FACULTAD DE DERECHO

UNIVERSIDAD DE LEÓN

CURSO 2019/2020

LA PRUEBA DIGITAL ANTE LOS TRIBUNALES. UNA VISIÓN JURÍDICO-TÉCNICA DESDE EL DERECHO COMPARADO ESPAÑOL Y COLOMBIANO.

THE DIGITAL EVIDENCE IN THE COURTS. A LEGAL-TECHNICAL VISION FROM THE SPANISH AND COLOMBIAN COMPARATIVE LAW.

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR/A: D. JUAN DAVID CARDONA PÉREZ

TUTOR/A: DÑA. EVA ISABEL SANJURJO RÍOS

DEDICATORIA

Dedico este trabajo a mi esposa, Erica Alexandra, ejemplo de lealtad, paciencia, amor y fortaleza. A mi hijo, Juan José, fuente de inspiración en cada proyecto que he decidido emprender. A mis padres y hermanos ejemplo de vida y unión familiar.

LISTA DE ABREVIATURAS

BD : Big Data

CGP : Código General del Proceso (colombiano) ley 1564/2012.

CPP : Código de procedimiento penal (colombiano) ley 906/2004.

IA : Inteligencia Artificial

IOT : Internet Of Things (Internet de las cosas)

ISO : International Estandar Organization (Organización Internacional de estándares)

LEC : Ley 1/2000, de 7 de enero, de enjuiciamiento Civil

LECRIM : Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal

ML : Machine Learning

OSINT : Open Source Intelligence (Inteligencia de Medios Abiertos)

SAP: Sentencia Audiencia Provincial

STC: Sentencia tribunal Constitucional

STS : Sentencia Tribunal Supremo

TFM : Trabajo Fin de Máster

TIC´s: Tecnologías de la información y las Comunicaciones.

UE : Unión Europea

INDICE

Pág.

RESUMEN

Este trabajo es una herramienta jurídica que facilita el tratamiento objetivo de la prueba o evidencia digital en un proceso judicial. Nace de la necesidad de una interpretación rigurosa de este tipo de información luego de analizar algunas falencias en el manejo dado a este material por parte del operador jurídico, producto de carencias en formación técnica en sistemas y de comprensión de los pormenores e intríngulis de la prueba o evidencia digital.

También brinda los elementos necesarios para la comprensión y afianzamiento de los conceptos para una valoración probatoria acorde con esta nueva clase de pruebas o evidencias, que, desde hace un tiempo atrás, aparecen como pieza fundamental en muchas de las investigaciones y procesos judiciales de la actualidad. Este trabajo responde a las necesidades judiciales del avance tecnológico, la llegada de internet, la IA, la BD, el ML, el IOT y la próxima computación cuántica, haciendo imperativo que nuestros fiscales, jueces, abogados, investigadores, peritos y demás que hacen parte de este nuevo mundo ciber jurídico se formen, entiendan y comprendan los elementos esenciales de la prueba o evidencia digital desde la Investigación Informática.

ABSTRACT

This work is a legal tool that facilitates the objective treatment of evidence or digital evidence in a judicial process. It arises from the need for a rigorous interpretation of this type of information after analyzing some shortcomings in the handling given to this material by the judicial operator, the product of deficiencies in technical training in systems and understanding of the details and intrengulis of the Digital Evidence or Evidence.

It also provides the necessary elements for understanding and entrenching concepts for an evidentiary assessment in line with this new kind of evidence, which, for some time, have been a fundamental part of many of today's investigations and judicial processes. This work responds to the judicial needs of technological advancement, the advent of the Internet, AI, BD, ML, IOT and the next quantum computing, making it imperative that our prosecutors, judges, lawyers, researchers, experts and others who are part of this new cyber legal world form, understand and understand the essential elements of digital evidence or evidence from computer research.

PALABRAS CLAVE

Prueba digital, evidencia digital, documento electrónico, firma electrónica, firma digital, valor probatorio.

KEYWORDS

Digital proof, digital evidence, electronic document, electronic signature, digital signature, probative value.

OBJETO DEL TRABAJO

El presente trabajo TFM aborda las dificultades técnicas y jurídicas en la interpretación de las normativas sobre la prueba o evidencia digital que se da por parte de los operadores de justicia en el desarrollo de los procesos judiciales. Estas dificultades se basan en el uso de herramientas jurídicas como la analogía y las equivalencias funcionales retrospectivas para resolver un problema que requiere de un conocimiento especializado y actualizado, así como un tratamiento diferenciado. Es aquí donde la prueba o evidencia digital sufre alteraciones integrales al ser interpretada como una prueba documental, comprometiendo no solo su contenido sino su grado de veracidad, rigurosidad y posibilidad de uso.

Para ello se realizó un estudio técnico-jurídico que combina dos marcos de análisis (el derecho y la informática) para el eficaz tratamiento y la correcta valoración de la prueba o evidencia digital, el cual contribuirá significativamente en la solución de los yerros interpretativos por parte de los operadores de justicia al momento de la apreciación y valoración de este tipo de prueba. Es por ello que **el problema** presente del TFM se basa en poder demostrar que el concepto de prueba o evidencia digital, su tratamiento, interpretación y valoración, se han venido realizando, en mi opinión, de manera errónea respecto a las fuentes jurídicas vigentes sobre el tema, respecto aquellas pruebas o evidencias digitales diferentes al documento electrónico.

La **delimitación del problema** se enmarca en la normativa española y colombiana respecto al tratamiento, interpretación y valoración de la prueba o evidencia digital, no obstante, dadas las condiciones actuales de un mundo virtualmente globalizado sin fronteras, las pretensiones de este trabajo son *erga omnes* ya que los problemas observados no son exclusivos de estos dos países. Servirá de guía para que el problema planteado sea operable y se valore de una forma más objetiva y actualizada cada prueba o evidencia digital, tal como se demostrará a lo largo del TFM.

Puntualmente como **objetivo general** se plantea aportar elementos técnicos y jurídicos suficientes a los operadores de justicia para realizar una correcta interpretación y valoración de la prueba o evidencia digital en los procesos judiciales. Para lograrlo se partirá resolviendo cuatro **objetivos específicos** a saber:

- Primero: Establecer la diferencia entre el documento electrónico, como medio de prueba documental y la prueba o evidencia digital.
- Segundo: Delimitar los conceptos de prueba o evidencia digital como medio y como fuente probatoria, logrando establecer las diferencias.
- Tercero: Conocer los requisitos legales mediante el estudio de derecho comparado entre España y Colombia para la admisibilidad y la valoración probatoria de la prueba o evidencia digital.
- Cuarto: Proponer el marco interpretativo de los conceptos jurídicos tratados para la valoración objetiva y actualizada de la prueba o evidencia digital dentro de los procesos judiciales.

Este trabajo busca beneficiar directamente a los operadores de justicia entregando argumentos y herramientas técnico-jurídicas, sobre las cuales los operadores de justicia podrán hacer un uso completo y correcto de la razón y la sana crítica, fortaleciendo su lógica y su conocimiento técnico-científico para una adecuada interpretación y valoración de esta.

Una vez aprendidas y comprendidas las vicisitudes e intríngulis propias de este nuevo medio de prueba estarán asimiladas las competencias necesarias para impartir justicia dentro de un campo virtual hasta ahora desconocido para muchos. De allí la **importancia o interés** acerca del desarrollo del presente tema, además el TFM servirá de refuerzo a la Facultad de Derecho, de la Universidad de León para apoyarse en el análisis y estudio del tema, así como de documento de consulta para los estudiantes de las diferentes facultades de derecho Europeas y Latinoamericanas. También permitirá a las Cortes o tribunales comprender de una forma más acertada los contenidos y contradicciones que conlleva la valoración de la prueba o evidencia digital.

La llegada de este nuevo campo virtual al que se hace referencia supone el romper paradigmas jurídicos, partiendo de la dogmática y los principios que rigen cada Área del Derecho. Lo anterior nos ubica frente a una temática de **actualidad,** en desarrollo, con términos y campos desconocidos para muchos dentro del mundo jurídico como el BD, el

ML, la computación cuántica, la IA, las redes neuronales artificiales, el IOT, entre otras cuestiones que se encuentran en constante cambio propio del avance tecnológico y que suponen grandes retos para el derecho y en especial para el derecho procesal.

DESCRIPCIÓN DEL MÉTODO Y LA METODOLOGÍA UTILIZADA.

El problema parte de una premisa general observada al revisar las carencias normativas sobre la prueba o evidencia digital. Por ende, se usó el método hipotético deductivo para la observación de cada uno de los elementos a tratar, su caracterización y relación con el problema planteado dentro del marco legislativo de España y Colombia. Se parte de la proposición de un fenómeno de interés (para este caso las falencias en la interpretación de la normativa sobre la prueba o evidencia digital) para observar si sus particularidades son coherentes con la naturaleza del problema (la falta de actualización de las leyes y el desconocimiento de conceptos informáticos).

Una vez realizado este paso, se planteó una hipótesis referente con la manera en cómo se relacionan los factores a tratar, en este caso, los tipos de prueba y evidencia digital con los diferentes códigos, leyes, decretos y demás material legislativo que abordan el tema.

Es así como parte de las piezas usadas para el planteamiento de la hipótesis en mención, fueron las halladas en las leyes españolas LECRIM, LEC y la Ley 59/2003, de 19 de diciembre, de firma electrónica. Al tiempo que las leyes colombianas 1564/2012 CGP, la ley 906/2004 CPP y 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. Además de las directivas y reglamentos UE, como por ejemplo la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica, el Reglamento UE 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Decreto 2364 de 2012, entre otras.

Esta hipótesis fue respondida por medio de la comprobación de cada uno de los yerros interpretativos mostrados a lo largo de este trabajo, logrando coherencia entre la proposición del problema y sus posibles causas. El derecho comparado brindó las herramientas necesarias para poder enlazar los conceptos e ideas.

Gracias a este camino investigativo es posible sustentar que se debe seguir una guía hermenéutica legislativa que permita encausar correctamente el material probatorio de naturaleza digital. Es más, la investigación no se queda en la demostración de la existencia de una falencia en la interpretación legal, además propone los parámetros de comprensión para cada uno de los elementos relacionados con el tratamiento de la prueba o evidencia digital.

TITULO I. DELIMITACIÓN CONCEPTUAL DE LA PRUEBA O EVIDENCIA DIGITAL DESDE LAS VERTIENTES JURÍDICA Y TÉCNICA.

Capítulo I. El documento electrónico como medio de prueba o evidencia digital.

Al hablar de prueba electrónica refiriéndonos al documento electrónico necesariamente debemos traer a colación el término prueba o evidencia digital, desde algunos autores que las tratan como sinónimos y otros que encuentran algunas diferencias. En el presente capítulo se intentará aclarar la cuestión, sin embargo, para llegar a ese punto se deben estudiar estos dos conceptos por separado.

La prueba electrónica recoge las pruebas documentales análogas (documentos físicos como contratos, títulos valores entre otros) mediante la utilización de un sistema electrónico, para lo cual algunos Estados, entre otros el español y el colombiano, han optado por regular el uso de los mensajes de datos, las firmas digitales y los documentos electrónicos, tratando estos como prueba electrónica, así lo recoge la ley 527/1999 en Colombia.[1] Y la Ley 59/2003, en España.

De igual manera LLOPIS BENLLOCH, encuentra algunas diferencias entre estos conceptos así:

"Al hablar de prueba electrónica, en mi opinión hablamos de dos conceptos diferenciados, que suelen entremezclarse. Por una parte, la aportación de documentos públicos electrónicos como prueba en juicio y por otra parte la constatación de hechos digitales"[2]

LLOPIS BENLLOCH hace referencia como prueba electrónica a todos aquellos documentos públicos o privados que hayan sido trasmitidos por medio de un sistema electrónico y no así la prueba o evidencia digital la cual debe ser corroborada por un perito informático, a contrario sensu de la prueba documental electrónica, que, por tratarse de un documento análogo que se convierte en digital y que lleva una firma electrónica, debe ser valorado como un simple documento. Este tema tendrá un desarrollo más profundo cuando

[1] Ley 527/1999 de 18 de agosto de 1999. (Diario Oficial No. 43.673/ 21 agosto /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.

[2] LLOPIS BENLLOCH, José Carmelo, *Prueba electrónica y notariado*, en: OLIVA LEÓN, Ricardo y VALERO BARCELÓ, Sonsoles, *La prueba electrónica validez y eficacia procesal*, Madrid, 2016, pág. 20.

a lo largo del mismo se desarrolle la equivalencia funcional del documento electrónico y en general, de la prueba o evidencia física, respecto a la prueba o evidencia digital.

En comparación, CANO MARTÍNEZ afirma que la "prueba electrónica es cualquier información obtenida a partir de un dispositivo o medio digital y que sirve para adquirir convencimiento de la certeza de un hecho"[3]

Está última definición se aparta un poco más del concepto exclusivo al que se refiere LLOPIS BENLLOCH y se acerca al concepto final de prueba o evidencia digital, puesto que abre las posibilidades no sólo a los documentos, sino que une estos con los hechos digitales, entendiendo como hecho digital cualquier acontecimiento que produce un resultado digital verificable (datos, imágenes, logs de auditoría, entre otros).

Teniendo como precepto estas definiciones, definiremos a continuación las clases de documentos y las clases de firmas que hacen parte del ambiente electrónico o virtual.

Es decir, aquellos que han pasado de lo análogo a lo digital adquiriendo características que, si bien son similares a la de los documentos y firmas análogas, no son iguales, y su tratamiento con fines probatorios debe ser diferente.

1.1 Clases de documentos en el entorno digital y virtual.

Para iniciar tomaremos como base la definición de documento, que acuña, CÁRDENAS RINCÓN respecto a lo que él manifiesta, considera CARNELUTTI y ECHANDÍA.

" El doctrinante nacional Devis Echandía considera que Documento es: toda cosa que sirve de prueba histórica indirecta y representativa de un hecho cualquiera". Y por su parte el tratadista internacional Carnelutti considera que "el documento no es sólo una cosa, sino una cosa representativa, o que sea capaz de representar un hecho"[4]

Ambas definiciones muy exactas respecto al documento análogo (papel), pero si se habla de documento electrónico las cosas cambian, teniendo como base las particularidades que hacen que un documento, que bien pudiese ser físico, sea legible en un medio

[3] CANO MARTÍNEZ, Jeimy José. *El peritaje informático y la evidencia digital en Colombia conceptos, retos y propuestas*. Uniandes, Bogotá, 2010, pág 100.
[4] CÁRDENAS RINCÓN, Erick. *Derecho del comercio electrónico y de internet.* Legis, Bogotá, 2017, pág 70.

electrónico. Y cambian aún más si a lo que se hace referencia es a un documento que por naturaleza ha sido creado digitalmente.

Por último y antes de abordar estos conceptos es de resaltar que las clases de documentos que se presentan a continuación pueden ser catalogados como públicos o privados dependiendo de quién lo emita[5], al igual que los documentos físicos.

1.1.1 Documento electrónico

El Reglamento de la UE 910/2014 del Parlamento Europeo y del Consejo, nos presenta en su artículo 3.35 una definición concisa de documento electrónico, pero que sirve para aclarar el concepto de lo que algunos llaman prueba electrónica diferenciándola de la digital. Esta postura será uno de los pilares de esta argumentación ya que manifiesta que deben abordarse como una sola, (la digital) de ahí el título del presente escrito.

En tal sentido, el Parlamento de la UE cita: "documento electrónico, todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual."[6] Otra definición al respecto la trae RINCÓN CÁRDENAS, quien aduce que "el documento electrónico se caracteriza por ser representativo de hechos o actos generados por seres humanos y no por contener cualquier tipo o parte de información"[7].

Por su parte la ley 527/1999 en Colombia, no se refiere en sentido estricto al documento electrónico, y adopta el término mensaje de datos en medios digitales. Y así lo trae su artículo segundo: "Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada 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"[8]

Tomando como base estas definiciones podemos concluir que el documento electrónico hace referencia a cualquier tipo de información que represente un

[5] Entidades o funcionarios públicos o personas naturales o jurídicas sin calidad de funcionario.
[6] Artículo 3.35, Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
[7] CÁRDENAS RINCÓN, Erick. *Derecho del comercio electrónico y de internet...* op.cit., pág 78.
[8] Artículo 2, Ley 527/1999 de 18 de agosto de 1999. (Diario Oficial No. 43.673/ 21 agosto /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.

acontecimiento producto de un hecho o un acto electrónico, entendiendo acto electrónico el realizado en un equipo electrónico por un ser humano, y que el mismo se encuentre en un soporte electrónico. Sin embargo, es imperativo establecer si existe una diferencia entre el mensaje de datos y el documento electrónico. Es en este sentido donde la ley colombiana se queda corta en su definición al hacer referencia únicamente al mensaje de datos, sin tener en cuenta que este puede ser automatizado mediante un "bot message"[9]. A diferencia del documento electrónico, este debe ser producido y consentido por un ser humano, consentimiento que se convalida mediante su firma electrónica. Sin embargo, ambos estarían dentro de la categoría de la prueba o evidencia digital y no así de la prueba electrónica, toda vez que están formados por unos y ceros, es decir, las dos tienen componentes binarios que son objeto de recolección y análisis.

Según lo que sostiene la normativa y algún sector doctrinal, como ejemplos de documentos electrónicos tenemos: los correos electrónicos, los documentos producidos por cualquier paquete ofimático, también aquellos documentos que en su inicio fueron análogos (físicos, en papel) y que luego de ser escaneados cuentan con firma electrónica que permitan la identificación del remitente y que en todo caso contienen información atribuible a un ser humano. Estas últimas si son objeto de valoración probatoria, para que sea considerado documento electrónico, deberá ser conocido el autor de estas.

1.1.2 Documento digital

Aclarado el concepto de documento electrónico, corresponde ahora definir el concepto, documento digital, lo cual se hace menos complejo si se tiene en cuenta que cualquier documento catalogado como electrónico una vez almacenado se convierte en digital. Suena contradictorio, pero así es como sucede, tal como se mencionó en el documento electrónico, que al ser almacenado en un medio físico o sistema virtual[10] adopta las características del documento digital, es decir ceros y unos.

Lo anterior se puede concluir de las diferentes definiciones que hacen alusión al documento digital. Por ejemplo, CÁRDENAS RINCÓN lo define como: "Cualquier tipo de información sin importar su naturaleza que llegue a representar un hecho, acto o idea y que

[9] Mensaje predeterminado por un usuario en una maquina con el fin de generar respuestas automatizadas, datos, palabras, audios o cualquier fragmento de estos que haga parte de una información.
[10] Definiciones que encontraremos en el capítulo III numerales 3.2.1 y 3.2.2.

se encuentre almacenada ya no en cualquier medio electrónico, sino que, en este caso, su soporte deberá ser soportado en medios digitales, es decir, en bits, unos y ceros, lenguaje que es solo inteligible para las computadoras y no para los humanos"[11]

Esta última definición incorpora un componente esencial al momento de su definición cuando la misma presenta …"bits, unos y ceros", toda vez que es uno de los dos presupuestos que requiere el documento para ser catalogado como digital. El otro estará dado en términos probatorios, dado que el documento, además de ser digital, debe venir firmado electrónica y digitalmente, conceptos que se desarrollaran en el punto "clases de firmas".

1.2 Clases de firmas.

Una vez estudiadas las clases de documentos, es necesario conocer el concepto de las firmas que pueden contener cada uno de estos, puesto que son estas las que finalmente terminan por darle validez a lo plasmado en el documento o al documento en sí dentro de procesos probatorios.

1.2.1 Firma electrónica y firma electrónica certificada.

La definición se aborda utilizando un lenguaje coloquial con el fin de hacerlo lo más claro posible y entendible, sin dejar de lado la parte técnica que es necesaria, para ello, se toma como base la siguiente definición que trae la Directiva y el Reglamento europeo sobre firmas electrónicas.

