de Justicia , 2019) ¿De algún modo se transgrede el límite constitucional e internacional del derecho a la intimidad que estipula que nadie podrá ser objeto de interferencias arbitrarias en su esfera interna al momento de exponerlos? ¿Cómo se corrobora si esta información, dada la trascendencia del caso, no fue alterada o editada para inculpar al ex guerrillero?

Expertos como los peritos informáticos forenses son competentes y manejan temas relacionados con la informática y sus debidos subtemas. Además de ser conocedores de normas, que regulan sus actividades y ciertas conductas que permite su experiencia y control en su área de trabajo. También de contar con "títulos oficiales" que refuercen su imagen cómo profesionales en el tema.

Finalmente, conforme avanza la tecnología y las ciencias, y se van actualizando las leyes en base a lo que se ve hoy en día, en este caso, el mundo moderno infestado de aparatos electrónicos inteligentes con la capacidad de infinidades de funciones, los jueces revelan su ignorancia en el

tema, a lo que aparecen muchos interrogantes por parte de éstos. Es por esto, que intervienen en el proceso judicial personas expertas en las áreas de tecnologías los cuales facilitan y responden a llamados de auxilio por parte de los jueces.

III. PRUEBA DIGITAL.

Equiparando las temáticas y antecedentes tratados a lo largo del artículo, se evidencia en la investigación la necesidad de abordar el fenómeno, se manifiesta que en el ámbito social genera incredulidad respecto a la veracidad de este tipo de pruebas informáticas, se ha expresado la facilidad de irrumpir en la seguridad de documentos, actos o derivados que se creen en medios tecnológicos por los diversos progresos de los mismos permitiendo que estas variaciones delictivas. Agregando a ello, el malestar de la inseguridad que se genera en razón a la posibilidad de una manipulación de información personal que involucre al ciudadano en delitos penales, civiles, demás legislaciones posibles, de la misma manera que se involucran indecisiones que desequilibran el ámbito jurídico en los desarrollos procesales.

Las pruebas digitales son en su esencia toda clase de información almacenada por medios electrónicos sin que podamos confundir esta definición con los “archivos” producidos por el hombre. Su diferencia se enfoca en que los archivos son de dominio de esta persona; son de su autoría, por ende, las pruebas digitales son toda clase de información que arrojan los medios electrónicos como huellas de ciertas acciones que demuestren su inocencia o culpabilidad frente al caso que se esté llevando. A continuación, algunos ejemplos de pruebas digitales: base de datos, página web, aplicaciones descargadas (Ronderos, 2015).

Adicionalmente, Stephen Mason dijo en una compilación de trabajos sobre Evidencia Electrónica Internacional:

> Por no tener un conocimiento, siquiera mínimo del tema, los abogados y especialistas en evidencia digital responsables por investigar casos y de decidir si es necesario adelantar investigaciones penales contra un individuo, están en riesgo de cometer errores graves. Es por esta razón que jueces, abogados y académicos deben considerar que es de vital importancia que comiencen a entender qué es evidencia digital (p. 70).

Con respecto a la definición de prueba digital, es conveniente dejar en claro su diferencia con evidencia informática, debido que existen muchas confusiones en razón a estos dos significados que parecen ser en su teoría muy parecidos.

En la doctrina, surgen otras conceptualizaciones sobre la evidencia digital, tales como:

> La evidencia digital o la prueba electrónica es cualquier medio probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio. Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o el original es requerido (Informática forense Colombia, 2017).

Sin embargo, como se puede observar, se confunden y utilizan la definición de prueba y evidencia como si fueran lo mismo, lo cual un perito informático llamado Javier Rubio Alamillo señala lo contrario.

Este experto aclara la diferencia significativa detrás de éstas dos palabras. Conviene distinguir que la evidencia digital o informática es a priori de la prueba digital, debido a que ésta no ha pasado por el proceso de identificación, adquisición, preservación y análisis antes de ser determinada como prueba.

> Una evidencia informática puede ser un disco duro, una memoria USB, un DVD, un CD-ROM, una página de Internet, una conversación mantenida a través de una red social o un teléfono móvil, un comentario en el muro de Facebook, etc. Todos estos elementos, en caso de que pudieran ser utilizados en un juicio, serían evidencias informáticas y no pruebas. Una vez estas evidencias han pasado por un proceso de identificación, adquisición, preservación y análisis, se podrán convertir en pruebas. (Alamillo, 2018).