"los datos de forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación"[12] luego el nuevo Reglamento de la UE 910/2014, la define como: "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar"[13]

[11] CÁRDENAS RINCÓN, Erick. *Derecho del comercio electrónico y de internet…* op.cit., pág 79.
[12] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica.
[13] Reglamento UE 910/2014 del parlamento europeo y del consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Es de aclarar que en España desde el año 2003 ya existía una norma relativa a la firma electrónica a raíz de la publicación de la Ley 59/2003, que aún se encuentra vigente y que en su artículo 3.4 versa "La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante"[14].

Por otra parte, el artículo 1.3 del decreto 2364 de 2012 en la normatividad colombiana trae la siguiente definición.

"Firma electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente."[15]

Vemos como las tres definiciones, el Reglamento de la UE, la ley española y el decreto normativo en Colombia, hacen referencia a dos palabras "confiabilidad" y "autenticación" siendo estas la clave de la firma electrónica. Cualquiera que sea el método electrónico utilizado para la firma, estas dos características son las que se deben tener en cuenta al momento de su valoración en los juzgados y tribunales.

1.2.2 Firma digital.

Como se mencionó en la anterior definición de firma electrónica, la firma digital es la que permite dar seguridad tanto al contenido del documento electrónico o digital como la certeza de que quien firma electrónicamente es sin lugar a duda quien dice ser. Esta firma está basada en algoritmos criptográficos[16] que permiten cifrar el contenido de un documento, al tiempo que hacen irrefutable la firma electrónica.

HOCSMAN entregó una definición de firma digital en cita a RAMOS SUÁREZ quien consideró que " una firma digital, es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es el autor (autenticación) y que no ha existido

[14] Ley 59/2003, de 19 de diciembre, de firma electrónica.
[15] Decreto 2364 de 2012, sobre la firma electrónica, Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
[16] Sucesión de pasos lógicos mediante un lenguaje de programación determinado por quien lo elabore, con el fin de encriptar un dato o conjunto de datos, entregando confidencialidad y seguridad.

ninguna manipulación posterior de los datos (integridad), para firmar un documento digital, su autor realiza su propia clave secreta (sistema criptográfico asimétrico), a lo que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio… por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor"[17] .

Capítulo II. Análisis jurídico del concepto de prueba o evidencia digital.

2.1 Hacia la búsqueda de su concepto a la luz de la normativa colombiana y española.

En el presente escrito pueden observar que en repetidas ocasiones se hace relación a dos términos que en principio parecieran excluyentes "prueba digital" o "evidencia digital", seguramente para muchos, el término es el mismo y su significado es igual. Sin embargo, como se ha evidenciado en estas primeras líneas, se busca que el contenido del presente trabajo pueda resultar útil en múltiples legislaciones. Es así como llegamos a identificar por qué se toman estas dos acepciones.

Si hacemos relación a los procesos judiciales en diferentes latitudes del orbe, nos damos cuenta de que, en gran parte de Latino América y centro América se le conoce como evidencia o elemento material probatorio a las cosas recolectadas dentro de las etapas de indagación e investigación, estas últimas haciendo relación al proceso penal, las cuales posteriormente, se convertirán en prueba en la etapa de juicio oral, tal como lo señala la rama judicial de Colombia en la sección de información de su portal web acotando.

"En el nuevo esquema acusatorio se distingue dos etapas, una investigativa y otra de juicio. En la primera, el órgano persecutor tiene la obligación de ordenar todos aquellos actos que tiendan a establecer principalmente la ocurrencia del delito y la individualización de sus responsables, entre los que encontramos allanamientos, registros, interceptaciones telefónicas, búsqueda selectiva en base de datos, entre otros. En la actividad investigativa se recogen informaciones, entrevistas, evidencias o materiales probatorios que eventualmente podrán ser utilizados en la siguiente etapa del proceso"[18].

[17] HOCSMAN, Heriberto Simón. *Negocios en Internet*. Astrea, Buenos Aires - Bogotá, 2013, pág. 357.
[18] Disponible en la url: https://www.ramajudicial.gov.co/web/noticias-paloquemao/informacion, recuperado el 25 de marzo de 2020, rama judicial república de Colombia.

Algo similar pasa dentro de los procesos del derecho privado, donde las evidencias pueden ser aportadas con la demanda, con la reforma de la demanda, con los términos para correr la demanda, para luego en la audiencia inicial el juez decretar las pruebas y en la audiencia de instrucción y juzgamiento, practicarlas, valorarlas y dictar sentencia. Así lo estipula, por ejemplo, el CGP, en sus artículos "392 al unisonó con los artículos 372 y 373"[19].

Sin embargo, es de aclarar que, dentro de la categoría de evidencias o elementos materiales probatorios, las "evidencias digitales" o "pruebas digitales" no se encuentran reguladas formalmente en el ámbito penal y es por ello por lo que se debe hacer uso del artículo 25 del CPP ley 906/2004[20] el cual remite al código de procedimiento civil, el mismo que en consonancia con el artículo 10 de la ley 527 de 18 de agosto de 1999. (Diario Oficial No. 43.673/ 21 agosto /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[21], introdujo los documentos digitales como pruebas documentales. También el artículo 247 del CGP ley

[19] Ley 1564 del 12 de julio de 2012, Artículo 392. Trámite. En firme el auto admisorio de la demanda y vencido el término de traslado de la demanda, el juez en una sola audiencia practicará las actividades previstas en los artículos 372 y 373 de este código, en lo pertinente. En el mismo auto en el que el juez cite a la audiencia decretará las pruebas pedidas por las partes y las que de oficio considere. No podrán decretarse más de dos testimonios por cada hecho, ni las partes podrán formular más de diez (10) preguntas a su contraparte en los interrogatorios. Para la exhibición de los documentos que se solicite el juez librará oficio ordenando que le sean enviados en copia. Para establecer los hechos que puedan ser objeto de inspección judicial que deba realizarse fuera del juzgado, las partes deberán presentar dictamen pericial. En este proceso son inadmisibles la reforma de la demanda, la acumulación de procesos, los incidentes, el trámite de terminación del amparo de pobreza y la suspensión de proceso por causa diferente al común acuerdo. El amparo de pobreza y la recusación solo podrán proponerse antes de que venza el término para contestar la demanda, Artículo 372: Audiencia inicial, Artículo 373:Audiencia de instrucción y juzgamiento.

[20] Ley 906 de 31 de agosto de 2004 "Por la cual se expide el Código de Procedimiento Penal", Artículo 25. Integración: En materias que no estén expresamente reguladas en este código o demás disposiciones complementarias, son aplicables las del Código de Procedimiento Civil y las de otros ordenamientos procesales cuando no se opongan a la naturaleza del procedimiento penal.

[21] Ley 527 de 18 de agosto de 1999. Diario Oficial No. 43.673/ 21 agosto /1999, op.cit, Artículo 10. admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

1564 del 12 de julio de 2012 el cual derogo el código de procedimiento civil colombiano[22] hace referencia a la valoración de los mensajes de datos.

No obstante, lo descrito por estas normas, ninguna de ellas aborda la evidencia digital o la prueba digital en *stricto sensu* de lo que se entiende por estos términos, es así como nos encontramos con distintas definiciones que han acuñado el termino evidencia digital. Así por ejemplo el instructivo para el hallazgo, identificación, embalaje de la evidencia de tipo digital de la Fiscalía General de la Nación Colombia, define evidencia digital[23], al tiempo que CISTOLDI y NUÑES, tecnifican un poco más el concepto aduciendo:

"la evidencia digital es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales. A modo de ejemplo, se mencionan algunos elementos que pueden convertirse en evidencia digital: Un archivo en un medio de almacenamiento, una línea de texto en un log de transacciones, el registro de acceso a un sitio web, datos en el registro de auditoría de una aplicación, datos de una ocurrencia en los registros de eventos del sistema"[24.]

Quizás la definición más completa y transparente para cualquier lector, bien sea jurídico o técnico, la acuña CANO MARTINEZ .

"Cualquier registro generado por, o almacenado en un sistema computacional, que puede ser utilizado como evidencia en un proceso legal."[25]

---

[22] Ley 1564 del 12 de julio de 2012, Artículo 247. Valoración de mensajes de datos. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.

[23] "EVIDENCIA DIGITAL: También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados, sino simplemente almacenados por o en un computador o medios equivalentes y registros o archivos híbridos que incluyen, tanto registros generados por computador o medio equivalente, como almacenados en los mismos", tomado del Instructivo para el hallazgo, identificación, embalaje de la evidencia de tipo digital, adoptado mediante resolución 0-5017 del 20 de octubre de 2009, publicado en el Diario oficial No 47.510 de 22 de octubre de 2009, por medio del cual se actualizan los documentos del proceso penal, como parte del subproceso de policía judicial y se adopta un documento dentro del mismo subproceso relacionados con la actividad investigativa de la sección de investigaciones y apoyo a unidades nacionales.

[24] CISTOLDI, Pablo Adrián y NUÑES, Luciano*, Introducción a la Informática Forense, Criminalística e Investigación Penal*, en: DI LORIO, Ana Haydée, *El rastro digital del delito Aspectos técnicos, legales y estratégicos de la Informática Forense* , Universidad FASTA, Mar del Plata, 2017, pág. 79-80.

[25] CANO MARTINEZ, Jeimy José. *Computación forense. Descubriendo los rastros informáticos*. Alfaomega Colombiana, Bogotá, 2015, pág. 202.

Una vez abordada la definición de evidencia digital, no queda más que conocer, el concepto de prueba digital, tal como se reconoce en las jurisdicciones del derecho español, para lo cual iniciaremos acotando que, para efectos en este país europeo, así como en diferentes Estados de la UE se utilizan los términos prueba digital y prueba electrónica indistintamente, es decir son sinónimas. En este sentido DELGADO MARTÍN define la prueba digital como "Toda información de valor probatorio contenida en un medio electrónico o trasmitido por dicho medio"[26]

A la par BUENO DE MATA haciendo referencia a la decisión del programa marco AGIS de la Dirección General de Justicia de la Comisión Europea, sobre cooperación judicial y policial en materia penal, presenta la prueba electrónica como: " La información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho"[27]

Se observa entonces como en todas y cada una de las definiciones tanto de evidencia como de prueba digital, se hace referencia al medio electrónico, mezclando este concepto con el concepto de formato digital, por cuanto se hace necesario acotar la definición de medio electrónico, que trae en sus anexos la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

"Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras"[28]

La anterior definición deja claro que una cosa es el medio de almacenamiento o transmisión y otra muy diferente lo que se almacena o transmite.

No obstante, las definiciones de diferentes autores, el concepto de prueba digital o electrónica en el marco de la UE no es diferente al de Latino América, puesto que no existe una definición normativa directa y explícita; sin embargo, en todos los países hay normas

[26] DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones,* Wolters kluwer España, Madrid, 2016, pág. 42.
[27] BUENO DE MATA, Federico, *Prueba electrónica y proceso 2.0*, Tirantlo blanch, Valencia, 2014, pág. 98.
[28] Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

que contienen preceptos que, de alguna manera hacen referencia a la prueba electrónica, tal y como lo refiere BUENO DE MATA en su obra prueba electrónica y proceso 2.0[29].

Así pues, la normativa española reconoce analógicamente la prueba digital o electrónica en la LEC, donde a partir de lo normado en el artículo 299.2 y 299.3[30] en concordancia con los artículos 383 y 384 de la misma Ley[31] se busca ampliar los medios de prueba análogos, permitiendo hablar de prueba digital, aunque el término no aparezca en strictu sensu. Por ello se hace uso de estos artículos, como lo que coloquialmente en el ámbito jurídico se conoce como cajón de sastre[32].en especial del artículo 299.3, referenciado anteriormente.

Ahora bien, Luego de presentar los diferentes conceptos de evidencia digital y prueba digital o electrónica y conocer como son abordados en el Estado colombiano y el Estado español, queda claro que el significado para ambos términos es el mismo. Sin embargo, al contrastarlos con el concepto de medio electrónico, se observa que los autores tienden a usarlos como sinónimos.

---

[29] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*… op.cit., pag 95 y 96.

[30] Ley 1/2000 del 7 de enero, Ley de enjuiciamiento civil española, Articulo 299 Medios de prueba, numeral 2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso. Numeral 3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.

[31] Ley 1/2000 del 7 de enero, Ley de enjuiciamiento civil española. Artículo 383. Acta de la reproducción y custodia de los correspondientes materiales. 1. De los actos que se realicen en aplicación del artículo anterior se levantará la oportuna acta, donde se consignará cuanto sea necesario para la identificación de las filmaciones, grabaciones y reproducciones llevadas a cabo, así como, en su caso, las justificaciones y dictámenes aportados o las pruebas practicadas. 2. El material que contenga la palabra, la imagen o el sonido reproducidos habrá de conservarse por el Letrado de la Administración de Justicia, con referencia a los autos del juicio, de modo que no sufra alteraciones.

Artículo 384. De los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso. 1. Los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que, por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga. 2. Será de aplicación a los instrumentos previstos en el apartado anterior lo dispuesto en el apartado 2 del artículo 382. La documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Letrado de la Administración de Justicia, que, en su caso, adoptará también las medidas de custodia que resulten necesarias. 3. El tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza.

[32] Aquellas normas que permiten ampliar la interpretación jurídica e implementar o ingresar términos o cosas que no se encuentran tipificadas en estricto sentido.

Una vez aclarado estos preceptos y tomando como base los postulados anteriormente descritos, se presenta por parte del autor una definición final, para conceptualizar la prueba o evidencia digital como: "todo dato o información que se encuentra alojado en un medio de almacenamiento físico o virtual, en formato digital, producto de la escritura, copia, o trasmisión de esos datos o información, a través de un dispositivo electrónico, incluyendo los que en su origen, antes de su almacenamiento o transmisión, fueron análogos."

2.2 Características de la prueba o evidencia digital.

Aclarados los conceptos de prueba electrónica y prueba o evidencia digital, pasemos a abordar las tres características de mayor relevancia que permitirán diferenciar la prueba o evidencia digital con las demás fuentes de prueba.

2.2.1 Volatilidad.

La volatilidad es quizás la particularidad de mayor relevancia en la prueba digital, tal como nos lo presenta DELGADO MARTÍN, "la prueba electrónica ostenta frecuentemente la característica de la volatilidad, es decir, la información o datos relevantes son mudables y sometidos a constante cambio, especialmente en relación con los contenidos de internet"[33].

Se conoce como información volátil aquella que es almacenada en la memoria RAM (memoria de acceso temporal) por sus siglas en inglés, la cual guarda la información y los datos mientras el equipo electrónico se encuentre encendido, y una vez apagado, esta se pierde, por ello es de suma importancia, al momento de conocer y valorar el procedimiento realizado por quien acopia la información, saber si se recolectaron o no.

Este tipo de datos son casi siempre de relevancia para el proceso, puesto que, en caso de no haberse recolectado constituiría una falta a los protocolos de recolección de la prueba digital y a las guías de buenas prácticas que hacen referencia a la misma, obviando información que puede resultar relevante en un momento determinado para un proceso, cualquiera fuere su ámbito.

Así lo define la guía INFOLAB del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense de la universidad FASTA de la Plata/Argentina:

[33] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones…* op.cit., pág 76.

"Adquisición de datos volátiles. Se trata de la obtención de datos existentes en dispositivos encendidos que pueden perderse definitivamente al ser apagado el artefacto".[34] Y así es ratificado por ALBERDI Y RUIZ DE ANGELI refiriéndose al análisis forense informático "El análisis forense informático debe tener en cuenta el nivel de volatilidad de los datos que se pueden convertir en información relevante a partir de la evidencia digital"[35].

De igual manera pasa con el contenido virtual alojado en las páginas web, en blogs o en redes sociales; en el momento la información puede estar presente, pero en instantes puede ser alterada, modificada o eliminada por las características complementarias y propias de la prueba digital y que se abordaran a continuación.

2.2.2 Eliminabilidad.

La prueba o evidencia digital, al igual que los elementos físicos de prueba son eliminables, pueden desaparecer mediante hechos causados o hechos fortuitos, sin embargo, cuando se hace referencia a lo digital, esa posibilidad de pérdida del elemento probatorio se amplifica, en el sentido que basta con un solo click o la simple obturación de una tecla, para que la información desaparezca, aunque en estos casos con una gran diferencia frente a los elementos físicos. En la gran mayoría de casos esta información o esos datos se pueden recuperar mediante una intervención forense.

Es ahí donde toma relevancia esta característica, aunada a la cualidad de que la evidencia o prueba digital sea recuperable (es decir la eliminabilidad en un sentido positivo). Tal como lo acota ANGUIANO JIMENEZ "los discos duros de los ordenadores no son tan fáciles de borrar como parece. Así, cuando se borra un fichero en un ordenador personal, en realidad no se borra del disco duro, sino que se marca para que las cabezas lectoras del ordenador no se dirijan a ese sector del disco. No obstante, los que quieren borrar de forma efectiva un disco duro siempre pueden optar por (i) llenarlo de información

[34] DILORIO, Ana Haidée. *Guía Integral de Empleo de la Informática Forense en el Proceso Penal*. Universidad FASTA, Mar del plata, 2016, pág11.
[35] ALBERDI, Juan Ignacio y RUIZ DE ANGELI, Gonzalo Matías, *Análisis Forense de Memoria Principal*, en: DI LORIO, Ana Haydée. *El rastro digital del delito Aspectos técnicos, legales y estratégicos de la Informática Forense*… op. cit., pág. 71.

re- escribiendo encima de lo que se quiere borrar (ii) formatear el disco duro con opciones disponibles en el propio sistema operativo del ordenador"[36]

Lo anterior ilustra el por qué puede llegar a ser recuperable la prueba o evidencia digital almacenada en un medio electrónico para su posterior valoración, al tiempo que lo que se valore allí sea la información y los datos digitales almacenados, mas no el elemento que los contiene, salvo que ese elemento sea la causa de la investigación o de la litis del caso. No se estaría hablando de una prueba digital y mucho menos electrónica, se trataría de un elemento material probatorio o evidencia física.

2.2.3 Alterabilidad y modificabilidad.

Respecto a estas dos características, es claro, tal y como se ha abordado líneas atrás que la manipulación de la evidencia digital es un gran reto no sólo para los peritos, sino para quienes posteriormente deben entender y valorar lo que ha sucedido con la misma en su proceso de recolección, brindado las garantías que se deben dar frente a su adquisición, puesto que las modificaciones de datos e información que se pueden realizar a un archivo, documento, log o cualquier otra fuente de prueba digital, están a la mano. Además de ser sencillo es casi que indetectable por quien tiene acceso a esta.

Por ello su tratamiento debe ser riguroso y se tiene que ceñir a los procedimientos planteados por las normativas internacionales para la recolección, tratamiento y análisis de la evidencia digital (a las cuales hace relación el capítulo II del título II).

Esto para garantizar la mismidad de la prueba, entendiendo que, no se hace comparable la modificación que lleva a la alterabilidad de un documento físico o un elemento material probatorio encontrado en la escena de un delito o que pruebe un hecho jurídico dentro de una litis (situaciones que serán perceptibles al ojo humano), con la modificación que conlleva a alterar una evidencia digital y que sólo se hace posible evidenciar con la utilización de herramientas forenses por parte de un perito informático. De lo contrario, bastaría la sola presentación del archivo, log o documento para tener la misma apariencia del original.

---

[36] ANGUIANO JIMENEZ, José María, *La prueba electrónica en la banca digital. El soporte duradero*, en: OLIVA LEÓN, Ricardo y VALERO BARCELÓ, Sonsoles, *La prueba electrónica validez y eficacia procesal*, Madrid, 2016, pág. 72-73.

Al respecto el Tribunal Supremo opina en la STS 300/2015 que la posibilidad de alteración o suplantación de una prueba o evidencia digital es bastante alta, dada la posibilidad que tiene el ser humano de manipular el contenido de la misma, al punto de fingir una identidad.[37]

Capítulo III. Particularidades y conceptos técnicos de la prueba o evidencia digital en un proceso judicial.

3.1 Los medios de almacenamiento de la prueba o evidencia digital.

En este apartado daremos a conocer los principales medios o dispositivos donde se puede generar o almacenar la prueba digital como fuente probatoria. Cabe recordar que cuando se habla de los medios de almacenamiento de la prueba o evidencia digital no equivale a hablar de los medios probatorios, sin embargo, estos medios de almacenamiento también pueden llegar a servir como medios de prueba dentro de un proceso judicial.

Tal es el caso del equipo de telefonía móvil que contiene un mensaje de WhatsApp, el cual se pretende incorporar al proceso para probar que se trata del mismo mensaje impreso mediante captura de pantalla o transcripción.

Sin ser este el medio más idóneo para la adquisición y preservación de la prueba o evidencia digital por falta de regulación acerca de la manera idónea o correcta de presentarse o incorporarse la prueba.

Este puede ser un ejemplo en el que el medio de almacenamiento de la prueba o evidencia digital puede ser empleado como medio probatorio, no obstante, el mismo debe ir acompañado de la solicitud de cotejo o interrogatorio de parte que verse sobre el contenido de la conversación[38].

Se hace necesario hacer referencia al concepto de medio de prueba con la finalidad de entender por qué se menciona el medio de almacenamiento de la evidencia digital como un medio probatorio.

---

[37] STS nº 300/2015 de 19 de mayo de 2015, F.J. 4º, (RJ 2015\1920) "La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo."

[38] DELGADO MARTÍN, Joaquín. *Investigación judicial y prueba digital en todas las jurisdicciones*…op.cit., pág. 53

En primera medida haremos referencia a la LEC en su artículo 299 y específicamente lo que hace referencia a lo descrito en su numeral segundo[39], al tiempo que al CGP en su artículo 165, mismo que hace referencia a los medios de prueba[40].

Es así como en un sentido amplio el concepto de medio de prueba se condensa en manifestar que es la forma como se incorporan al proceso las fuentes probatorias, con la finalidad que el juez pueda obtener información sobre los hechos objeto del proceso[41].

En el mismo sentido lo presenta ORTUÑO NAVALON al resaltar que "medio de prueba es un concepto procesal, referido a la actividad necesaria para introducir dicha realidad en el proceso"[42], concepto que refuerza el hecho que un medio de almacenamiento pueda o no, ser considerado un medio de prueba.

Esto dependiendo la relación o equivalencia que se otorgue respecto los medios convencionales, en este caso al intentar equipararle con el medio de prueba documental.

Así lo referencia la Sentencia 702/205, de la sección 27ª de la Audiencia Provincial de Madrid "La documental consistente en el Acta de cotejo por el Letrado de la Administración de Justicia de los mensajes del teléfono cuya transcripción ha sido aportada por la denunciante (Acta de fecha 6 de mayo de 2015 realizada ante el Letrado del Juzgado de lo Penal nº 3 de Getafe). La actuación del Letrado de la Administración de Justicia otorga fe pública sobre el contenido del teléfono móvil en el momento en el que se realiza el cotejo. Aunque dicha fe pública no se extiende a acreditar que los mensajes que obran en

[39]Ley 1/2000 del 7 de enero, Ley de enjuiciamiento civil española. Artículo 299. Medios de prueba. 1. Los medios de prueba de que se podrá hacer uso en juicio son: 1.º Interrogatorio de las partes. 2.º Documentos públicos. 3.º Documentos privados. 4.º Dictamen de peritos. 5.º Reconocimiento judicial. 6.º Interrogatorio de testigos. 2. También se admitirán conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso. 3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.

[40] Ley 1564 del 12 de julio de 2012 el cual derogo el código de procedimiento civil colombiano Artículo 165. Medios de prueba. Son medios de prueba la declaración de parte, la confesión, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios, los informes y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez. El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio, preservando los principios y garantías constitucionales.

[41] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones*…op.cit., pág. 44.

[42] ORTUÑO NAVALON, María del Carmen. *La prueba electrónica ante los tribunales,* tirant lo blanch, Valencia, 2014, pág. 34-35.

dicho dispositivo hayan sido remitidos por el número de teléfono concreto del acusado, ni que los mismos hayan sido recibidos por el teléfono de la denunciante; y tampoco se extiende a acreditar con fehaciencia que dicho contenido no ha sido objeto de manipulación anterior"[43].

No obstante que no se comparta la posición de la Audiencia, es evidente que tanto magistrados como algunos doctrinantes sostienen que la prueba digital es equivalente funcionalmente con la prueba documental, debate que si bien se tratará en este escrito no se hará en este momento.

Así las cosas, los principales medios de almacenamiento de la prueba o evidencia digital los podemos dividir en dos. Medios de almacenamientos físico con formato digital y los sistemas de almacenamiento virtual (o en la nube), los cuales finalmente se convertirán en medios de prueba documental, por su contenido y como se precisó anteriormente deberá ir acompañada de otros medios que precisen acerca de la fuente de prueba que allí se encuentra alojada. Veamos cada uno de ellos.

3.1.1 Medios de almacenamiento físico con formato digital.

En estos medios encontramos los sistemas de almacenamiento en dispositivos móviles, donde no se habla del equipo móvil o de telefonía celular como un todo al momento del almacenamiento de la información y los datos que finalmente son los que van a representar la fuente de prueba o evidencia digital, sino de su sistema de almacenamiento, representada por su **memoria flash**, definida por MANDADO PÉREZ y MANDADO RODRIGUEZ como "Memorias de almacenamiento de datos borrables eléctricamente en su totalidad o por bloques" [44].

La particularidad de estas memorias es que la información y los datos sí pueden ser eliminados en su totalidad tan sólo con el reinicio de fabrica del equipo, puesto que están configurados para liberar todos sus sectores de almacenamiento. No obstante, si los datos son borrados, esta información se puede llegar a recuperar. La dificultad está en que, dada su capacidad que es más reducida que la de los demás medios de almacenamiento actuales,

[43] SAP Madrid nº 702/2015 de 24 de noviembre de 2015, F.J. 2º, (ARP\2015\1313)
[44] MANDADO PÉREZ, Enrique y MANDADO RODRIGUEZ, Yago. *Sistemas Electrónicos Digitales, 9ª edición,* Marcombo, Barcelona, 2008, pág. 552.

es muy probable que en poco tiempo esa información o esos datos sean sobre escritos, perdiendo los mismos. Este tipo de almacenamiento es el mismo que usan los pen drive más conocido en el medio como USB.

Estas características son muy relevantes al momento de valorar la prueba digital u ordenar una intervención temprana por parte de los operadores de justicia.

Por otra parte, encontramos dentro de esta categoría de medios de almacenamiento físico, **los discos duros o HDD** por sus siglas en inglés (Hard Disk Drive), así lo define IBAÑEZ CARRAZCO Y GARCÍA TORREZ "dispositivo compuesto por una o varias láminas rígidas de forma circular, recubiertas de un material que posibilita la grabación magnética de datos"[45].

Normalmente este medio de almacenamiento se encuentra en los computadores de escritorios, portátiles, servidores, no obstante que sean empleados en otros dispositivos electrónicos como por ejemplo los **corta fuegos (firewall)** o los **sistemas de grabación digital de video (DVR)** o **consolas de video juego** (Xbox, Nintendo, entre otras) se caracterizan por su gran capacidad de almacenamiento y porque a diferencia de la memoria flash este requiere un tratamiento especial para la eliminación total de los datos y la información, por cuanto se hace más factible su recuperación, teniendo menor probabilidad de sobreescritura rápida.

En la actualidad han tomado fuerza, los **discos de estado sólido o comúnmente conocidos como SSD** (por sus siglas en inglés) como medio físico de almacenamiento. Estos medios son definidos por OLIVA HABA, MANJAVACAS ZARCO y MARTIN MÁRQUEZ como "dispositivo de almacenamiento de datos que usa memoria no volátil, como flash, o memoria volátil, como la SDRAM. Para almacenar datos, en lugar de los platos de los discos duros convencionales".[46]

Estos medios de almacenamientos cumplen la misma función que los discos duros convencionales, la de almacenar información y datos, sin embargo, su funcionamiento es

[45] IBAÑEZ CARRASCO, Patricia y GARCÍA TORRES, Gerardo. *Informática I con enfoque en competencias,* Cengage Learning, México D.F, 2009, pág. 19.
[46] OLIVA HABA, José ramón, MANJAVACAS ZARCO, Custodia y MARTIN MÁRQUEZ, Pedro Luis. *Montaje y mantenimiento de equipos, sistemas microinformáticos y redes,* ediciones parainfo, Madrid, 2014, pág. 137.

diferente, “La información se graba directamente en bloques de memoria en los semiconductores, y el controlador se encarga de localizarla directamente y entregarla al ordenador. Así, tanto la escritura como el acceso a la información son mucho más ágiles”[47].

La gran diferencia respecto a los demás medios de almacenamiento físico es que esta cuenta con dos tipos de memoria para almacenar:

Una volátil, que almacena los datos temporales para que la búsqueda de la información sea rápida; pero que al apagar o reiniciar el sistema la misma se pierde, y una memoria flash, que permite el almacenamiento de los datos y la información de manera permanente, haciendo posible que la misma sea recuperable, (el nivel de recuperación de la información dependerá en gran medida de su capacidad).

Es importante señalar que son estos mismos medios de almacenamiento los que en mayor medida son utilizados por los **entes de IA y robots autónomos** a los cuales nos referiremos en el siguiente apartado.

Estos son los medios utilizados en las cámaras digitales, en las grabadoras de audio digital, así como en dispositivos GPS[48], coches autónomos entre otros, aclarando que no es el único medio utilizado por estos dispositivos, pues también puede haber sistemas o dispositivos híbridos, que combinan memorias flash y SSD.

3.1.2 Sistemas de almacenamiento virtual (en la nube).

En la actualidad es común escuchar el término “la nube” o el “cloud”, cuando nos referimos a que la información se encuentra alojada en un lugar remoto donde se pueden buscar los datos o realizar consultas. Es decir, pasamos de almacenar la información contenida en documentos físicos que reposaban en libros u hojas almacenadas en anaqueles a la digitalización de la información.

Mucha información aún se guarda en medios físicos que luego pasa a almacenarse en sistemas o medios virtuales que comúnmente conocemos como la nube, pero ¿qué es lo virtual?, ¿qué es la nube?, SILVA nos presenta una definición diametral al concepto de realidad vs virtual, refiriéndose a lo virtual como “lo virtual está subordinado a lo real y

[47] Disponible en la url: http://noticias.gti.es/servidores-y-almacenamiento/que-es-un-disco-duro-ssd/ , recuperado el 29 de marzo de 2020, GTI software & networking.
[48] Global Position System o Sistema de Posicionamiento Global.

circunscrito a la esfera de la representación. Dicho de otra manera, las imágenes generadas por los ordenadores electrónicos suponen un horizonte fenoménico simulado, un acercamiento especioso a la realidad. Lo virtual pues se considera una copia forzosamente degradada, una "realidad divorciada del mundo", un simulacro, un doble de lo real, aunque descabalado, la virtualidad imita mal a lo real"[49].

La anterior definición nos abre un claro panorama para entender este sistema como aquella representación del medio de almacenamiento físico que se encuentra en algún lugar, instalado en un dispositivo electrónico (servidor), lugar y dispositivo que no podemos ver ni tocar, pero que, por la prolongación de esa realidad del medio físico, podemos llevar con nosotros a cualquier lugar, siempre y cuando tengamos el canal (internet) para acceder a esa copia de la realidad.

Tal y como es en la realidad, este sistema de almacenamiento ha puesto en aprietos no sólo a los operadores de justicia y en especial a los jueces y magistrados que son quienes finalmente deben valorar y tomar decisiones frente a lo que se presenta como prueba digital, sino a quienes deben recolectarla.

Pasaremos a analizar su complejidad probatoria, teniendo en cuenta que en estos sistemas de almacenamiento en la nube o virtual, la información y los datos que se hayan almacenados y a los cuales difícilmente se tendrá acceso, puesto que su ubicación física será un enigma, de alguna manera deberán ser recolectados y aportados al proceso. Por cuanto se hará necesaria la intervención de un tercero, que para los casos actuales corresponderá a la empresa prestadora del servicio del sistema de almacenamiento de dicha información.

Por ejemplo, Amazon con el sistema **AWS**[50], Google con el sistema **Google Drive**, Apple con su sistema **iCloud**, Microsoft con **OneDrive**, entre otras, que se convierten en los garantes de la información y los datos, convirtiendo el equipo informático o electrónico únicamente en el medio para acceder al sistema de almacenamiento, por cuanto se

[49] SILVA, Carlos, *Capas sin espesor: aproximación psicosocial a la cibercultura,* en: RANGEL, Ana Lisset y LADRÓN DE GUEVARA, Irene. *Voces digitales ida y vuelta a la cibercultura*, latina, Caracas, 2003, pág. 42.
[50] Amazon Web Services.

dispondrá de dos maneras legales para acceder a la recolección de la prueba o evidencia digital en estos casos.

La primera mediante una orden judicial que ordene a la empresa propietaria del sistema de almacenamiento en la nube, aportar determinada información como fuente de prueba aún sin el consentimiento del usuario contratante del servicio, situación que es inviable en algunos países. La segunda es que sea el propio usuario quien suministre las credenciales de acceso, lo que supone, si no se actúa con la suficiente cautela que, la recolección y posterior presentación de una prueba digital pueda carecer de legalidad y que además su autenticidad e integridad fácilmente pueda ser puesta en duda (temas sobre los que profundizaré en el Titulo II capitulo II del presente escrito con relación a la ubicuidad y la extraterritorialidad de la prueba digital, como principales talanqueras para la efectiva valoración de esta).

Dentro de estos sistemas de almacenamiento en la nube encontramos las páginas web y las redes sociales tales como **Facebook, Instagram, Twitter, Snapchat, linkedIn**, sólo por citar algunas. Todas ellas con las mismas características descritas anteriormente, con el agravante que en estas últimas la información subida es volátil, es decir en un momento determinado puede ser eliminada o modificada en cuestión de segundos. Lo que supone que, si no se cuenta con la recolección de esos datos o información garantizando la integridad y autenticidad en tiempo real o mientras dure el mensaje en el medio de almacenamiento virtual sin ser modificado o eliminado, difícilmente será recuperable.

Por otra parte, se tiene la mensajería instantánea o chats virtuales, como por ejemplo **WhatsApp, Wechat, Telegram, Imo**, entre otras, aplicaciones que cuentan con un sistema híbrido de almacenamiento, es decir, los mensajes que salen del equipo móvil o informático pueden quedar almacenados en el servidor virtual de la empresa prestadora del servicio, pero también quedan almacenados en el sistema de almacenamiento físico del dispositivo móvil. Esto hasta cuando se produzca alguno de los supuestos descritos en el apartado anterior donde se referenciaron los medios de almacenamiento físico, es decir hasta que sea eliminado en su totalidad del medio de almacenamiento.

Por último, se hace referencia **a los correos electrónicos**, los cuales a diferencia de las aplicaciones de mensajería instantánea disponen de un sistema de almacenamiento

virtualizado, proporcionado por el prestador de servicio del correo (**Gmail** de la empresa Google, **Outlook** de Microsoft, entre otros) y para la forma de recolección de la prueba o evidencia digital estará supeditada por los mismo dos supuestos citados para los sistemas convencionales de almacenamiento en nube como lo son, mediante orden judicial a la empresa o cedido por el usuario. Sin embargo, hay una excepción y es el caso de algunos correos corporativos de empresas que disponen de su propio medio de almacenamiento, en servidores propios y accesibles en cualquier momento de forma presencial. Allí la prueba digital correrá a cargo de la empresa.

El reto nuevamente para el Derecho Procesal y en especial para los operadores de justicia está en la interpretación y valoración que le den no sólo a la fuente de prueba sino al tratamiento que se le ha dado a la recolección de esta, donde se hace imperativo legislar frente a la unificación de la manera de recolectar la prueba o evidencia digital.

3.2 Lo que se extrae y se recupera como prueba o evidencia digital: la fuente de prueba digital.

Es tiempo de abordar lo que pueden contener esos medios de almacenamiento susceptibles de extracción o recuperación, con el fin de presentarse como fuente de prueba en el ámbito digital. Se partirá de la definición misma de fuente de prueba que nos presenta SENTIS MELENDO al afirmar que fuente de prueba es "un hecho cosa o fenómeno que sirve para verificar la verdad del hecho afirmado"[51]. En complemento, TESONE, FERRER y CAÑABATE asientan que "las fuentes de prueba son conceptos preexistentes al proceso: las partes, testigos, documentos, la cosa que ha ser examinada, el conocimiento técnico del perito"[52].

Tomando como base estos preceptos abordamos el concepto de la fuente de la prueba en el mundo digital para así comprender cuáles son aquellas fuentes de prueba digitales, que se tienden a confundir con los medios de prueba.

---

[51] SENTIS MELENDO, Santiago. *La prueba los grandes temas del derecho probatorio,* editorial EJEA, Buenos Aires, 1978, pág. 147

[52] TESONE, Rodolfo, FERRER, Jordi y CABAÑATE, Josep. "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en materia penal". *Economist & jurist.* 2012, pág web, disponible en la url: https://www.economistjurist.es/articulos-juridicos-destacados/la-obtencion-de-la-prueba-electronica-su-acceso-al-proceso-civil-y-la-garantia-de-derechos-en-materia-penal/ , recuperado el 13 de abril de 2020.

Un concepto que nos permite comprender el tema, es el presentado por BANACLOCHE PALAO, quien hace una distinción entre fuente y medio de prueba pero esta vez traslapándole al mundo digital, menciona "En el mundo digital, la fuente de la prueba radica en la información contenida o transmitida por medios electrónicos, mientras que el medio de prueba será la forma a través de la cual esa información entra en el proceso (Actividad probatoria)"[53], concepto que deja claro que la fuente probatoria como evidencia o prueba digital no es el medio de almacenamiento como ya se explicó, ni el dispositivo electrónico *per se*, sino la información y los datos que en el están contenida sin importar su formato o extensión[54].

Teniendo como base lo anteriormente dicho a continuación se describen las formas más comunes en las que podemos encontrar las fuentes de prueba dentro del ambiente digital.

3.2.1 Registros, datos o información generados por equipos electrónicos o de tecnología informática y almacenados en medios físicos y sistemas virtuales.

Para abordar este apartado, se hace necesario conocer la diferencia entre dato e información y así una vez entendido estos dos conceptos, pasar a evaluar cómo pueden formar parte de un proceso como fuentes de prueba.

FERNÁNDEZ ALARCÓN nos presenta la diferencia entre datos e información "los datos consisten en hechos y cifras que tiene de algún modo una existencia propia e independiente y que tiene poco significado para el usuario. Una de las características más significativas de los datos es que por ellos mismos no indican si son relevantes o irrelevantes"[55]

Se hace referencia a los siguientes ejemplos: hora, fecha, número de cédula, número de cuenta, un nombre, entre otros que, al verlos, no nos representan más que un hecho, pero si no se ubican dentro de un contexto determinado no podrán ser valorados en su unidad,

---

[53] BANACLOCHE PALAO, Julio. *La prueba en el proceso penal,* en: BANACLOCHE PALAO, Julio y ZARZALEJOS NIETO, Jesús, *aspectos fundamentales del derecho procesal penal segunda edición,* editorial La Ley, Madrid, 2011, pág. 273.