También, se debe de tener en cuenta el cuidado que se le da a las evidencias digitales, debido a que su información es frágil y de manipulable acceso. Tanto como la persona interesada y el perito debe encargarse de darle en su mayor interés, vigilancia y custodia a las evidencias para no provocar que éstas puedan desaparecer o que un tercero tenga acceso a la manipulación de éstas.

> El NIST (National Institute of Standards and Technology) (Timothy Grance, 2006) la define como la aplicación de la ciencia a la identificación, recopilación, examen y análisis

> de datos, al tiempo que se preserva la integridad de la información y se mantiene una estricta cadena de custodia de los datos. (Arévalo, 2018)

Al llegar aquí, después de presentar las distintas definiciones, se puede presenciar que a veces algunas páginas de internet tienen errores de acuerdo a la información suministrada, aspecto que provoca confusión, convenciendo a muchas personas de información errónea y mal presentada. Por ende, es importante conocer las publicaciones de expertos, para aplicar y proceder correctamente con respecto al tema de interés solicitado.

La evidencia digital se rige alrededor de tres principios básicos: Relevancia, se asemeja a los elementos que son concernientes a la situación que se analiza o investiga, con el fin de probar algo planteado alrededor de los hechos. Suficiencia, las evidencias acumuladas y analizadas son las requeridas para soportar hallazgos y constatar afirmaciones efectuadas sobre la investigación. Por último, la confiabilidad en cuanto ratifica repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital. (Semprini, 2017)

En relación a lo anterior, su reconocimiento jurídico debe estar fundamentado en la veracidad de la información que otorga la prueba al caso, pues los medios electrónicos pueden ser quebrantados con mucha facilidad y esto entorpece la búsqueda de la justicia. Cuando en una investigación se procura inspeccionar en medios informáticos o interceptar comunicaciones, es susceptible de transgredir derechos fundamentales como los presentes en los artículos 15 sobre la intimidad personal, y el artículo 21 sobre la honra, de la Constitución Política de Colombia.

No obstante, el material electrónico no cuenta con amplio repertorio jurídico, sin embargo se pueden evidenciar fundamentos jurisprudenciales como la sentencia C 334 del 2010, que habla fundamentalmente de los documentos electrónicos en cuanto su búsqueda puede vulnerar el manejo de tratamiento de datos personales, habeas data, pero que si se modifican afectan a los principios de su inalterabilidad y autenticidad.

En pleno siglo XXI, manipular los medios electrónicos es bastante sencillo, pues hasta una persona del común, sin ser experto en materia informática se puede impedir que se acceda a su información personal, almacenada en sus dispositivos, o dado el caso, hasta manipular esta misma.

Manipular los medios electrónicos no implica mayor dificultad, debido la misma sociedad exige el progreso laboral y personal de las personas; un avance en temas jurídicos relacionado a lo

informático, son los mensajes de WhatsApp, que podrían ser fuente de prueba documental, pericial, testimonial, e incluso en interrogatorio de parte, pero es importante aclarar que estos presentan ciertas vulnerabilidades, pues hasta una persona del común, sin ser un perito informático puede impedir que se acceda a su información personal, almacenada en su instrumento tecnológico, o dado el caso, la alteración de la misma.

Reconociendo que en razón a lo anterior se apoyan argumentos respecto a cuándo se trata el acceso al mundo de la informática, trayendo a colación lo dicho por Tim Berners-Lee, "resulta imprescindible hacer que la web esté disponible para todo el mundo, no obstante, también se sabe que, aunque la web ha creado oportunidades, también se ha convertido en un escenario para nuevos delitos." (Europa Press, 2019)

Por otra parte, como se mencionó anteriormente, y como se evidencia, para nadie es un secreto que esta revolución tecnológica es un fenómeno muy nuevo, que avanza a gran velocidad, pues como lo plasmó Tim Berners-Lee, el 12 de marzo de 2019 a los 30 años de la creación de la Web es importante reflexionar en lo que se ha convertido; ya sea en una plaza pública, una biblioteca, un consultorio médico, una tienda, una escuela, un estudio de diseño, una oficina, un cine, un banco, y mucho más […] (Europa Press, 2019)

Esto evidencia que las relaciones interpersonales y jurídicas de las personas están migrando a un espacio cibernético, y por esto se encuentran grandes vacíos y/o lagunas legales, y por ello si se considera que, aunque se encuentren peritos en la materia, y el Estado interviene activamente para que no sean violadas las políticas de seguridad de algunas compañías informáticas, y de los mismos ciudadanos; se deben establecer parámetros, y normas que regulen estas relaciones que efectivamente, en algunos casos afectan el orden público.