[54] Por ejemplo, .doc para documentos; .ppt para presentaciones en Power Point; .pdf para documentos en formato de lectura; .mp3 o mp4 para archivos de audio; .jpg para imágenes, entre muchos otros.

[55] FERNÁNDEZ ALARCÓN, Vicenc. *Desarrollo de sistemas de información, una metodología basada en el modelado,* Ediciones UPC, Barcelona, 2006, pág. 19.

puesto que por sí solos no proporcionan de ninguna forma juicios ni interpretaciones. Sin embargo, si esa hora o esa fecha se encuentran dentro de un registro de ingreso a un sistema y las mismas están vinculadas a un nombre o número de cédula e incluso a una huella dactilar este dato pasa de ser un dato irrelevante para entregarnos información de utilidad, la cual podrá ser interpretada, razonada y valorada. Es en este sentido que aparece el concepto de Información que el mismo FERNÁNDEZ ALARCÓN define como "conjunto de datos procesados con significado, y dotados de relevancia y propósito"[56].

De lo anterior se puede deducir que es la información la que ilustra los hechos, ya que es esta la que recoge los datos en conjunto, datos que al ser interpretados podrán valorarse como información que puede o no presentar relevancia o demostrar un hecho concreto dentro de un proceso.

Por último, aparecen los registros que bien debieron presentarse primero antes que el concepto de dato e información, pero que su definición se presenta de última toda vez que es precisamente el registro la génesis del dato y de la información.

Así lo trae VALHONDO quien al momento de explicar el concepto de datos hace referencia a los registros de estos "los datos pueden ser descritos como **registros** estructurados o transacciones"[57]. Es decir, son aquellos actos humanos o programados en un sistema informático o electrónico, que permiten que un dato sea almacenado, bien como unidad o bien como información.

Dentro de esta categoría, encontramos: los logs, la meta data, los algoritmos, los ficheros y archivos, veamos cada uno de ellos:

3.2.1.1 Logs.

Son todos aquellos registros almacenados en forma de datos y que al ser analizados en su totalidad entregan información que puede o no ser relevante. Este tipo de fuente probatoria es muy útil, toda vez que entrega indicios fuertes sobre la autoría de un hecho. Por ejemplo, un sistema que este diseñado para que su acceso se dé por medio de una huella (acceso biométrico) que estará asociada a un número de cédula o ID y que al tiempo

[56] Ibidem.
[57] VALHONDO, Domingo. *Gestión del conocimiento, del mito a la realidad,* ediciones Diaz de Santos, Madrid, 2010, pág. 48.

almacene la hora y la fecha del acceso a dicho sistema; esos datos analizados en conjunto pueden llevar a demostrar quién ingreso al sistema, más allá de lo que en el mismo se haya realizado, que será seguramente el hecho que se busca demostrar.

3.2.1.2 Meta data.

El concepto de meta data o metadatos, esta dado por la raíz griega *meta* que significa después de o más allá de y el termino latín *datum* que significa dato, si este significado lo llevamos al campo digital la meta data será entonces los datos que describen otros datos, tal como lo cita RILEY " La definición clásica es literal, basada en la etimología de la palabra misma: los metadatos son "datos sobre datos". Con esta definición amplia, uno podría esperar que los metadatos se puedan encontrar en todas partes, y de hecho lo es"[58].

Con base en lo anterior tenemos que, la meta data son todos aquellos datos que describe el elemento digital o virtual que contiene la información. Por ejemplo, un documento de Word trae como metadato, su autor, la hora de creación y de modificación, el nombre del equipo donde se realizó, entre otros datos.

3.2.1.3 Algoritmos.

En la actualidad es quizás la fuente de prueba más controvertida y la que mayor atención debe cobrar frente a los nuevos retos probatorios que trae consigo el derecho en comunión con la tecnología, especialmente la industria tecnológica.

Hemos oído acerca de los entes autónomos, robots dotados de IA, redes neuronales digitales o artificiales, entre otros términos que hace unos pocos años atrás parecieran sacados de una película de ciencia ficción, pero que hoy son una realidad. Es allí donde encontramos y encontraremos la fuente de prueba a la que nos referimos, fuente que, entre otras cosas, puede llegar a probar la responsabilidad civil de quienes desarrollan o utilizan estos equipos o entes frente a los daños que se deriven del equivocado funcionamiento de los mismos.

Comencemos por decir que un algoritmo es una secuencia lógica de pasos que nos lleva a un resultado, el mismo debe cumplir con unas características básicas que son: 1.

[58] RILEY, Jenn. *Understanding metadata what is metadata, and what is it for?,* National Information Standards Organization (NISO), Baltimore, 2017, pág. 1.

finitud, que tenga un inicio y un fin. 2. Definible: debe ser preciso sin ambigüedades. 3. Efectividad: que las acciones u operaciones para lo que fueron diseñados puedan ser ejecutadas en principio de forma exacta, que sea finito[59].

Teniendo como base esta definición se hará referencia al algoritmo informático, el cual puede llegar a presentarse como fuente de prueba. Este tipo de fuente probatoria la encontraremos en los robots autónomos que funcionan mediante la programación lógica, diseñada en principio por un humano.

De igual manera es el principio básico de la IA entendiendo esta como aquella que a partir de un algoritmo inicial sumado a la repetición o a otros datos que puedan almacenarse en su base de datos, puedan desarrollar nuevas funciones y hasta tomar decisiones diferentes para las que fueron programadas.

En la actualidad poca o ninguna referencia se tiene frente a la valoración de estos como fuente de prueba. Se hace necesario acotar que para la valoración de esta fuente probatoria inexorablemente se debe de contar con un experto en la materia, lo que constituye este tipo de prueba o evidencia digital dentro de la categoría de especial.

3.2.1.4 Ficheros y archivos.

Estos son los más comunes y conocidos dentro de los que ingresan en el listado de lo que se debe considerar prueba o evidencia digital. Hacemos referencia a las carpetas y los archivos que en ellas se contienen, también conocidos como ficheros, es decir todos aquellos archivos que contengan audio, texto, imágenes y en general datos e información; y que se encuentran almacenados con una extensión específica que es la que permite que mediante la interacción del ser humano con la máquina (Hardware) y esta a su vez con un programa (software) estos datos e información puedan ser captados por los sentidos.

Dentro de esta categoría encontramos los archivos del paquete ofimático como Word, Excel,[60], los de audio como por ejemplo aquellos con formato .mp3, .wav entre otros, o de video como por ejemplo archivos .mp4.

---

[59] KNUTH, Donald E. *El arte de programar ordenadores volumen 1, algoritmos fundamentales,* editorial Revreté S.A, Barcelona, 2002, pág. 5-6.

[60] DESONGLE CORRALES, Juan. *Ayudante técnico de informática de la junta de Andalucía volumen II, Editorial MAD, SL, Sevilla, 2005, pág. 155, define ofimática como "*El termino viene de la unión de

Al momento de hablar de prueba o evidencia digital, generalmente este tipo de fuentes son las más comunes junto al correo electrónico y los mensajes transmitidos por los equipos electrónicos o de tecnología informática y a las cuales se hace referencia a continuación.

3.2.2 Registros, datos o información, transmitidos por equipos electrónicos o de tecnología informática y almacenada en medios físicos y sistemas virtuales.

Aquí se tratarán los correos electrónicos o E-mail (electronic mail), así como a los mensajes de texto, los mensajes y archivos enviados mediante las plataformas de mensajería instantánea, como por ejemplo WhatsApp, Wechat, Messenger entre otros, los cuales son generados y transmitidos por medio del uso de los equipos electrónicos o de tecnología informática.

La definición de correo electrónico la trae la Directiva 58/2002/CE, del 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[61]. El correo electrónico lo compone un contenido en texto plano, sus anexos que puede o no llevarlos adjuntos y que normalmente se trata de los tipos de archivo que se vieron en el apartado 3.3.1.4 "ficheros y archivos" y por otra parte los datos y la meta data, que normalmente se encuentran en el encabezado y que es necesario de conocimientos técnicos para su correcta interpretación. Por ejemplo, la obtención de la dirección IP de origen, dirección IP destino que normalmente corresponderán a las del servidor de correo, ¿cuántos receptores tiene el correo?, ¿cuál es el nombre de usuario y dirección de E-mail del emisor?, ¿Cuál es el nombre de usuario y dirección de e-mail del receptor?; entre otros que nos presenta NOTARIO, PARRA DE GALLO, VEGETTI Y LEONE[62]

En todo caso, debemos aclarar que tanto para los correos electrónicos como para los mensajes de texto y de mensajería instantánea, la prueba o evidencia digital que se

---

informática y oficina y trata de la automatización de oficinas y de los procesos del trabajo que se realizan en las mismas".

[61] "Correo Electrónico: todo mensaje de texto, voz o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que este acceda al mismo".

[62] NOTARIO, Enzo, PARRA DE GALLO, Beatriz, VEGETTI, Marcela, LEONE, Horacio. "Herramienta para el Análisis Forense de Correos Electrónicos". RISTI *Revista lbérica de Sistemas de tecnologías e Información*. 2019, nº 32, pág 20.

recolecta y se presenta como fuente probatoria es la información y los datos que trae el mail en su cuerpo, al igual que la que contienen los archivos o ficheros anexos o adjuntos.

Por otra parte, es de vital importancia al momento de la valoración de este tipo de prueba o evidencia digital que se conozca el medio de almacenamiento del cual se produjo su extracción o recuperación, puesto que los protocolos o las maneras de realizar esta labor pericial varían dependiendo el sistema de almacenamiento.

Así, por ejemplo, si se trata de un mensaje alojado en el disco duro del PC o en la memoria flash del móvil, el mismo podrá ser realizado mediante la intervención de dicho medio de almacenamiento, respetando en todo caso los protocolos para la recolección de la evidencia digital a los cuales se ha venido haciendo mención, además de garantizar los derechos fundamentales como la intimidad, la privacidad y protección de los datos.

Cabe resaltar que en la mayoría de los casos este procedimiento se hace mediante la extracción de información y no la recuperación, en especial para lo que tiene que ver con el correo electrónico, puesto que una vez borrado del buzón de correo el mismo no se puede recuperar[63], y es ahí donde aparece la otra manera de recolección que es mediante orden judicial que ordene al proveedor de buzón de correo, entregar la información y este último deberá garantizar que la recolección se hizo de forma adecuada, por cuanto no debería ser tomado por válido la simple entrega sin la deposición de quien haya aportado la prueba o evidencia digital. Ambas maneras son válidas, pero ambas deben valorarse conforme a la manera técnica de cómo se llevó a cabo el proceso y en todo caso que se garantice su integridad y su autenticidad.

3.2.3 Datos e información adquirida mediante OSINT.

Al igual que los algoritmos, entra a formar parte de las nuevas fuentes probatorias. Al hacer referencia a estos términos se deben abordar desde un lenguaje coloquial a fin de

[63] DI LORIO, Ana Haydée. "La recuperación de la información y la informática forense: Una propuesta de proceso unificado", memorias del Simposio Argentino de Informática y Derecho (SID 2015)- JAII 44, SADIO. 2015, nº44. Pág. 124. define extracción lógica y recuperación física. "Una cosa es, la información o los datos digitales que se encuentra almacenados en un medio de almacenamiento y que son perceptibles a los sentidos de la vista y la audición mediante la simple interacción de la persona y el aparato que contiene el medio, mediante las aplicaciones o los programas que tiene instalados, incluyendo su sistema operativo (extracción de información); otra cosa diferente es cuando la información o los datos han sido borrados de la unidad lógica de ese equipo electrónico, pero que aun así pueden seguir almacenados en la unidad física , sin embargo, ya no son perceptibles por el humano con esa simple interacción, sino que se hace necesario el uso de herramientas forenses o software forense para poder acceder y visualizar estos datos o información (recuperación de la información)".

garantizar el entendimiento de los operadores de justicia, por cuanto a medida que se definan sus conceptos se hará referencia a los retos y particularidades que trae consigo la valoración de este tipo de información.

Información que se adquiere a través del manejo automatizado de grandes cantidades de datos o que aun siendo pocos permiten vincular particularidades de estos para posteriormente presentar una información que en últimas es direccionada a probar uno o varios hechos en particular. En su orden serán explicados BD, ML y OSINT.

3.2.3.1 Big data.

Cada vez son más los datos que las personas dejan a disposición de terceros en el ciberespacio, durante la transición de la ciudadanía física a una ciudadanía digital, donde nuestros datos personales, así como nuestra información se convierten en los principales activos no sólo de nosotros mismos, sino de las empresas que ven en ellos su principal fuente económica.

Lo anterior para hacer referencia a la definición que trae JOYANES respecto a lo que es el BD "son los grandes conjuntos de datos que tienen tres características principales: volumen (cantidad), velocidad (de creación y utilización) y variedad (tipos de fuentes de datos no estructurados, tales como la interacción social, video, audio, cualquier cosa que se pueda clasificar en una base de datos)"[64]. Es decir, son grandes cantidades de datos que superan cualquier tipo de análisis humano, que pueden estar en un mismo lugar o disgregado en diferentes fuentes de almacenamiento que puede ser físico pero que en un alto porcentaje es virtual.

Es así como estos grandes volúmenes de datos se ven procesados con el fin de buscar algún tipo de conexión o relación entre sí que permita generar información interpretable y relevante para quién le interesa. Esto se hace por medio del siguiente concepto que nos ocupa el ML.

3.2.3.2 Machine Learning.

[64] JOYANES AGUILAR, Luis. *Big Data, análisis de grandes volúmenes de datos en organizaciones,* editorial Alfa omega, México D.F, 2013, pág. 15.

Así como el BD son los grandes conjuntos de datos, estos datos no pasarían de ser simples datos, tal como lo definimos en el apartado 3.2.1 del presente texto, algo con existencia propia e independiente y que tiene poco significado para el usuario, pero si esos datos son sometidos a una técnica o disciplina que mediante algoritmos sea capaz de procesarlos y arrojarnos una información que sea representativa y que además prediga un resultado a posteriori sería más útil.

De esto trata el ML, tal como lo presenta la firma CLEVERDATA "Machine Learning es una disciplina científica del ámbito de la IA que crea sistemas que aprenden automáticamente. Aprender en este contexto quiere decir identificar patrones complejos en millones de datos. La máquina que realmente aprende es un algoritmo que revisa los datos y es capaz de predecir comportamientos futuros. Automáticamente, también en este contexto, implica que estos sistemas se mejoran de forma autónoma con el tiempo, sin intervención humana."[65]

Concepto suficientemente claro que invita a la reflexión frente a la integridad de la prueba o evidencia digital, puesto que difícilmente podemos conocer el algoritmo con el que dicha máquina procesa los datos para entregar el resultado, por cuanto se rompe el principio de contradicción, perdiendo garantía frente al derecho al debido proceso.

Por otra parte, se desconoce si estos datos o esa información, para poder entregarse, han sido modificados en parte o en su totalidad. Es así como para la correcta valoración de esta prueba o evidencia digital debería exigirse la entrega del algoritmo utilizado para el procesamiento de esos datos por parte del propietario y así poder ser controvertidos.

Por último, hacemos relación a la técnica de búsqueda de información en medios abiertos (OSINT).

3.2.3.3 OSINT.

Definamos el concepto de OSINT. Para ello nos permitimos citar a HOEPMAN y LEENES quien la definen como el "proceso de recolección, análisis y uso de la

[65] Disponible en la url: https://cleverdata.io/que-es-machine-learning-big-data/ , recuperado el 14 de abril de 2020, Cleverdata corp.

información disponible en fuentes abiertas, para propósitos de inteligencia"[66]. Esta técnica de inteligencia en medios abiertos aparece en el panorama probatorio en el momento en que los datos recolectados y procesados se presentan ante los tribunales como prueba documental en inicio, puesto que con la recopilación de los datos y la información generada a partir de los mismos se plasma por parte de los investigadores de las partes un informe que entrega desde ubicaciones de personas hasta su perfil criminógeno, elaborado a partir de la información que una persona pueda tener como suya en el "ciber espacio"[67], o incluso y lo que se hace preocupante al momento de la valoración de esta prueba o evidencia digital, que sea un tercero el que presente esta información en ese mundo virtual.

Esta práctica ha venido a remplazar lo que en la legislación Colombiana se conoce como búsqueda selectiva en bases de datos, contemplado en el artículo 244 del CPP[68], en el cual se hace referencia a las búsquedas en bases de datos de acceso público, pero a diferencia de estas, las búsquedas que se hacen por medio de OSINT utilizan herramientas de ML, las cuales mediante un barrido de BD en el ciber espacio retorna la información solicitada, con el fin que vaya siendo procesada con la ayuda del algoritmo o los algoritmos prediseñados en las herramientas utilizadas por parte de un analista de datos o incluso muchas veces por los mismos investigadores de las partes; para el caso de la Fiscalía de su policía judicial.

Los interrogantes en esta prueba o evidencia digital, con fines de su adecuada valoración probatoria son entre muchos otros, ¿de dónde exactamente se obtuvo los datos o la información?, ¿fue autorizado el tratamiento de esos datos por parte de quien los está suministrando? o, por el contrario, ¿los datos fueron filtrados en la web por algún

---

[66] HOEPMAN, Henks y LEENES, Ronald. " Open source intelligence and privacy by Design". *Computer Law and Security Review.* 2013, nº 29, pág. 676.

[67] ASENCIO GUILLEN, Antonio y MARCO, Julio Navío. *La génesis del ciberespacio, una visión desde las teorías de la comunicación,* UNED publicaciones, Madrid, 2017, pág.1. Quienes definen el ciber espacio como un…" conjunto de posibles comunicaciones que se desarrollan en el ámbito digital, a través de los diferentes dispositivos, canales y medios, y que permitan la interconectividad entre los usuarios"

[68] Ley 906 de 31 de agosto de 2004 "Por la cual se expide el Código de Procedimiento Penal" ARTICULO 244: La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. Cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos.

ciberdelincuente? por cuanto se trataría de información ilegal, ¿qué información de la presentada es la que realmente la persona llevó al entorno digital?

Cuestiones que conllevan a que los datos y la información recolectada, aunque deberán ser valoradas en contexto, sean criticadas en su integridad, autenticidad y su confiabilidad, es decir preguntarse ¿por qué son confiables esos datos? y ¿cuál es su fuente?

Es así como esta información debe ser tratada como lo que son: prueba o evidencia digital. No como prueba documental, que si bien es cierto se viene haciendo por equivalencia funcional, ya hemos ido sentando bases de peso, del por qué no se puede dar esa equivalencia para este tipo de fuentes probatorias.

Además de valorar la prueba o evidencia digital en sí misma, los operadores de justicia deberán ponderar los derechos fundamentales que allí pueden colisionar, al momento de la adquisición, como lo son la intimidad, la privacidad de los datos y la información y la libertad de información, aspectos que se han venido desarrollando por parte de la Corte Constitucional Colombiana. En tal sentido la misma en Sentencia C-602 de 2016 hace referencia a los tipos de información y la forma de acceder a ella, enmarcándola en (Pública, Privada y semi Privada)[69], por cuanto se hace necesario inicialmente conocer por lo menos si esta práctica se enmarca en alguno de los supuestos citados y así poder valorar su licitud.

Por otra parte, para acercarse a una acertada interpretación y valoración que permita al juez hacer uso de la razón y la sana crítica, (conceptos que se desarrollaran en el Titulo II de este texto), este deberá resolver a lo sumo cuatro interrogantes fundamentales: 1. Procedencia, es decir preguntarse ¿de dónde ha salido el contenido y si es el contenido original? 2. La fuente ¿Quién ha subido el contenido?, 3. La fecha ¿cuándo fue creado el contenido y si es concordante esta con los hechos? y 4. Localización ¿En qué lugar fue creado el contenido?, interrogantes que seguramente en la pericia deben ilustrarse puesto que generalmente son metadatos y si bien pueden ser alterados, dependerá de la pericia para así refutarse.