Para nadie es un secreto que la revolución tecnológica es un fenómeno muy nuevo, que avanza a gran velocidad, ,y por esto se encuentran grandes vacíos y/o lagunas legales, y por ellos se considera que aunque se encuentren peritos en la materia, el Estado tendría que intervenir para que no sean violadas las políticas de seguridad de algunas compañías informáticas, y de los mismos ciudadanos; como se refleja en el CONPES 3854, se deben establecer parámetros, y normas que regulen estas relaciones que efectivamente, en algunos casos afecta el orden público.

Hay una subclasificación que se debe tener en cuenta en cuánto a términos diferenciadores sobre la evidencia digital, ya que es un tipo de evidencia física que pueden ser almacenadas y analizadas con herramientas y técnicas especiales.

Ahora bien, el documento electrónico se entiende como una representación conveniente apta de reproducir una cierta manifestación de la voluntad, materializada a través de las tecnologías de la información, que se expresan a través de mensajes digitalizados que requieren de máquinas para poder ser distinguidas. Finalmente, mensaje de datos se refiere a la "información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros. El intercambio electrónico de datos, internet, correo electrónico, telegrama, telefax, etcétera" (Ley 527, 1999, art. 2).

Continuamente las leyes 904 de 2004 en su artículo 236 contiene avances ya que menciona a los expertos en el área forense digital, como se describe a continuación:

> Cuando el fiscal tenga motivos jurídicos para inferir que el sujeto procesal está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la recuperación de dicha información, para que expertos en informática forense custodien la información que recuperen (Ley 906, 2004, art. 236).

Lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso. También lo hace la ley 527 al establecer el criterio para valorar probatoriamente un mensaje de datos:

> Para la valoración de la fuerza probatoria de los mensajes de datos se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. (Ley 527, 1999, art. 11).

Uno de los puntos más importantes a tener en cuenta los expertos y encargados de investigar es, que además de ser competentes en su área de manejo, de igual forma deben tener conocimiento en el ámbito jurídico para evitar vulneraciones a derechos constitucionales que podrían, posteriormente, ser una excusa utilizada para el rechazo del resultado de la investigación

y se tache como pruebas ilícitas. Sin embargo, con base a lo anterior, es de suma importancia plantear la siguiente cuestión: ¿hasta qué instancia es permitido investigar a una persona y limitar su privacidad, sin que se vulneren sus derechos constitucionales? Se menciona un ejemplo, donde: X trabaja en una empresa en donde se venden objetos usados; todas estas ventas son realizadas online, en computadoras y demás equipos electrónicos que es en donde están todos los registros de las compras allí realizadas.

También, todos los ingresos son recibidos a un programa manejado por todos los empleados de la empresa, por ende, el total de los ingresos por las compras entran a una misma cuenta. X decide hackear la cuenta y se roba todos los ingresos de ventas realizados en 4 meses, que son aproximadamente 20.000.000 de pesos. Surgen muchas preguntas. ¿No es justo investigar a fondo a X sin importar vulnerar los derechos constitucionales debido a que él vulnera los derechos de demás personas e hizo algo ilícito? ¿Qué sería lo justo para el juez? ¿Si se decide que no se puede investigar a x y con esa información se pudieron haber obtenido pruebas que demuestren su culpabilidad, sería premiar al culpable y afectar a la víctima? ¿Se necesitará una reforma en donde sea más estricta la ley y se pudiese violar su privacidad con tal de condenar al culpable?

Es aquí donde nuestro sistema jurídico, y los jueces deben evaluar la eficacia y la veracidad de estas pruebas informáticas, ya que, sin estos acervos probatorios en cada proceso, no se podrá demostrar nada, sin estas pruebas cibernéticas no habrá cabida en determinar si en efecto si transgredió los derechos fundamentales de las partes involucradas, en relación a esto, aún no existe ninguna herramienta jurídica que facilite a los jueces la decisión en estos casos, donde todavía las normas o el contenido jurídico al respecto es muy limitado.

Es por ello que se asignan responsabilidades derivadas a expertos por sus criterios, caso concreto, el perito tiene múltiples funciones, entre éstas está la de investigar los hechos y el de posterior a tener éstos, su análisis como tal. Estos hechos son los que serán presentados como fácticos y reales en la demanda, por esto, después de que el perito indague y tenga los resultados de su investigación, debe asegurar su autenticidad para que sean una pieza clave como prueba de su demanda.

Por el contrario, si la información estuviese en sitios web, páginas públicas, computadoras sin ningún tipo de clave, o cualquier otra herramienta electrónica que sirva para acceder a

información que sirva como base para la investigación, no se requerirá ningún tipo de permiso de parte del juez, debido que ésta se considera pública lo cual hace más fácil la investigación. Pero, hay que tener en cuenta, que si la información está en archivos de un tercero, si se es esencial una autorización judicial sin importar que éste no sea el principal autor del crimen, se protegerán también sus derechos constitucionales.

El artículo 250 de la Constitución Política consagra como regla general que la afectación de derechos y garantías constitucionales para la obtención de elementos materiales probatorios u otro tipo de información debe ser autorizada previamente por el juez de control de garantías. El Fiscal deberá entonces solicitar de manera expresa y específica la autorización judicial previa. El empleo del término "afectación" supone, según su grado, una "limitación" o "restricción" al ejercicio o goce de un derecho fundamental. Dicha limitación o restricción (i) debe estar prevista en una ley (principio de reserva legal) y requiere, además, (II) de la intervención judicial (principio de reserva judicial), para determinar si resulta irrazonable o desproporcionada". (La prueba en el proceso penal)

CONCLUSIONES

Es verídico afirmar el hecho de que en la actualidad, con los avances tecnológicos existentes, todo medio tecnológico puede ser modificado o alterado. Por esto, se crea la necesidad de adecuar estrategias las cuales permitan la efectividad probatoria en el marco jurídico, ya que para su validez tendrá que cumplir con la autenticidad de la misma. Por ende, la cadena de custodia se muestra indispensable ya que limita y prevé la intervención de la prueba y así evitar alteraciones a las evidencias que anteponen y mal direccionan el proceso bajo el cual se necesitan.

Además, se muestra relevante igualmente la creación de nuevos medios para implementar de manera más adecuada las herramientas de materiales probatorios dentro de los procesos jurisdiccionales de acuerdo a la época actual.

La evidencia digital goza de ciertos principios los cuales limitan su definición. Aquellos son: la relevancia que califica los hechos sujetos a tener en cuenta como evidencia, y analiza su importancia dentro del proceso. La suficiencia recoge las evidencias planteadas y analiza su peso probatorio. Y por último la confiabilidad en cuanto a la repetibilidad y auditabilidad sobre la cuál fue obtenida la prueba.

REFERENCIAS

Alamillo, J. R. (16 de agosto de 2018). *Perito informático.* https://peritoinformaticocolegiado.es/blog/diferencias-entre-evidencia-informatica-y-prueba-informatica/

Arévalo, P. A. (2 de Junio de 2018). *Revista Economía y Política.* Revista Economía y Política: https://www.redalyc.org/journal/5711/571167817003/html/

Bernal, J. F. (24 de Julio de 2000). *Código Penal Colombiano.* http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20160208_02.pdf

Carrero, S. P. (2021). El documento electrónico y el entorno digital; una nueva realidad en materia probatoria. https://repository.usta.edu.co/bitstream/handle/11634/34576/2021soniacarrero.pdf?sequence=1

Constitución Política de Colombia [Cons.] (1991) Artículo 20 [título II]. 41 Ed. Legis.

Congreso de Colombia. (24 de julio de 2018) [Ley 1928 de 2018]. DO: 50.664. El 19 de mayo de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html.

Congreso de Colombia. (1 de septiembre de 2004). Artículo 236 [Capítulo III]. Código de Procedimiento Penal. [Ley 906 de 2004]. DO: 45.658.