[69] Sentencia nº C-602/2016 de 02 de noviembre de 2016, F.J 1.5.1 (D-11332).

TITULO II. ADMISIBILIDAD Y VALORACIÓN PROBATORIA DE LA PRUEBA O EVIDENCIA DIGITAL.

Conocidos los intríngulis técnicos de la prueba o evidencia digital en los cuales encontramos bastos vacíos legales y establecidas las diferencias con el documento electrónico, en sentido que, si bien hace parte de la evidencia digital, el mismo merece una valoración diferenciada, más nunca análoga a la prueba o evidencia digital a la que ya nos referimos.

Pasamos ahora a analizar alguna de las cuestiones procesales más relevantes sobre la misma, abordándola en los diferentes momentos donde el juzgador (juez o magistrado) pasa a ocupar un papel preponderante dentro de los procesos judiciales. Este análisis se verá resumido en tres momentos: un primer momento, donde se evalúa la admisibilidad de la prueba digital; un segundo momento a justipreciar su eficacia y fuerza probatoria; y un tercer momento, proceder a valorar lo que en ese momento ya habrá de ser las fuentes de prueba, teniendo como base lo desglosado en el título I del presente escrito.

El presente título será abordado teniendo en cuenta, por un lado, lo versado y aplicado en la materia respecto de la legislación y la jurisprudencia española y por otro, lo acuñado en materia probatoria respecto al tema en la legislación colombiana, buscando demostrar que, tanto en uno como en otro Estado, este tipo de prueba o evidencia debe ser comprendida, tratada y valorada de la misma forma, pudiendo incluso aseverar que al tratarse de una prueba que sin importar el lugar donde se genere, guarda las mismas características técnicas, por cuanto su aceptación, comprensión y valoración en el ámbito probatorio debe darse atendiendo a las mismas razones y circunstancias, *erga omnes*.

Capítulo I. La admisibilidad de la prueba o evidencia digital.

Para hablar de admisibilidad de la prueba o evidencia digital primero se debe conocer de manera general a que refiere el termino admisibilidad probatoria, por lo que iniciaremos haciendo referencia a lo versado por BUENO DE MATA, quien entiende el término como "el resultado de un juicio valorativo hecho por el juzgador acerca de las condiciones que ha de reunir el medio o la actividad probatoria que se propone para que pueda ser introducido

en el proceso"[70]. En contraste, un concepto jurisprudencial presentado por ORTUÑO NAVALON, quien interpretando lo versado por el Tribunal Constitucional en STC 236/2002, de 9 de diciembre[71], menciona que "para la doctrina constitucional, toda prueba que pretenda ser incluida en un proceso, ha de reunir los requisitos de pertinencia, necesidad o utilidad y licitud"[72].

Teniendo como base lo citado anteriormente, y acoplando ambas definiciones, podemos decir que la admisibilidad es la acción que ejecuta un juez mediante el examen de cumplimiento o no de requisitos normados, que deben ser cumplidos en su totalidad, como lo son: los de pertinencia, necesidad, legalidad y licitud, los que determinarán en todo caso, cuáles serán los medios probatorios que se practicarán y valorarán dentro de un proceso judicial en concreto.

Lo anterior nos lleva a revisar cada uno de esos criterios a los que se refiere la admisibilidad.

1.1 Criterios de admisión.

Tal como se hizo referencia, los criterios de admisión de la prueba se dividen en tres. Su pertinencia, utilidad y ante todo su legalidad. Criterios que deben de ser cumplidos por todos y cada uno de los medios probatorios que se deseen hacer valer dentro del proceso, tal como aparece en las distintas legislaciones que venimos analizando, sea el caso la LEC y el CGP que al unísono versan sobre estas particularidades. La primera (LEC) en su artículo 283[73], se traduce en la pertinencia y utilidad de la prueba desde un sentido negativo, es decir la impertinencia y la inutilidad, y, por otra parte, el artículo 287[74], deja claro el concepto de ilicitud.

---

[70] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*… op.cit., pág 221.
[71] STC nº 236/2002, de 9 de diciembre de 2002, F.J. 4º, (RJ 2002/236).
[72] ORTUÑO NAVALON, María del Carmen. *La prueba electrónica ante los tribunales*… op. cit, pág. 109.
[73] Ley 1/2000 del 7 de enero, Ley de enjuiciamiento civil española, Artículo 283. Impertinencia o inutilidad de la actividad probatoria. 1. No deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente. 2. Tampoco deben admitirse, por inútiles, aquellas pruebas que, según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos. 3. Nunca se admitirá como prueba cualquier actividad prohibida por la ley.
[74] Ley 1/2000 del 7 de enero, Ley de enjuiciamiento civil española, Artículo 287. Ilicitud de la prueba. 1. Cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes. Sobre esta cuestión, que también podrá ser suscitada de oficio por el tribunal, se resolverá en el acto

De igual manera, encontramos en el CGP, que en su sección tercera (régimen probatorio), título único (pruebas) capítulo I (disposiciones generales), en especial el artículo 168[75] hace referencia a la pertinencia, utilidad y legalidad, mencionando que si la misma no goza de estas características será rechazada de plano.

Revisado lo anterior y al igual que se analizó en el acápite referente a los medios probatorios, la admisibilidad de la prueba o evidencia digital no aparece normada en stricto sensu, por lo que nuevamente debemos preguntarnos si estos mismos requisitos o particularidades serán o no válidas al momento de decretar la admisibilidad de la prueba o evidencia digital; al respecto ABEL LLUCH hace referencia argumentando que "la admisibilidad de la prueba electrónica debe atender algunos de sus factores o características específicas, y concretamente, lo decisivo es que al proceso de traslación de una realidad intangible -el entorno digital- a otra tangible e incorporable a un soporte susceptible de ser llevado a presencia judicial, se efectúe con arreglo a un proceso de registro y salida de datos que resulte técnicamente verificable"[76]. De tal manera que, para que una prueba digital sea admisible deberá cumplir estos tres principios a los cuales se ha hecho alusión y que desarrollaremos a continuación.

1.1.1 Pertinencia.

Es el primer supuesto para la admisión de la prueba digital, que al igual que para los demás medios probatorios estará dado por la relación que este tenga con el proceso o caso objeto de la *litis (thema dicidendi),* tal como nos lo presenta DELGADO MARTÍN refiriéndose al concepto de pertinencia de la prueba digital, el mismo acota " ha de existir una relación lógica entre el hecho que pretende acreditarse mediante el concreto medio probatorio y los hechos que constituyen el objeto de la controversia, así como una aptitud o

---

del juicio o, si se tratase de juicios verbales, al comienzo de la vista, antes de que dé comienzo la práctica de la prueba. A tal efecto, se oirá a las partes y, en su caso, se practicarán las pruebas pertinentes y útiles que se propongan en el acto sobre el concreto extremo de la referida ilicitud. 2. Contra la resolución a que se refiere el apartado anterior sólo cabrá recurso de reposición, que se interpondrá, sustanciará y resolverá en el mismo acto del juicio o vista, quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en la apelación contra la sentencia definitiva.

[75] Ley 1564 del 12 de julio de 2012, Artículo 168. Rechazo de plano. El juez rechazará, mediante providencia motivada, las pruebas ilícitas, las notoriamente impertinentes, las inconducentes y las manifiestamente superfluaso inútiles.

[76] ABEL LLUCH, Xavier, *juicio de admisión de la prueba electrónica,* en: ABEL LLUCH, Xavier y PICÓ I JUNOY, Joan, *La prueba electrónica,* Editorial Bosh, Barcelona, 2011, nº pág. 383-384.

idoneidad para formar la debida convicción del juzgador"[77], por consiguiente es menester que el medio de prueba a usarse dentro del proceso para hacer valer las fuentes de prueba estén estrechamente vinculadas con el caso.

Es de resaltar que la pertinencia como uno de los requisitos de admisibilidad en la legislación española se encuentra incorporada como un derecho fundamental consagrado en el artículo 24.2 de la carta Magna[78].

1.1.2 Utilidad.

La utilidad dentro del test de admisibilidad de la prueba o evidencia digital hace referencia a la fuente probatoria con la que se quiere demostrar un hecho, en el sentido que la misma deberá ser idónea para lograr demostrar el particular, al respecto BUENO DE MATA refiere que el artículo 283 de la LEC entrega una definición en negativo, es decir desde la inutilidad de la actividad probatoria, es así como el artículo en cuestión en su apartado segundo resalta que, son inútiles las pruebas, que según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos.[79]

En este sentido la prueba inútil se entenderá como aquella que, al no adecuarse el medio para demostrar el fin propuesto, razonablemente se podrá concluir que esta no alcanzará el resultado para lo cual se pretende incorporar[80].

1.1.3 Legalidad y licitud.

Nos encontramos frente al último de los requisitos que conceden la admisibilidad de la prueba digital al proceso y tal como se observa en el título, el mismo trae dos acepciones que debemos resolver por separado, por un lado, encontramos la ilegalidad y por el otro la ilicitud, ambos tienden a confundirse y en ocasiones a usarse como sinónimos. Sin

---

[77] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones*… op.cit., pág 51.

[78] Constitución Española de 1978, articulo 24, numeral 2 "Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, **a utilizar los medios de prueba pertinentes para su defensa**, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

[79] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*… op.cit., pág 229.

[80] DE LA OLIVA SANTOS, Andrés, derecho proceso civil. El proceso de declaración. Editorial universitaria Ramon Areces, Madrid, 2000, pág. 291.

embargo, son términos diferentes que en todo caso deben cumplirse. Su gran diferencia radicará en que, mientras la prueba ilegal será aquella que ha sido obtenida con falta a los principios y normas contemplados en la ley siendo inadmisible de pleno derecho, la prueba ilícita será aquella que ha sido obtenida vulnerando los derechos fundamentales.[81]

Es así como la legalidad, la pertinencia y la utilidad son criterios legales de admisión de los medios de prueba, que pueden identificarse respetando los requisitos formales procesales. En este caso los requisitos formales procesales del medio de prueba digital, mientras que la ilicitud no constituye un parámetro legal para la admisibilidad, sino que actuará como mecanismo para excluir una prueba que haya sido admitida, por haber vulnerado derechos fundamentales al momento de obtenerla[82].

Entendiendo que a la fecha no se dispone de leyes procesales que estipulen o normen acerca de este medio probatorio de manera autónoma, la legalidad estará dada en el sentido que la prueba se haya incorporado por quien está legitimado para hacerlo y dentro de los plazos previstos en cada norma procesal según la jurisdicción correspondiente.[83]

Por lo anterior, se plantea como solución procesal temporal a la espera de legislación en la materia la aplicabilidad de los protocolos y estándares internacionales, de los cuales ya existe jurisprudencia al respecto, en donde la Corte Constitucional Colombiana mediante sentencia C-334 de 2010[84] exigió la aplicación de los estándares internacionales respecto al

---

[81] MIRANDA ESTRAMPES, Manuel. "La prueba ilícita: la regla de exclusión probatoria y sus excepciones". *Revista Catalana de Seguretat Pública,* 2010, pág 3 y ss.

[82] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*… op.cit., pág 232.

[83] Al respecto BUENO DE MATA ibidem, pág 233 a 234, relaciona que: …"en el proceso civil la legitimación corresponde a las partes, en virtud del principio de aportación", además de hacer referencia a las pruebas que de oficio puede ordenar el tribunal, sin embargo resalta …"tanto en el juicio ordinario como en el juicio verbal, por carecer el juez, en términos generales, de conocimientos técnicos e informáticos que le lleven a actuar de oficio, por lo que su actuación es posible, pero bastante limitada", ahora bien respecto al criterio temporal este asienta …" se deberán respetar los plazos procesales generales en cuanto al momento de la aportación del material probatorio, puesto que o sino entraría en juego la preclusión procesal y la improrrogabilidad de plazos".

[84] STS nº C-334/2010 de 12 de mayo de 2010, F.J 2.1.1 (D-7915), De esta sentencia se extractan dos fundamentos jurídicos relevantes. El primero con relación a la necesidad de un estándar legal que habilite la admisibilidad de la prueba o evidencia digital. …"Con el cumplimiento de ciertos protocolos y del control previo de legalidad, los documentos electrónicos pueden llegar al proceso inalterados y su estudio puede efectuarse con todas las garantías para el investigado y para el propósito de perseguir el delito. Llegan como pruebas, ancladas en la cadena de custodia, con la seguridad de que puedan convertirse en evidencia digital. Por esto, **es necesario desarrollar un "estándar legal de políticas de seguridad informática", que habilite la admisibilidad de pruebas de tal naturaleza, con presunción iuris tantum de validez como evidencia digital".**

manejo de la evidencia digital y sugirió un estándar legal de políticas de seguridad informática, que habilite la admisibilidad de pruebas de tal naturaleza.

Capitulo II Una visión de algunos instrumentos normativos en materia de aportación de la prueba o evidencia digital al proceso judicial.

Sin lugar a duda la presencia de las TIC´s en el mundo, ha traído grandes retos para los Estados, y en especial al campo jurídico, al campo de las leyes, que desde sus albores fue concebido de manera reactiva, es decir a medida que sucede un acontecimiento o hecho que requiere de una determinada aplicación normativa, actúa para resolverla con base en lo existente. Pero cuando se trata de un hecho nuevo, no queda más que repensar las normas, bien sea para crear una nueva que se adecue al caso, o modificar las ya existentes; mientras esto sucede abordar por analogía o equivalencia funcional de lo que hasta ese momento se asemeje al particular.

Esta práctica hasta el día de hoy es aplicable en todas y cada una de las legislaciones del orbe, sin embargo, el que a hoy se siga realizando no quiere decir que sea lo correcto o lo más adecuado, en especial cuando se piensa en un e-world o mundo conectado, donde internet, la nube, el ciber espacio, la IA, el IOT, el BD, el ML, las redes neuronales, la robótica, la tecnología 4 y 5G e incluso ya se habla del 6G o sexta generación, aún sin haberse implementado la quinta y si pensamos un poco más allá, nos encontraremos con la computación cuántica. Nos lleva a pensar en un Derecho Globalizado, con una teoría general aplicable *erga omnes*, por lo menos en algunas materias.

Este aspecto lo presenta TWINING en su obra Derecho y Globalización, donde entre otros aspectos resalta "Nadie estaría dispuesto a negar el impacto que ejerce la descentralización del Estado como sujeto de derecho y la aparición de múltiples sujetos transnacionales en el mundo contemporáneo, que nos demandan herramientas teórico-jurídicas diferentes a las tradicionales"[85]. Pues bien la valoración de la prueba digital es una

---

El segundo insta a la aplicabilidad y cumplimiento de los protocolos forenses internacionales para el manejo de la evidencia digital. …"Contrario a lo establecido en la sentencia STS nº C-336 de 2007, la recuperación de información aludida de que trata el art. 237 CPP, debe ser sujeta a un control previo, que asegure, con el lleno de los requisitos legales, constitucionales y **el cumplimiento de los protocolos forenses internacionales del manejo de la evidencia digital, la cadena de custodia, es decir, la inalterabilidad de sus contenidos y la preservación de los datos sensibles de la persona afectada con la actuación".**

[85] TWINING, William. *Derecho y globalización,* Siglo del Hombre Editores, Bogotá, 2003, pág. 1.

de esas materias que debe de abordarse adoptando una teoría por lo menos procesal globalizada, puesto que la prueba o evidencia digital será la misma en cualquier Estado, gozará de las mismas características y su forma de recolección al igual que su valoración probatoria, deberá obedecer a unas prácticas mundialmente reconocidas, prácticas y estándares que como vemos ya se encuentran desarrollados y a los cuales algunas cortes remiten y se basan para ejercer el control procesal y la valoración de este tipo de pruebas.

Es así como en el medio aparecen algunos protocolos, estándares e incluso normativa internacional que versa sobre la materia y sobre la cual debiéramos navegar, para marcar el norte de la prueba o evidencia digital dentro los procesos judiciales.

2.1 Convenio de Budapest sobre la cibercriminalidad[86].

El presente Convenio en su apartado segundo contempla las normas procesales, estableciendo los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia.[87] Es de resaltar que el presente Convenio ha sido ratificado tanto por Colombia como por España[88].

Para el tema procesal que nos ocupa el Convenio tal como lo trae el informe explicativo del Consejo Europeo "establece los siguientes poderes procesales: conservación rápida de datos informáticos almacenados; conservación y revelación parcial rápidas de los datos relativos al tráfico; la orden de presentación; el registro y la confiscación de datos informáticos almacenados; la obtención en tiempo real de datos relativos al tráfico, y la interceptación de datos relativos al contenido"[89].

---

[86] "El Convenio de Budapest y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001) y el Convenio fue abierto a la firma en Budapest, el 23 de noviembre de 2001, con motivo de la celebración de la "Conferencia Internacional sobre la ciberdelincuencia" tomado del Informe Explicativo del consejo de Europa sobre el convenio de Budapest contra la cibercriminalidad, pág 1. Disponible en la url: https://rm.coe.int/09000016802fa403 , recuperado el 18 de abril de 2020,

[87] Disponible en la url: https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ , recuperado el 18 de abril de 2020, ESET SECURITY.

[88] España ratifica el Convenio el 1 de octubre del año 2010 por medio del instrumento de ratificación publicado en el Boletín Oficial del Estado el 17 de septiembre de 2010 con referencia BOE-A-2010-14221. Por su parte, Colombia ratifica el convenio el 24 de julio de 2018 mediante la Ley 1928/2018.

[89] Informe Explicativo del Consejo de Europa sobre el Convenio de Budapest contra la Cibercriminalidad, pág 6. Disponible en la url: https://rm.coe.int/09000016802fa403, recuperado el 18 de abril de 2020, Council Of Europe.

Por lo anterior el Convenio de Budapest será entonces nuestro primer y único referente normativo con fuerza vinculante para los Estados miembro que verse en materia procesal digital, para el caso en materia penal, puesto que el mismo versa sobre la evidencia que se pueda recolectar frente a los delitos informáticos, materia ampliamente desarrollada por VELASCO SAN MARTÍN, quien en su obra plantea los aciertos, desaciertos, pero sobre todo la exigencia vinculante del citado Convenio sobre la Cibercriminalidad.[90]

2.2 Ley 527 de 1999, de Comercio Electrónico-El valor probatorio de un mensaje de datos (LEY COLOMBIANA).

Esta Ley hace referencia al valor probatorio del mensaje de datos, contenido en un documento electrónico como evidencia digital, más no así para las demás fuentes digitales de prueba. Sin embargo, al regirnos por un derecho *ius* positivista, diremos que al no haber otra norma que verse sobre la materia esta es la que deberá entenderse y aplicarse al momento de valorar la prueba o evidencia digital.

Situación que lleva al juzgador a incurrir en una falacia de tipo *ignoratio elenchi*[91] al momento de valorar la prueba, puesto que este entenderá haber probado algo frente a una materia, y realmente prueba algo distinto e incluso no logra probarlo, sino contraponerlo a la definición de Prueba o Evidencia Digital, tomando así una decisión valorativa errada producto de la confusión legislativa.

2.3 Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos (ESPAÑA).[92]

Esta circular en resumen versa por un lado sobre los conceptos técnicos a tener en cuenta en las investigaciones judiciales que tengan dentro de sus medios y fuentes probatorias lo digital como precepto y por otro lado hace referencia a cada una de las etapas

---

[90] VELASCO SAN MARTÍN, Cristos. *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos.* Tirantlo blanch, Valencia, 2016. Págs 75 a 89 y 236 a 259.