Corte Constitucional, Sala Segunda de Revisión, T- 6.457.214. (26 de junio de 2018) Sentencia T-243-18. [MP Diana Fajardo Rivera]. https://www.corteconstitucional.gov.co/relatoria/2018/t-243-18.htm

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

Corte Constitucional de Colombia, Sala Plena. (02 de noviembre de 2016). Sentencia C-604/16. MP, Luis Ernesto Vargas Silva. https://www.corteconstitucional.gov.co/relatoria/2016/C-604-16.htm

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

Corte Constitucional de Colombia, Sala plena. (24 de septiembre del 2020). Sentencia C-420/20. MP, Richard S. Ramirez Grisales. https://www.corteconstitucional.gov.co/relatoria/2020/C-420-20.htm#:~:text=C%2D420%2D20%20Corte%20Constitucional%20de%20Colombia&text=La%20emergencia%20econ%C3%B3mica%20causada%20por,Colombia%20y%20en%20el%20mundo.

Corte Constitucional de Colombia, Sala Plena. (22 de mayo de 2019). Sentencia C-224/2019. MP, Cristina Pardo Schlesinger. https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm

Cortés, J. A. (2021). ICDP: https://icdp.org.co/corte-constitucional-aclaro-que-los-pantallazos-impresos-de-whatsapp-tienen-el-valor-de-prueba-indiciaria/

Corte Suprema de Justicia, 55395 (Sala de Casación Penal 29 de Mayo de 2019).

Departamento Nacional de Planeación. (14 de julio de 2011 [CONPES 3701]. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

Europa Press. (2019). La World Wide Web cumple 30 años y su creador reclama lograr que sea un espacio libre y abierto. *Europa Press*, 1.

El Tiempo, 23 de septiembre de 1999, 12:00am). Congreso de Colombia. (24 de julio de 2018) [Ley 1928 de 2018]. DO: 50.664. El 19 de mayo de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html.

Estos son los tres ciberdelitos de mayor impacto en Colombia en 2021. (26 de Diciembre de 2021). *EL ESPECTADOR. https://www.elespectador.com/colombia/mas-regiones/estos-son-los-tres-ciberdelitos-de-mayor-impacto-en-colombia-en-2021/*

Fernández, J. (22 de marzo de 2018). La prueba tecnológica en la era digital. [Archivo de Video]. https://www.youtube.com/watch?v=IR6ATRSCsN4

García, M. I. (2021). Delitos Informáticos: una perspectiva jurisprudencial y legal en Colombia. Proyecto de investigación. https://www.researchgate.net/publication/356069850_Delitos_informaticos_una_perspectiva_jurisprudencial_y_legal_en_Colombia_1

Gómez, J. G. (01 de marzo de 2019). *Legis Ámbito Jurídico*. https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/libertad-de-expresion-en-redes-sociales-es.

Gómez, H. J. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos informáticos? *Banca & Economía*, 11.

Gómez, D. S. (20 de abril del 2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial Colombiano. Ratio Juris. https://www.redalyc.org/journal/5857/585764837011/html/

Guarnizo, M. P. (2020). LA NATURALEZA JURÌDICA DE LOS DELITOS INFORMÀTICOS EN COLOMBIA.

https://repository.unad.edu.co/bitstream/handle/10596/41392/mpguarnizop.pdf?sequence=1&isAllowed=y

Guzmán, A. (8 de abril de 2020). Procesalistas estudian el valor probatorio de los “pantallazos” de WhatsApp. Ámbito Jurídico. (Video); https://www.ambitojuridico.com/noticias/general/procesal-y-disciplinario/procesalistas-estudian-el-valor-probatorio-de-los

Guzmán, A. (17 de julio del 2017). La prueba electrónica. Entrevista. Agencia Nacional de Defensa Jurídica del Estado. (Video); https://www.youtube.com/watch?v=8IebLRPkCU4

Hernández, I. (2019). Unos 20 millones de colombianos no tienen acceso a Internet. *RCN radio*, 1.

Informática Forense Colombia. (12 de marzo de 2017). https://www.informaticaforense.com.co/la-evidencia-digital/

Ley 1273 de 2009. 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”. 05 de Enero del 2009.