[91] …"Aristóteles muestra que él entiende por premisa contradictoria o Ignoratio Elenchi, aquella que se refiere a casos en los que, por falta de agudeza lógica, un argumentador cree que ha probado una cosa, pero, en el mejor de los casos, ha probado otra distinta" asi lo cita MORAGA, Ramón. "Argumentación Ideal y falacias Unidad I: Argumentación". *Instituto Nacional José Miguel Carrera. Lengua Castellana y comunicación*, Tercero Medio. Disponible en la url: http://www.scribd.com/doc/17547111/Modulo-3-argumentación-falacias, recuperado el 18 de abril de 2020.

[92] BOE-A-2019-4244. Disponible en la url: http://www.boe.es, recuperado el 24 de abril de 2020, Boletín Oficial del Estado.

que se deben tener en cuenta al momento del registro y recolección de la prueba digital por parte de la policía judicial y los peritos. Pero además trae un valor agregado frente a la forma o instrumentos para la realización de equipos remotos con el ánimo de dar legalidad a lo recolectado en los mismos.

2.4 Normativa ISO 27037:212. Indicaciones para la identificación, recolección, adquisición y preservación de la evidencia digital.

Este estándar es básico si se tiene en cuenta que con su aplicación se preserva los principios de legalidad, autenticidad, integridad y disponibilidad futura, haciéndola confiable y entregándole suficiencia[93].

2.5 Normativa ISO 27042:2015. Indicaciones para el análisis e interpretación de la evidencia digital.

Estándar que nos entrega las directrices de cómo se debe analizar e interpretar la evidencia digital, aquí están contemplados los mecanismos para la identificación y el análisis, siendo así de fundamental aplicación y conocimiento para la valoración de la fuente de prueba digital, ya que la misma por si sola se tratará como se mencionó en apartado anterior de simples datos.

Capítulo III. La prueba digital anticipada como garantía o no de principios y derechos dentro de los procesos judiciales.

Una de las principales características de la prueba o evidencia digital es su volatilidad, en tal sentido se ha venido entendiendo que en la mayoría de las veces este tipo de prueba no se podrá practicar en el juicio o la vista si no ha sido recolectada y preservada con anterioridad guardando y garantizando su integridad, A continuación, hacemos referencia a ello, al tiempo que establecemos la viabilidad o no de su práctica respecto a la prueba o evidencia digital.

---

[93] SEMPRINI, Gastón. "El Análisis integral de la evidencia digital", *memorias del Simposio Argentino de Informática y Derecho.* 2017, nº 46, pág 91. Define esta norma como…" Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones."

Tomando como base el ámbito penal tendremos que decir que son todos aquellos actos de indagación o investigación que se realizan (en la etapa de instrucción) refiriéndonos a la legislación Española y (en la etapa de indagación) si hacemos referencia a la legislación Colombiana, con el fin de recolectar pruebas o evidencias que sean útiles dentro de un proceso para llegar a determinar un hecho específico, tal como se encuentra representado en el libro II del CPP[94] y en los Libros II y IV, título II capítulo II y III así como el Titulo III capítulo II de la LECRIM[95].

Tomando como base lo anterior, diremos que son esas diligencias las que se debe llevar a cabo respecto a la prueba o evidencia digital. Y la garantía dentro del proceso, versará sobre su integridad, toda vez que la misma permitirá en cualquier momento del proceso recolectar y preservar la prueba hasta el momento de su práctica en la audiencia de juicio oral, sin perjuicio que la misma corra riesgo de modificarse y si así fuere ese hecho podrá ser demostrable técnicamente por un experto en la materia, que para el caso se trataría de un perito en informática forense.

Esto es viable dadas las condiciones y características de la prueba o evidencia digital, mismas que permiten que una vez recolectada se conserve idéntica, aunque esta haya desaparecido al momento de llegar al juicio (en especial para las fuentes probatorias de carácter virtual o aquellas alojadas en medios o sistemas de almacenamiento virtual). Cuestión que siempre permitirá que la prueba pueda ser practicada en juicio oral sin importar el experto que la reproduzca, la evalúe y la explique en el estrado judicial, permitiendo de esta forma la valoración por parte del Juez o Magistrado, puesto que allí se revelaran todas y cada una de las características de la prueba o evidencia digital a las cuales nos referiremos en el siguiente capítulo como lo son su integridad, su licitud, su disponibilidad futura y eventualmente su autenticidad.

---

[94] Ley 906 de 31 de agosto de 2004 "Por la cual se expide el Código de Procedimiento Penal" Libro II Técnicas de indagación e investigación de la prueba y sistema probatorio. Artículos 200 a 335.

[95] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. LIBRO IV. De los procedimientos especiales, TÍTULO II. Del procedimiento abreviado, Capítulo II. De las actuaciones de la Policía Judicial y del Ministerio Fiscal. Capítulo III. De las diligencias previas. TÍTULO III. Del procedimiento para el enjuiciamiento rápido de determinados delitos, Capítulo II. De las actuaciones de la Policía Judicial.

Caso contrario sucede con la prueba anticipada la cual es entendida por BUENO DE MATA[96] como aquella que es practicada de manera excepcional antes de la etapa procesal prevista, o incluso antes del proceso como prueba preconstituida[97]. Él mismo hace referencia a que la figura de la prueba anticipada es aplicable a la prueba electrónica por disponer de figura legal para tal fin según lo versado en los artículos 293 a 296 de la LEC 1/2000 y en segundo lugar por la característica de volatilidad que tiene la prueba electrónica.

Si tomamos como referencia el concepto de prueba anticipada que nos trae la sentencia de la Corte Constitucional Colombiana C-830 del 8 de octubre de 2002[98] nos damos cuenta que este no sería el mecanismo para acudir a la jurisdicción con el fin de brindar garantía dentro de los procesos judiciales puesto que la misma una vez recolectada no corre el riesgo de no poder ser practicada a posteriori, puesto que su práctica no dependerá de la persona que la recolectó o de quien haya realizado el informe pericial en un inicio.

A *contrario sensu* de lo que sucede con el testimonio de una persona que se encuentra en grave estado de salud, lo cual hará poco probable que se cuente con su testimonio si se espera hasta la audiencia de juicio. Esto sin perjuicio que lo solicitado como prueba anticipada sea el testimonio de la persona de manera virtual, cuestión que constituiría una prueba anticipada que versará sobre el testimonio, no sobre el medio de prueba digital, que a pesar de convertirse en el momento de su almacenamiento en una fuente de prueba digital, a la cual se le deben de aplicar todos y cada uno de los protocolos para su

[96] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*…op.cit., pág. 245.
[97] RIZO GOMEZ, Belén. *La anticipación de la prueba en el proceso civil,* tirant lo blanch, Valencia, 2010, pág 69. "La prueba preconstituida se efectúa sin intervención judicial y depende de la voluntad de la parte que pretende en un futuro introducir el dictamen en el proceso alcanzando valor probatorio."
[98] Sentencia nº C-830/2002 de 8 de octubre de 2010, F.J 1 (D-3991), la cual asiente respecto a la prueba anticipada …" Desde el punto de vista práctico las pruebas anticipadas con fines judiciales se explican por la necesidad de asegurar una prueba que después, al adelantarse el proceso correspondiente y por el transcurso del tiempo y el cambio de los hechos y situaciones, no podría practicarse, o su práctica no arrojaría los mismos resultados, como ocurre por ejemplo cuando una persona que debe rendir testimonio se encuentra gravemente enferma", … "Desde el punto de vista constitucional dichas pruebas tienen su fundamento en la garantía de los derechos fundamentales de acceso a la justicia, el debido proceso y el derecho de defensa o contradicción, contemplados en la Constitución, en cuanto ellos implican, para las partes e intervinientes del proceso, no solamente la facultad de acudir a la jurisdicción y lograr que se cumpla la plenitud de las formas propias del mismo, sino también la de aducir y pedir la práctica de las pruebas necesarias con el fin de controvertir las de la contraparte y alcanzar la prosperidad de sus pretensiones o defensas, de conformidad con las normas sustanciales".

conservación, disponibilidad e integridad, será valorada por el Juez o Magistrado no como prueba digital sino como prueba testimonial.

Por cuanto es evidente entonces que la prueba o evidencia digital como medio de prueba no podrá constituirse en sí misma como argumento para la solicitud de su práctica anticipada, dada entre otras razones por su exigencia *sine qua non* de disponibilidad futura. Lo que finalmente termina por garantizar tal como lo trae la sentencia anteriormente referenciada, no sólo los derechos fundamentales de acceso a la justicia, el debido proceso y el derecho de defensa o contradicción sino el derecho a la práctica de la prueba con el fin de contradecir las de la contraparte.

Capítulo IV. La valoración de la prueba o evidencia digital como constante en los procesos judiciales.

Hemos llegado al punto cumbre de nuestro texto donde se recoge todo lo descrito anteriormente, esperando que hayan sido herramientas de utilidad para que en este punto los operadores de justicia, rompiendo paradigmas, puedan realizar una inmejorable valoración de la prueba, en este caso de la prueba o evidencia digital. Teniendo como base el concepto de valoración de la prueba que nos entrega NIEVA FENOLL quien la define como "La actividad de percepción por parte del juez de los resultados de la actividad probatoria que se realiza en un proceso"[99]; labor que requiere de toda la atención puesto que de ella dependerá que al final de un caso se haya o no hecho justicia, puesto que será el juzgador quien haya entregado un valor a la misma.

La excelsa labor consiste en poder analizar, evaluar, comprender y entender lo que mediante la articulación de tres fuerzas se quiere demostrar tal como lo manifiesta BENTHAM al manifestar, que la tarea valorativa "necesita de la combinación y la sinergia de tres fuerzas: la propia parte suministradora de toda la información relevante para la defensa de sus intereses en el proceso; la del letrado, capaz de articularla jurídicamente

[99] NIEVA FENOLL, Jordi. *La valoración de la prueba,* Marcial Pons, Ediciones Jurídicas y Sociales, Madrid, 2010, pág. 34.

transformándola de fuentes en medios probatorios válidos y el juez o tribunal, que atribuirá un valor concreto a las diferentes pruebas deducidas ante él."[100]

Tarea que además deberá entregar una seguridad jurídica, "teniendo en cuenta las relaciones de interdependencia entre el sistema jurídico y la realidad social"[101]; realidad social que nos plantea la llegada o mejor la consolidación de las nuevas tecnologías al mundo no sólo social sino jurídico, tal como lo representa en su frase el maestro CANO MARTINEZ "Si la inseguridad jurídica es la norma en un mundo interconectado, la administración de la evidencia digital debería ser la constante"[102].

En un mundo hiperconectado como en el que nos encontramos en la actualidad, donde la mayoría de las labores que realizamos, nuestras comunicaciones, el estudio, nuestro trabajo y las relaciones comerciales en general se realizan a través del uso de los sistemas informáticos, un mundo donde no sólo los seres humanos nos encontramos navegando en el ciberespacio, sino también las cosas (IOT).

Es un nuevo mundo que merece especial atención sobre todo en lo que a regulación se refiere, pues si bien es cierto que a la fecha se cuenta a nivel mundial con diferentes regulaciones acerca de la materia en lo referente a la ciberseguridad, el comercio electrónico y la cibercriminalidad, poca atención se le ha prestado a la forma como se deben probar cada uno de los actos y hechos que se suscitan en cada uno de estos ambientes, en cada jurisdicción del derecho respecto a lo digital.

Esto conlleva inexorablemente a cometer yerros al juzgador respecto a la valoración de la prueba o evidencia digital como medio probatorio independiente y más aún a las fuentes de prueba que allí se contengan, viendo como tras casi cuatro décadas desde que la internet entró en funcionamiento, aún se sigue valorando este tipo de evidencias haciendo uso de equivalencias funcionales y analogías con las evidencias y pruebas físicas, más exactamente las documentales. Cuestión que nos lleva a replantear la forma de valorar este tipo de pruebas o evidencias, comprendiendo inicialmente sus elementos valorativos que se

---

[100] BENTHAM, Jeremy. *Antología (Edición de COLOMER Josep M. Traducciones de HERNÁNDEZ ORTEGA Gonzalo y VANCELLS Montserrat),* Edicions 62, Barcelona, 1991, pág. 4.
[101] BUENO DE MATA, Federico. *Prueba electrónica y proceso 2.0*…op.cit., pág. 257.
[102] CANO MARTINEZ, Jeimy José. *El peritaje informático y la evidencia digital en Colombia, conceptos, retos y propuestas*…op.cit., pág. 53.

encuentran estipulados, tales como, la eficacia, la fuerza, el uso de la razón y la sana crítica; para luego revisar el concepto de libertad probatoria respecto a este controvertido nuevo medio de prueba como lo es el digital.

Es así como a esta altura, en el presente texto ya se han dilucidado diferentes cuestiones tanto técnicas como jurídicas, de modo y de forma acerca de la prueba o evidencia digital, quedándonos por evaluar los elementos que se deberán tener en cuenta para una correcta valoración de la prueba o evidencia digital.

4.1 Elementos valorativos de la prueba o evidencia digital.

Los elementos valorativos de la prueba o evidencia digital corresponden a los mismos elementos que se tienen en cuenta para la valoración de cualquier otra prueba o evidencia diferente a la digital, sin embargo al aparecer un nuevo componente como lo es el componente digital, estos elementos añaden nuevas perspectivas así como nuevos conceptos que permitirán garantizar el cumplimiento de cada uno de los que a continuación se relacionan como lo son la eficacia probatoria, la fuerza probatoria, el uso de la razón y la sana crítica y la libertad probatoria.

En tal sentido DELGADO MARTÍN asiente "Si se cumplen los requisitos de obtención e incorporación de la prueba digital al proceso, está puede desplegar eficacia probatoria, siendo objeto de valoración por parte del juez o tribunal de conformidad con las reglas de la sana crítica (sistema de libre valoración de la prueba)"[103]. Es así como iniciaremos por abordar el primero de los elementos (la eficacia)

4.1.1 Eficacia probatoria.

Antes de aproximarnos a dar un concepto de eficacia probatoria en el ámbito digital, debemos aclarar dos puntos de interés que, si bien se han venido desarrollando a lo largo del texto, será este el momento para identificarlos de forma concreta.

El primer punto hace referencia al documento electrónico como prueba o evidencia digital y el segundo hará referencia a todas aquellas fuentes probatorias que se pueden exponer mediante la prueba o evidencia digital como medio de prueba independiente,

[103] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones…* op.cit., pág 77.

diferente a la prueba documental, que por equivalencia funcional se viene valorando por los tribunales el documento electrónico.

Lo anterior debe comprenderse claramente puesto que de allí deviene que hay que diferenciar entre la eficacia probatoria que se le debe entregar al documento electrónico con base en la normativa actual (es decir con base en la LEC y la ley colombiana 527 de 1999 acompañada del CGP) y la eficacia que se le debe dar a cualquier otra fuente de prueba que pretenda hacerse valer como prueba o evidencia digital.

Es así como la gran mayoría de los autores, a través de la doctrina a la par con los diferentes jueces y magistrados a través de su jurisprudencia, se han limitado a describir los supuestos que se deben tener en cuenta para otorgar no sólo la eficacia a la cual nos referimos, sino la fuerza probatoria respecto del documento electrónico o el mensaje de datos que el mismo pueda contener; creyendo que estos mismos supuestos son aplicables para las demás fuentes digitales contenidas en el medio de prueba digital.

Por lo anterior se deja claro que una cosa es, la eficacia que se le entrega a un documento electrónico a partir de los supuestos de: pertinencia (artículo 281.1 LEC), necesidad o idoneidad (artículo 283.2 LEC), aunados, como lo cita ORTUÑO NAVALÓN, a los presupuestos de autenticidad, exactitud y licitud. Siendo estos últimos los que constituyen el presupuesto de la **eficacia probatoria del documento**[104]**,** (se resalta en negrilla toda vez que es clara su postura que son características del documento); otra muy diferente es la eficacia que se debe entregar a las pruebas o evidencias digitales diferentes al documento electrónico.

Sobre el anterior concepto referente a la eficacia probatoria del documento electrónico como prueba digital versan un gran número de autores, citando un último CANO MARTINEZ quien arguye que “Las pruebas informáticas gozan de una eficacia natural por el simple hecho de ser documentos electrónicos, además del deber existente en cabeza del legislador y del derecho positivo de regular y determinar el alcance de cada una

[104] ORTUÑO NAVALON, María del Carmen. *La prueba electrónica ante los tribunales*… op. cit, pág. 110.

de ellas"[105] dando a entender que el alcance que otorga lo positivo del derecho, no es óbice para eliminar la prueba que reposa en el documento electrónico.

Cada uno de los autores refieren tres garantías frente a la eficacia probatoria del documento electrónico que deben respetarse para otorgar dicha eficacia. Son ellas, la autenticidad, la integridad y la licitud, además de las que se garantizaron previamente para su admisibilidad. Entendiendo que estas garantías siempre han versado sobre el supuesto de que toda prueba o evidencia digital se asemeja a un documento, a continuación, se hará el comparativo frente a estas mismas garantías, pero frente a la prueba o evidencia digital, diferente al documento electrónico.

Al revisar el tema desde la normativa, vemos que la ley colombiana 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, en sus artículos del 10 al 12 versa sobre el tema. Sin embargo, al analizarse la norma se evidencia una clara contraposición de cada uno de estos artículos en lo que a prueba o evidencia digital se refiere.

Si bien pueden llegar a adecuarse al documento electrónico como prueba, no sucede igual para las demás fuentes de prueba digital, incluyendo el mensaje de datos contenido en un mensaje de correo electrónico o un sistema de mensajería como WhatsApp.

Iniciemos por el artículo 10 que un su párrafo segundo cita "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" [106]

Se hace referencia y da a entender de forma precisa que, si un mensaje de datos no es presentado como prueba o evidencia digital que es su forma original, sino que el mismo es

[105] CANO MARTINEZ, Jeimy José. *El peritaje informático y la evidencia digital en Colombia, conceptos, retos y propuestas*…op.cit., pág. 79-80.

[106] Ley 527 de 18 de agosto de 1999. Diario Oficial No. 43.673/ 21 agosto /1999, op.cit, Artículo 10. admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

presentado en un documento físico, es decir, impreso en un papel, no se le podrá negar eficacia, e incluso adelantándonos un poco, tampoco se le podrá negar fuerza probatoria.

Lo anterior no tiene ningún sentido, incluso si lo que se pretende probar es el simple documento electrónico. Y así lo estipula la misma ley 527/99 en su artículo 11, en una clara contraposición a lo antedicho en el artículo 10 cuando cita "Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente."[107]

Situación que no se comprende si se tiene en cuenta que lo que se conservó en el medio digital puede ser susceptible de modificación sin que sea perceptible al ojo humano, diferente a lo que sucede con un documento físico, es decir impreso o manuscrito; situación que a toda luz en un documento impreso que intente representar lo que fue generado en el medio digital, es improbable puesto que no habrá forma de lograr tal supuesto, independiente de que este tenga impresa una supuesta firma electrónica que en todo caso se desconoce si corresponde a lo que se trajo del ambiente digital (característica de integridad que se abordará en el siguiente apartado), también se hará referencia a la forma en la que se identifique a su autor o iniciador.

Todo lo expuesto en el párrafo anterior se termina por corroborar con el análisis que podemos hacer del artículo 12 de la misma ley 527/99 en su tercer y cuarto párrafo nos acota respecto a la conservación de los mensajes de datos y documentos "Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y que se conserve, de haber alguna, toda

[107] Ley 527 de 18 de agosto de 1999. Diario Oficial No. 43.673/ 21 agosto /1999, op.cit, Artículo 11 criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento"[108].

Artículo que por sí mismo trae las exigencias frente a la exactitud de la información donde se permitan determinar datos como la hora, la fecha, el autor, su destinatario, cosa que será inviable mediante una representación simulada y trasladada de su ambiente natural (el digital) a un ambiente irreal que no proyecta con exactitud y mucho menos entrega las tres garantías antes nombradas y a las cuales nos referimos a continuación iniciando con la Integridad.

En el mismo sentido encontramos que en la normativa española se exigen los mismos tres requisitos para la prueba o evidencia digital tal como lo trae la LECRIM, en su artículo 588 sexies c1 al referirse a la integridad cita "Fijará también las condiciones necesarias para asegurar la **integridad de los datos y las garantías de su preservación** para hacer posible, en su caso, la **práctica de un dictamen pericial**"[109]. Situación que hace evidente que se hace necesaria la pericial informática para garantizar la integridad y eventualmente llegar a determinar el autor. Por su parte, la LEC, en su artículo 382 versa sobre el tema[110] en una clara contraposición a lo versado en la LECRIM, puesto que al igual que la ley 527/99 de

[108] Ley 527de 18 de agosto de 1999. Diario Oficial No. 43.673/ 21 agosto /1999, op.cit, artículo 12 conservación de los mensajes de datos y documentos. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones: Que la información que contengan sea accesible para su posterior consulta. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento. No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos. Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

[109] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, Artículo 588 sexies c. Autorización judicia**l.** La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

[110] Artículo 382. Instrumentos de filmación, grabación y semejantes. Valor probatorio. 1. Las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes. Al proponer esta prueba, la parte deberá acompañar, en su caso, transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso. 2. La parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido. 3. El tribunal valorará las reproducciones a que se refiere el apartado 1 de este artículo según las reglas de la sana crítica.

Colombia no quita valor ni eficacia probatoria si los medios de prueba presentados por la parte demandante a pesar de que sean digitales se presentan en un formato distinto, e incluso da la posibilidad de demostrar a ambas partes la autenticidad o no posterior a la impugnación de la prueba[111].

Esta situación va en contra del principio de control de convencionalidad que en todo caso recae sobre la magistratura y si se traslada a la jurisdicción penal faltaría al principio de presunción de inocencia, el cual deberá ser vencido por parte del Estado, por lo que es en este último en el que recae la carga de la prueba y deberá demostrar y brindar las garantías de las que versa el articulo 588 sexies C1 al cual ya se hizo referencia, desde el inicio de la adquisición de la prueba ya que de lo contrario la prueba deberá decretarse ilegal por falta de los requisitos legales.

Por todo lo anterior queda claro que una cosa es la eficacia que por equivalencia funcional se pueda llegar a otorgar, con algunos reparos de los que se han venido hablando, al documento electrónico y otra la eficacia evaluada desde la prueba o evidencia digital como medio independiente. Ahora pasemos a entender los elementos que entregan eficacia probatoria a la prueba o evidencia digital.

4.1.1.1 Autenticidad.

La autenticidad de la prueba electrónica estará dada por la determinación de su autor, así lo acuña ORTUÑO NAVALON al señalar que la garantía de autenticidad "supone la identificación de la autoría del documento y del contenido que este refleja"[112]. Pues bien, esta garantía en el documento electrónico la puede entregar la firma electrónica del autor la

[111] STS nº 300/2015, de 19 de mayo de 2015, FJ 4º, (RJ 2015\1920) aquí el aparte …" Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido"

[112] ORTUÑO NAVALON, María del Carmen. *La prueba electrónica ante los tribunales*… op. cit, pág. 111.

cual será proporcionada por una entidad certificadora o un tercero certificado según lo normado en la ley colombiana 527/99 y la Ley 59/2003, de firma electrónica.

Hasta aquí no existe problema alguno más que el supuesto firmante aduzca no corresponderse e impugne la autenticidad del documento, por lo que, quien aporta la prueba deberá demostrar que la firma es auténtica, acudiendo en todo caso a una pericial informática que deberá demostrar que el dispositivo electrónico asignado o destinado para tal fin no fue vulnerado, mientras la parte que impugna, podrá demostrar lo contrario y que además mediante dicha vulneración obtuvieron sus credenciales para el acceso al sistema de firma electrónica que bien sea dicho de paso se corresponderá funcionalmente con la firma manuscrita, por cuanto es deber de cuidado, reserva y resguardo por parte de quien la tenga asignada. Por ello en el documento electrónico que goza de firma electrónica la autenticidad se presume.

Cuestión diferente sucede con la prueba o evidencia digital, como por ejemplo los mensajes de WhatsApp, los mensajes en redes sociales, los logs de auditoría, la meta data, las fotografías, los videos entre otras fuentes de prueba digital, las cuales si bien se les puede demostrar su integridad (siguiente apartado) difícilmente se podrá garantizar su autor, por cuanto a diferencia del documento electrónico donde el autor se presume de facto, en este tipo de prueba o evidencia digital la autoría de la fuente digital estará en duda y ésta no se puede presumir.

Se deberá entonces trasladar la garantía de autenticidad de la prueba digital a la identificación del dispositivo donde se encuentra almacenada la evidencia o prueba digital, o desde donde fue enviada, demostrando que la prueba o evidencia digital que se pretende hacer valer es auténtica respecto al dispositivo electrónico que contiene el medio de almacenamiento de donde se produjo su recolección, más no frente al autor humano que la produjo.

Al respecto y haciendo referencia a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia española[113], DELGADO MARTÍN resalta “En el ámbito de la prueba electrónica, cabe

[113] Anexo definiciones de la ley 18/2011, Define autenticidad como: “ propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos”

definirse como la propiedad o característica consistente en que se garantiza la autenticidad del origen de los datos, es decir, se garantiza la fuente de la que proceden los datos"[114]. Abordada esta garantía, procedemos a definir quizás la garantía más importante en lo que refiere a la prueba o evidencia digital: la integridad.

4.1.1.2 Integridad y disponibilidad futura.

Abordaremos ahora una garantía que conlleva a otorgar como valor añadido una adicional. Se trata de la garantía de integridad, que conlleva a garantizar la disponibilidad de la prueba o evidencia digital a futuro. Debemos aclarar que, para garantizar este supuesto al documento electrónico, el mismo además de llevar la firma electrónica que garantiza la autenticidad desde su autor, deberá ir firmado digitalmente, concepto que se desarrolló en el título I del presente texto. De lo contrario, difícilmente se podrá entregar esta garantía respecto de este tipo de documentos.

Ahora bien, con referencia a las demás pruebas o evidencias digitales, esta garantía no es diferente y debemos conceptualizarla como aquélla que permite conservar el contenido de la prueba o evidencia digital incólume, por cuanto la integridad corresponderá entonces a la certificación de que el contenido de la prueba digital no ha sido alterado, modificado, eliminado, adicionado o en general, que la prueba se conserva en su estado original, el mismo que tenía al momento de su recolección y aseguramiento y que esta no ha sido manipulada.

Al respecto DELGADO MARTÍN define la integridad desde la concepción del documento electrónico refiriéndose a la misma como prueba electrónica, pero que al tratarse de una garantía que aplica indistintamente para ambas es más que acertada, "por integridad de la prueba electrónica cabe entender la propiedad o característica consistente en que los datos (activo de información) no han sido alterados de manera no autorizada. En definitiva, se trata de aplicar la construcción de la cadena de custodia a este ámbito: la preservación de los datos"[115] .

[114] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones…* op.cit., pág 82.
[115] Ibidem pág. 82.

Tomando como base lo dicho por DELGADO MARTÍN es preciso aclarar el concepto de cadena de custodia, el cual ya ha sido ampliamente desarrollado por la jurisprudencia y a la cual ya hemos hecho referencia durante el escrito y sólo por citar alguna otra hacemos referencia a la STS 777/2013, de 7 octubre[116].

Decimos que es preciso aclarar que para la prueba o evidencia digital per se no se corresponderá al mismo formato físico de los demás medios de prueba, es decir la cadena de custodia en el ámbito digital, no corresponderá al documento ya conocido impreso en una hoja de papel y diligenciado por los intervinientes o por quienes hayan tenido contacto con la prueba.

En este caso la cadena de custodia digital corresponderá a la firma digital que al momento de su recolección tal como lo plantea el estándar internacional ISO 27037.Y deberá generar el perito (o quien haga sus veces) mediante un algoritmo o Código HASH[117] que garantice la no modificación del contenido de la prueba o evidencia digital.

4.1.1.3 Licitud respeto a la intimidad digital y del propio campo virtual.

Tal como se referenció en el Capítulo I. Admisibilidad de la prueba o evidencia digital, del presente título, la licitud de la prueba o evidencia digital estará dada por el respeto a los derechos fundamentales en el momento de su obtención. PINTO PALACIOS y PUJOL CAPILLA lo presentan afirmando que "Toda prueba que se obtenga con

---

[116] STS nº 777/2013, de 7 octubre de 2013, FJ 7º, (RJ 2013\7891) cita … "La cadena de custodia sirve para acreditar la "mismidad" del objeto analizado, la correspondencia entre el efecto y el análisis o informe, su autenticidad. No es presupuesto de validez sino de fiabilidad. Cuando se rompe la cadena de custodia no nos adentramos en el campo de la ilicitud o inutilizabilidad probatoria, sino en el de la menor fiabilidad (menoscabada o incluso aniquilada) por no haberse respetado algunas garantías. Son dos planos distintos. La ilicitud no es subsanable. Otra cosa es que haya pruebas que por su cierta autonomía escapen del efecto contaminador de la vulneración del derecho (desconexión causal o desconexión de antijuricidad). Sin embargo la ausencia de algunas garantías normativas, como pueden ser las reglas que aseguran la cadena de custodia, lo que lleva es a cotejar todo el material probatorio para resolver si han surgido dudas probatorias que siempre han de ser resueltas en favor de la parte pasiva; pero no a descalificar sin más indagaciones ese material probatorio".

[117] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones…* op.cit., pág 83, entrega una concreta definición del algoritmo HASH aduciendo …" Se trata de un algoritmo matemático que se realiza sobre el conjunto de os datos contenidos en un concreto dispositivo o soporte digital: el resultado genera un valor de 32 o más dígitos de tal forma que, si se modifica un solo bit del conjunto de datos sobre el que se ha realizado, el valor del hash es diferente". A continuación, se deja la url donde se puede generar en línea un algoritmo HASH a una prueba o evidencia digital: https://md5decrypt.net/en/Sha512/ .

vulneración de derechos fundamentales ha de reputarse nula. Esta nulidad, en principio, se extiende a todas las demás pruebas que se obtienen gracias al acto previo legítimo"[118].

Pues bien, esta garantía o presupuesto en el ámbito digital va más allá de los derechos fundamentales clásicos, debiéndose llevar por la misma naturaleza de la prueba a la evaluación de derechos fundamentales digitales y a los lugares virtuales que la aplicación de estos trae consigo. Así lo representa ORTUÑO NAVALON al sostener que "La doctrina ha sostenido la aparición de lo que se denomina una "tercera generación" de derechos fundamentales, que vendría integrada por las garantías del ciudadano frente a los ataques a sus libertades procedentes de las nuevas tecnologías; y así se califican como "libertades informáticas" al conjunto formado por el derecho al secreto de las comunicaciones informáticas y telemáticas, la intimidad informática y el derecho a la autodeterminación informativa."[119]

Es así como si de una orden de entrada y registro lícitamente obtenida se desprendiera que en la práctica del registro se hallaren dispositivos electrónicos que pudiesen contener medios de almacenamiento con información de tipo digital, se deberá contar con una orden de registro a estos dispositivos como domicilio virtual.

De ahí que el ingreso a cada red social y a cada buzón de correo deberá garantizarse mediante una orden que en todo caso cumpla con los requisitos de necesidad, pertinencia, utilidad y proporcionalidad que permitan tomar una medida restrictiva de derechos fundamentales, más allá de que el acceso a esas redes o buzones de correo esté predeterminado por el usuario. Esto no querrá decir que él mismo esté permitiendo su ingreso, en el entendido que él y nada más que él es quien conoce y tiene la potestad de ingreso al domicilio virtual inicial dentro del cual pueden encontrarse otros domicilios virtuales (facultad qué solo es viable en el ciberespacio).

Respecto de lo versado anteriormente, la STS 204/2016, de 10 de marzo (Sala de lo Penal, Sección 1ª) haciendo referencia, al derecho a la intimidad personal, a los dispositivos digitales de almacenamiento masivo de información, a su acceso, además de los distintos ámbitos de protección que reciben un tratamiento unitario, así como al derecho

[118] PINTO PALACIO, Fernando y PUJOL CAPILLA, Purificación. *La prueba en la era digital,* Wolters Kluwer, Madrid, 2017, Pág 155.
[119] ORTUÑO NAVALON, María del Carmen. *La prueba electrónica ante los tribunales*… op. cit, pág. 88.

constitucional de nueva generación constitutivo de una protección del propio entorno virtual[120]. Expresa que el derecho a la intimidad es un derecho que al igual que el de la protección al propio entorno virtual no es absoluto.

Sin embargo, cuando nos referimos al propio entorno virtual o digital, entendiendo este como aquel entorno donde se dispone de datos e información de carácter reservada e íntima que no sólo puede llegar afectar a la persona dueña del dispositivo de almacenamiento digital sino a terceros que se relacionen dentro de esa información, como lo son fotografías, conversaciones, entre otras, tal procedimiento de acceso al medio de almacenamiento y registro a las fuentes de información que allí se encuentran alojadas hace inviable técnicamente la posibilidad de no llegar a conocer otros datos e información que nada tengan que ver con el hecho de la causa.

A pesar de que en la legislación colombiana la implementación y la regulación de los derechos fundamentales digitales no ha sido adoptada, en la actualidad el CPP en su artículo 236[121] faculta al ente investigador para la recolección de la información dejada al

[120] STS nº 204/2016 de 10 de marzo de 2016, F.J. 11º, (RJ 2016/11142), entre muchos otros fundamentos jurídicos se toma el siguiente …"La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital."

[121] Ley 906 de 31 de agosto de 2004 "Por la cual se expide el Código de Procedimiento Penal", Artículo 236. Recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones**.** Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; 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 aplicables analógicamente, 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. PARÁGRAFO. Cuando se trate de investigaciones contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la Policía Judicial dispondrá de un término de seis

navegar por internet y otros medios semejantes, de donde se puede deducir que esos otros medios hacen referencia a lo que hace referencia el propio entorno virtual y la intimidad digital a la que nos hemos referido.

Es así como, con relación a la presente cuestión, el acceso y posterior registro y análisis de las fuentes de información es restrictiva de los derechos a la privacidad de la información y los datos, el de la intimidad e incluso el de domicilio digital. Sin embargo, estas actuaciones son permitidas bajo ciertas condiciones o normas tal como lo trae, el citado artículo. No obstante, es de resaltar que tal como versa el mismo artículo 236, el hecho de incautar los dispositivos dentro del registro al bien inmueble no faculta al acceso a la información; por cuanto se deberá solicitar una orden diferente para realizar la citada actuación.

Cabe resaltar que de la misma manera deberá ser aplicada la norma, cuando el dispositivo electrónico o el medio de almacenamiento físico sea obtenido de manera diferente a un acceso al domicilio. En todo caso los agentes de policía judicial deberán comunicar al fiscal en la legislación colombiana y al juez instructor en la española, tanto de las actuaciones de incautación como de la solicitud, de ser pertinente, para el acceso a estos. Frente a este tema y haciendo uso del derecho comparado en la legislación española encontramos la LECRIM en su artículo 588 sexies a 1. y 588 sexies a 2, al igual que el 588 sexies B C 1 y 2 .

4.2 Fuerza probatoria, uso de la razón y la sana crítica frente a la prueba o evidencia digital.

La fuerza probatoria en sentido estricto hace referencia tal y como nos lo presenta LÓPEZ "a la operación mental que hace el juez para formar su convicción a partir de los medios de prueba aportados al proceso".[122] Medios de prueba dentro de los cuales aparece la prueba o evidencia digital, acerca de la cual nos ilustra el Consejo de Estado Colombiano en su sentencia radicado 76001-23-33-000-2015-01577-01 donde refiere respecto al uso de la fuerza probatoria en relación con un mensaje de datos que "Para la valoración de la

(6) meses en etapa de indagación y tres (3) meses en etapa de investigación, para que expertos en informática forense identifiquen, sustraigan, recojan, analicen y custodien la información que recuperen.

[122] CARRASCOSA LÓPEZ, Valentín. Valor probatorio del documento electrónico. *Informática y Derecho: revista iberoamericana de Derecho informático*, 1995, no 8, pág. 139.

fuerza probatoria de los mensajes de datos a que se refiere esta ley (527/99 en su artículo 11), se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente".[123]

Es así como dentro de ese ejercicio mental el juez debe hacer uso de la razón y la sana crítica, entendiéndose esta desde la aplicación de las tres reglas fundamentales que la componen, como lo son, las reglas de la lógica, las máximas de la experiencia y el conocimiento científico afianzado, sin dejar al libre albedrío tal razonamiento, ya que de lo contrario nos encontraríamos frente a la libre convicción del juzgador (apartado siguiente) y no frente al uso de la razón y la sana crítica, tal como no lo presenta la sentencia de la Corte Constitucional Colombiana C-202/2005[124].

Al respecto de estas tres reglas HUNTER AMPUERO manifiesta "Ninguna de estas tres directrices es suficiente por sí misma. La corrección lógica de la valoración probatoria no excusa del error ni de la injusticia cuando se aplica aisladamente. Las máximas de la experiencia son esencialmente mutables, en tanto la experiencia humana es también forzosamente variable, y por ello tampoco escapan del error. El conocimiento científicamente afianzado, por último, aunque respaldado por la objetividad, tampoco es infalible" "Una correcta ponderación de acuerdo con la sana crítica implica necesariamente una conjugación de estas reglas"[125].

---

[123] Sentencia 76001-23-33-000-2015-01577-01, de 17 de marzo de 2016, Sección quinta de la Sala de lo Contencioso Administrativo del Consejo de Estado Colombiano, F.J. 5.2.

[124] Sentencia C-202/2005 de 08 de marzo de 2005, FJ 5, (D-5336) frente al uso de la razón y la sana crítica refiere "Las reglas de la sana crítica son, ante todo, las reglas del correcto entendimiento humano. En ellas interfieren las reglas de la lógica, con las reglas de la experiencia del juez. Unas y otras contribuyen de igual manera a que el magistrado pueda analizar la prueba (ya sea de testigos, peritos, de inspección judicial, de confesión en los casos en que no es lisa y llana) con arreglo a la sana razón y a un conocimiento experimental de las cosas" ( ) …" "El juez que debe decidir con arreglo a la sana crítica, no es libre de razonar a voluntad, discrecionalmente, arbitrariamente. Esta manera de actuar no sería sana crítica, sino libre convicción"

[125] HUNTER AMPUERO, Iván. "Control judicial de las reglas de la sana crítica (Corte Suprema)", *Rev. derecho (Valdivia)*, 2012, vol.25. nº 1, pág 247.

Analizando cada una de las máximas que nos presenta HUNTER AMPUERO frente al uso de la razón y la sana crítica, refiriéndonos a la prueba o evidencia digital tendremos que decir:

Primero: Mediante un "examen lógico" referente a la prueba o evidencia digital no se puede llegar a valorar la misma en su totalidad puesto que se trata de una prueba o evidencia de especial característica que no basta con aplicar la "lógica"[126], ya que la integridad de esta prueba no admite un grado de incertidumbre puesto que el método utilizado para garantizar tal característica se hace científicamente inalterable, ahora bien si nos referimos a la autenticidad la misma siempre va tener un grado de incertidumbre, por cuanto se concluye entonces que la integridad de la prueba o evidencia digital siempre deberá ser razonada con un alto grado de certeza desde la lógica pero con un alto grado de incertidumbre frente a su autenticidad, entendiendo esta última desde el autor.