Ley 2213 del 2022. Por medio de la cual se establece la vigencia permanente del decreto legislativo 806 de 2020 y 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 y se dictan otras disposiciones. 13 de Junio del 2022. D.O.No. 52.064

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y el 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. 21 de agosto de 1999. D.O. No. 43.673.

Limón, J. Prueba Electrónica y Digital en los procesos judiciales. Video. https://www.youtube.com/watch?v=neMKat2Y-cI

Lorduy, J. (2022). Más de 29.000 ciberdelitos se han denunciado en 2022. Portafolio. https://www.portafolio.co/economia/finanzas/mas-de-29-000-ciberdelitos-se-han-denunciado-en-2022-568103

Lozada, A. (2019, septiembre). [Entrevista con Ángela Lozada, ingeniera de sistemas y abogada. Miembro de un laboratorio forense digital

Martínez, N. H. (2018). JEP solicitó a la fiscalía audios y videos del proceso contra 'Santrich'. *Asuntos: legales,* 1. https://www.asuntoslegales.com.co/actualidad/jep-solicito-a-la-fiscalia-audios-y-videos-del-proceso-contra-santrich-2772352

Ministerio de Tecnologías de la Información y las Comunicaciones. (2 de junio de 2016). *https://www.mintic.gov.co/*. El 19 de mayo de 2019, de https://www.mintic.gov.co/portal/604/w3-article-15410.html.

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. https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Ministerio de Justicia y del Derecho, (2022). Es un hecho la permanencia de las tecnologías de la información y las comunicaciones en las actuaciones judiciales. https://www.minjusticia.gov.co/Sala-de-prensa/Paginas/Es-un-hecho-permanencia-de-las-tecnologias-informacion-comunicaciones-en-actuaciones-judiciales.aspx

Moreno, O. M. (2022 de Febrero de 2022). DOCUMENTOS ELECTRÓNICOS COLOMBIA 2022. (D. Castro, Entrevistador)

Ochoa, C. A., Bermúdez, L. C., & Martínez, O. C. (2020). LA PRUEBA ELECTRÓNICA Y DIGITAL. Aclaración de las diferencias jurídicas en Colombia. *Institución Universitaria Politécnico Grancolombiano*, 38.

Ortiz, G. (2019). Ponencia: *Redes sociales: límites y libertades*. Presidenta de la Corte Constitucional. Corte Constitucional. Llevada a cabo en Medellín, Colombia.

Orozco, O. D. (s.f.). DOCUMENTOS CONPES. *REVISTA JURÌDICA.* REVISTA JURÌDICA. https://colaboracion.dnp.gov.co/CDT/Normatividad/Revista%20OAJ/Primera%20edici%C3%B3n/Concepto%20unificado%20-%20CONPES.pdf

Principios Fundamentales de la Prueba Digital. (13 de julio del 23021). IEJ CAMPUS VIRTUAL. (Video); https://www.youtube.com/watch?v=DGrPXHhv2wk

Revista Semana. (28 de diciembre de 2017). *https://www.semana.com/*. https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

Revista Dinero. (2019). El cibercrimen es un delito más rentable que el narcotráfico. *Dinero*, 1. Gómez, J. G. (01 de marzo de 2019). *Legis ámbito jurídico*. https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/libertad-de-expresion-en-redes-sociales-es.

Rodrigo, L. B. (2020). Evidencia Digital Aspectos Generales. Rama Judicial, Consejo Superior de la Judicatura. https://escuelajudicial.ramajudicial.gov.co/sites/default/files/11_cartilla_evidencia_digital_-_aspectosgenerales.pdf

Ronderos, J. G. (11 de Noviembre de 2015). https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf

Rojas, J. H. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. LOGOS CIENCIA & TECNOLOGÌA. https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/339/pdf_1

Semprini, G. (s.f.). *El Análisis integral de la evidencia digital.* SID, Simposio Argentino de Informática y Derecho.

Toro, N. (2019). *Los mensajes de datos y la prueba electrónica*. Bogotá, Colombia: Leyer.

Yepes, M. M., Pérez, J. A., & Peinado, M. (2021). APLICACIÓN DE LA PRUEBA ELECTRÓNICA EN EL MARCO NORMATIVO COLOMBIANO. *Institución Universitaria Politécnico Grancolombiano*, 277.