Segundo: Basados en las "máximas de la experiencia" y entendiéndolas desde la definición que nos trae DEVIS HECHANDÍA representándolas como "un criterio objetivo, interpersonal o social ... que son patrimonio del grupo social … de la psicología, de la física y de otras ciencias experimentales"[127], debemos decir que la prueba o evidencia digital pertenece claramente a las ciencias de la ingeniería, desde el ámbito del uso de las TICS (Tecnologías de la información y las comunicaciones), por consiguiente será deber inequívoco del juzgador al momento de valorar este tipo de prueba hacer uso de esta máxima que unida al conocimiento científico será las que finalmente den claridad sobre su correcta apreciación y valoración aplicando el uso de la razón y la sana crítica.

Tercero: hacemos referencia al "conocimiento científico afianzado" que junto al punto anterior forman parte de las máximas *sine qua non* a aplicar en la valoración de la prueba o evidencia digital, mediante el uso de la razón y la sana crítica probatoria, puesto que para este nuevo tipo de prueba es necesario tener conocimientos técnicos especiales

[126] Según el significado que trae la RAE. Lógica que, a semejanza del raciocinio natural, admite una posibilidad de incertidumbre en la verdad o falsedad de sus proposiciones, Recuperado de la url: https://dle.rae.es/l%C3%B3gico el 21 de mayo de 2020.
[127] DEVIS HECHANDÍA, Hernando. *Teoría General de la Prueba Judicial*, Editorial Zavalia, Buenos aires, 1981, pág. 336.

que como lo manifiesta HUNTER AMPUERO "han sido respaldados por el mundo científico, por su propia naturaleza en este caso la naturaleza digital"[128].

Por lo anterior debemos decir que hay una realidad que no se puede negar respecto a este método de valoración que unido al que trataremos en el siguiente apartado (libre valoración de la prueba), es desconocido en la actualidad por la gran mayoría de juzgadores, que poco o ningún conocimientos técnico o científico tienen que les permitan valorar adecuadamente la prueba o evidencia digital "con base en su conocimiento privado, las características informáticas de los distintos dispositivos tecnológicos que compongan el acervo probatorio", tal como lo cita ORTUÑO NAVALON[129].

Respecto de la fuerza probatoria que entrega el uso de la razón y la sana crítica en relación con la prueba o evidencia digital, ABEL LLUCH señala dentro de las tres posturas doctrinales a las cuales hace referencia[130], una en particular, que, en consonancia con la postura adoptada desde el inicio del presente escrito, versa sobre la prueba o evidencia digital como "naturaleza especialísima", por cuanto el uso de la razón y la sana crítica así debe de ser contemplada "especial". Este mismo sector exige al tribunal prestar especial atención no sólo a las cuestiones técnicas de la prueba o evidencia digital sino a sus características que entregan eficacia probatoria como lo son la integridad, autenticidad y licitud a las cuales ya nos referimos ampliamente.

De tal manera que al respecto del uso de la razón y la sana crítica, esta deberá ser limitada, sin salirse de los parámetros clásicos de sus reglas (de la lógica, las máximas de la experiencia y el conocimiento científico) apoyándose de las propias conclusiones que se

---

[128] HUNTER AMPUERO, Iván. "Control judicial de las reglas de la sana crítica (Corte Suprema)", *Rev. derecho (Valdivia)…*op.cit., pág. 47.

[129] ORTUÑO NAVALON, María del Carmen. La prueba electrónica ante los tribunales… op. cit, pág. 258.

[130] ABEL LLUCH, Xavier, juicio de admisión de la prueba electrónica, en: ABEL LLUCH, Xavier y PICÓ I JUNOY, Joan, La prueba electrónica…op. cit, pág. 169-172. Define además estos dos sectores doctrinales: un primer sector que sostiene que por la naturaleza de la prueba no se aporta nada nuevo, ya que las reglas de la sana crítica, por definición hará referencia siempre a un caso en concreto, tratándose entonces de una redundancia cuando se hable de la prueba digital "por la naturaleza especial". Un segundo sector por su parte plantea que la expresión "según su naturaleza" permite distinguir dos tipos de pruebas digitales, uno que trata de los documentos electrónicos que han sido trasladados de la realidad física a la digital como lo son por ejemplo los documentos electrónicos y los mensajes de datos que se contengan en él, que permitirán aplicar la valoración desde la sana crítica que plantea el artículo 319 y 326 de la LEC respecto a los documentos públicos y privados y la ley 527/99 Colombiana; y un segundo grupo que refiere a los instrumentos informáticos que debieran ser valorados respecto a la equivalencia funcional de los mismos, por ejemplo los medios audiovisuales y a los que se deben aplicar las mismas reglas de valoración de las que versa el artículo 382 LEC y CGP.

presenten de la pericia informática[131]. Por consiguiente, la fuerza probatoria que se le otorgue a la prueba o evidencia digital estará dada por el uso de la razón y la sana crítica basada en las características propias de la especialidad de la prueba (autenticidad, integridad y veracidad, además de la licitud).

4.3 Libertad probatoria respecto de la prueba o evidencia digital.

Las leyes procesales colombiana y española se rigen en mayor medida por el otorgamiento de la libre valoración probatoria que se les otorga a los juzgadores (Jueces y Magistrados) y salvo excepciones legales que así lo determinen por el sistema legal o tasada, sin que esto quiera decir al igual que en el uso de la razón y la sana crítica que los juzgadores tengan total discrecionalidad, tal como lo explica DELGADO MARTÍN al definir la prueba legal y el sistema de prueba libre de la siguiente manera:

"Las pruebas legales son aquellas en las cuales la ley señala por anticipado al juez el grado de eficacia que debe atribuir a determinado medio probatorio" es decir que un hecho debe o no ser declarado por el juez con base en la conclusión fáctica que entrega la propia ley. "Prueba libre, el juez realiza esa valoración según las reglas de criterio racional; lo que no significa pura discrecionalidad o arbitrariedad, sino que los criterios aplicados por el juez han de recogerse en la motivación de la sentencia".[132]

Respecto al tema de la libre valoración probatoria de la prueba o evidencia digital, DELGADO MARTÍN lo aborda dando respuesta en cinco puntos al interrogante ¿qué significa la libre valoración de la prueba electrónica digital? En los mismos términos refiere básicamente a que la libertad probatoria del juez estará supeditada a las reglas del uso de la razón y la sana crítica, puesto que la especialidad técnica y tecnológica de esta, difícilmente permitirá al juez encontrar una racionalidad distinta a lo que arroje un resultado pericial respecto de la integridad y la autenticidad de la prueba o evidencia digital.[133]

---

[131] DE URBANO CASTRILLO, Eduardo. *La valoración de la prueba electrónica,* Tirant Lo Blanch, Valencia, 2009, pág. 120-121.

[132] DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones…* op.cit., pág 78.

[133] Ibidem, pág. 79. Respecto al interrogante ¿qué significa la libre valoración de la prueba electrónica digital? …"en primer lugar, la ley no obliga al juez a tener por probados los hechos que surjan de una prueba digital" ( )…"En segundo lugar, significa que la ley no determina que la prueba electrónica, solamente puede tener eficacia probatoria si se cumplen ciertos presupuestos legales" ( )…"En tercer lugar, también quiere decir que el juez valorará la prueba electrónica conforme a las reglas de la sana crítica, según la naturaleza del soporte"

Al respecto de lo planteado por DELGADO MARTÍN se debe hacer precisión en su planteamiento segundo donde a pesar que la ley a la fecha no plantea ninguna normativa que permita dar eficacia a la prueba digital no es menos cierto que la jurisprudencia tal como se desarrolló en el capítulo I del presente Titulo ya se ha pronunciado al respecto y guardando el respeto por el bloque de constitucionalidad da cabida a la aplicación obligatoria de los estándares internacionales para la recolección y preservación de la evidencia digital.

Por otra parte si del hecho se deduce que sólo la prueba digital puede dar fe de la ocurrencia del mismo se deberá garantizar la eficacia probatoria de esta, es decir su rigurosa apreciación desde la integridad y autenticidad que puede o no derivar en la veracidad de los hechos objeto del litigio, por consiguiente la libertad probatoria del juez respecto a la motivación de la sentencia no se podrá fijar solamente en su racionalidad, en el sentido común que pueda él representarse frente a la prueba o evidencia digital y en todo caso deberá ante el reducido conocimiento técnico- científico que pueda tener acerca de la materia, apoyarse en la prueba pericial informática que para este medio de prueba deberá ser de obligatorio cumplimiento, siendo este el medio de prueba más idóneo para dar certeza al juzgador de las garantías de la prueba o evidencia en cuestión.

4.4 Apreciación en conjunto de la prueba o evidencia digital desde la autenticidad, la integridad, la veracidad y la autoría.

La prueba o evidencia digital goza de unas características técnicas especialísimas que incluso difícilmente permite conocer la autoría de estas, de allí que surja la importancia de la valoración de la prueba o evidencia digital en conjunto, puesto que no se advierte de que manera se pueda probar la autoría de una prueba o evidencia digital, salvo que la parte dentro de un proceso civil, laboral, mercantil entre otros acepte de facto su autoría. O en el ámbito penal se produzca una captura del ciberdelincuente en flagrancia lo que difícilmente puede suceder en el mundo virtual.

( )…"En cuarto lugar, el alto componente tecnológico de la prueba electrónica determinará con frecuencia la importancia de los conocimientos científicos en su valoración" ( )…"En quinto lugar, en la valoración conforme a la sana crítica el juez habrá de tener en cuenta la postura procesal de cada una de las partes en relación con la concreta prueba electrónica".

Es así como MORA DÍAZ conceptualiza la necesidad de valorar la prueba en conjunto como "La valoración de la prueba digital de un concreto proceso ha de ser apreciada en relación con el valor probatorio de las restantes pruebas practicadas"[134]. Aunque su valoración debe ser individual e independiente a los demás medios de prueba, su apreciación siempre deberá hacerse en conjunto, lo anterior si se tiene en cuenta que la autoría siempre tendrá un asomo de duda razonable, y es por ello que la autenticidad de la prueba o evidencia digital se entiende desde el medio o dispositivo del cual se recolecto y no desde su autor.

Respecto a la valoración de la prueba o evidencia digital, se ejemplifica con la sentencia 69/2017 de la AP Barcelona Sección 18ª [135], donde se referencian unos mensajes de WhatsApp los cuales al momento de tenerse en cuenta para el fallo se apreciaron en conjunto con otros medios de prueba, entre los que se observa el interrogatorio, sin embargo, al reparo debe decirse que la prueba digital para este caso (los mensajes de whatsapp), no debieron haber sido tomados en cuenta por carecer de las garantías de integridad y autenticidad.

Por último, traemos a colación la sentencia T-043/2020 del 10 de febrero de 2020 proferida por la corte constitucional colombiana, donde deja más que claro que la prueba o evidencia digital que para el caso se resume en mensajes de whatsapp obró únicamente como prueba indiciaria, puesto que el sentido o mejor la motivación de la sentencia se concretó mediante la valoración de los medios probatorios en conjunto.[136]

---

[134] MORA DÍAZ, Rocío. "La valoración de la prueba en soportes informáticos". *El derecho, noticias jurídicas.* 2004, nº 20, pág 15.

[135] SAP nº 69/2017 de 31 de enero de 2017, F. J. 3º, (JUR 2017\106183) entre otras versa "De esta forma, la sentencia recurrida entendemos que ha valorado con corrección la prueba electrónica en conjunción con el resultado del interrogatorio de ambas partes y específicamente el de la Sra. Inocencia y acierta al considerar acreditado que existía relación entre la misma y el demandante al tiempo de la concepción del menor cuya filiación se reclama en el proceso."

[136] Sentencia nº T- 043/20 de 10 de febrero de 2020, F. J. 53, (T-7.461.559) en su fundamento jurídico 53 refiere…"En relación con los diferentes medios de prueba obrantes en el expediente y que fueron valorados por la Sala, debe precisarse que si bien la accionante allegó diferentes capturas de pantalla de conversaciones sostenidas en la aplicación WhatsApp, las cuales presentan un valor de prueba indiciaria, conforme lo señalado en precedencia (supra 21), estos elementos fueron analizados de forma conjunta con los demás rudimentos probatorios, entre ellos, el derecho de petición, el número de estudiantes matriculados en el 2018, y las razones ofrecidas por la accionada para no contratar nuevamente a la señora Dora Patricia Ramírez Monsalve, lo cual permitió estructurar el razonamiento efectuado en esta providencia"

CONCLUSIONES

PRIMERA: Tanto en la legislación española como en la colombiana, los documentos y firmas electrónicas como los digitales y los documentos virtuales, pertenecen a la categoría de prueba o evidencia digital y así deben ser tratados los datos y la información contenidos en ellos.

SEGUNDA: A raíz de la investigación efectuada, considero que el equivalente funcional de la prueba o evidencia digital sólo puede otorgarse al documento electrónico siempre y cuando cumpla los requisitos funcionales del documento físico.**(ver anexo 1)**.

TERCERA: La aparición de nuevas fuentes probatorias dentro de la categoría de la prueba o evidencia digital hace que los operadores de justicia, además de romper paradigmas frente a la equivalencia funcional de la prueba digital, se cuestionen frente a la necesidad de presentar alternativas que conlleven a la regulación de las prácticas de la prueba digital, en especial cuando se trate de IA y técnicas OSINT.

CUARTA: Pienso que resulta imperativo legislar frente a la unificación de la manera de recolectar la prueba o evidencia digital en cada uno de los medios de almacenamiento tanto físicos como virtuales. Mientras esto sucede se deben de emplear los instrumentos internacionales que versan sobre la materia.

QUINTA: El concepto de prueba o evidencia digital, su tratamiento, interpretación y valoración, se han venido realizando, en mi opinión, de manera errónea respecto a las fuentes jurídicas vigentes sobre el tema, respecto aquellas pruebas o evidencias digitales diferentes al documento electrónico. Es más, la legislación ha llegado a verse obsoleta al definir y enmarcar los presupuestos que deben cumplirse desde lo procesal para el tratamiento especial que requiere este tipo de prueba o evidencia, conformándose con aplicar la definición y los requisitos legales de los documentos impresos, tanto públicos como privados, para equipararlos al documento electrónico. Esto, aunque hoy sea viable y jurídicamente correcto, no se adapta al avance de la tecnología ni al surgimiento de las nuevas fuentes de prueba digital que siguen siendo equiparadas con la valoración y el tratamiento que se le da al documento físico.

SEXTA: La prueba o evidencia digital no deberá solicitarse como prueba anticipada, puesto que la misma deberá traer intrínseco la garantía de disponibilidad futura y en todo caso no se advierte riesgo alguno de perdida si dentro de las labores previas de recolección de esta se respetan los protocolos y estándares para la identificación, recolección y preservación, garantizando desde ese mismo instante su integridad. Por cuanto no se advierte la necesidad de su práctica anticipada, salvo que existan razones o causas suficientemente justificadas.

SÉPTIMA: La integridad de la prueba o evidencia digital será garantizada por la firma digital (HASH), mientras la autenticidad desde la autoría, sólo se puede otorgar de facto al documento electrónico si este tiene impresa la firma electrónica asignada al autor. Por otra parte, en la prueba o evidencia digital, la autenticidad del medio de prueba digital la entregará el dispositivo electrónico o medio de almacenamiento físico o sistema virtual desde donde fue recolectada la prueba o evidencia digital; por cuanto, en mi concepto, la prueba pericial frente al medio de prueba o evidencia digital deberá ser de obligatorio cumplimiento con el fin de entregar juicios de valor que refuercen el uso de la razón y la sana crítica de los jueces y magistrados. Y es que, sólo con el aporte de pruebas o evidencias digitales dentro de un proceso judicial, se hace inviable determinar la autoría de estas. Excepcionalmente, no resultaría necesario en los procesos penales en casos de flagrancia o en las demás jurisdicciones por su confesión.

OCTAVA: La eficacia o no de la prueba o evidencia digital deberá valorarse de forma individual, sin embargo, su apreciación con fines de poder entregar fuerza probatoria deberá hacerse en conjunto con los demás medios de prueba, en especial cuando de los hechos se requiera conocer el autor.

PROPUESTA FINAL DEL AUTOR:

El presente TFM fundamenta la propuesta del autor en la actualización de las normativas procesales respecto al tratamiento de la prueba o evidencia digital como medio probatorio autónomo. Proponiendo además la validez y unificación *erga omnes* de los conceptos tratados para su aplicación en los Estados que serán parte del protocolo adicional tercero del Convenio sobre la Cibercriminalidad de Budapest (en desarrollo) en lo que refiere a la jurisdicción penal. En las demás jurisdicciones, inicialmente se propone realizarse de manera interna por parte de cada Estado en sus códigos procesales o en las leyes de enjuiciamiento según sea el caso.

BIBLIOGRAFÍA

ABEL LLUCH, Xavier, juicio de admisión de la prueba electrónica, en: ABEL LLUCH, Xavier y PICÓ I JUNOY, Joan, La prueba electrónica, Editorial Bosh, Barcelona, 2011, págs. 383 a 391.

ALBERDI, Juan Ignacio y RUIZ DE ANGELI, Gonzalo Matías, *Análisis Forense de Memoria Principal*, en: DI LORIO, Ana Haydée. *El rastro digital del delito Aspectos técnicos, legales y estratégicos de la Informática Forense,* Universidad FASTA, Mar del plata, 2017, págs. 517 a 548.

ANGUIANO JIMENEZ, José María, La prueba electrónica en la banca digital. El soporte duradero, en: OLIVA LEÓN, Ricardo y VALERO BARCELÓ, Sonsoles, La prueba electrónica validez y eficacia procesal, Madrid, 2016, págs. 68-89.

ASENCIO GUILLEN, Antonio y MARCO, Julio Navío. *La génesis del ciberespacio, una visión desde las teorías de la comunicación,* UNED publicaciones, Madrid, 2017.

BANACLOCHE PALAO, Julio. *La prueba en el proceso penal,* en: BANACLOCHE PALAO, Julio y ZARZALEJOS NIETO, Jesús, *Aspectos fundamentales del Derecho Procesal Penal,* segunda edición, editorial La Ley, Madrid, 2011, págs. 234 a 273.

BENTHAM, Jeremy. *Antología* (edición de COLOMER Josep M. Traducciones de HERNÁNDEZ ORTEGA Gonzalo y VANCELLS Montserrat), Edición 62, Barcelona, 1991.

BUENO DE MATA, Federico, *Prueba electrónica y proceso 2.0*, Tirantlo blanch, Valencia, 2014.

CANO MARTÍNEZ, Jeimy José. *El peritaje informático y la evidencia digital en Colombia conceptos, retos y propuestas*. Uniandes, Bogotá, 2010.

CANO MARTINEZ, Jeimy José. *Computación forense. Descubriendo los rastros informáticos.* Alfaomega Colombiana, Bogotá, 2015.

CÁRDENAS RINCÓN, Erick. *Derecho del comercio electrónico y de internet*. Legis, Bogotá, 2017.

CISTOLDI, Pablo Adrián y NUÑES, Luciano, *Introducción a la Informática Forense, Criminalística e Investigación Penal*, en: DI LORIO, Ana Haydée, *El rastro digital del delito Aspectos técnicos, legales y estratégicos de la Informática Forense*, Universidad FASTA, Mar del Plata, 2017, págs. 46 a 83.

DE LA OLIVA SANTOS, Andrés, *Derecho Procesal civil. El proceso de declaración*. Editorial universitaria Ramon Areces, Madrid, 2000.

DE URBANO CASTRILLO, Eduardo. *La valoración de la prueba electrónica,* Tirantlo blanch, Valencia, 2009.

DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones,* Wolters kluwer España, Madrid, 2016.

DESONGLE CORRALES, Juan. *Ayudante técnico de informática de la Junta de Andalucía,* volumen II*,* Editorial MAD, SL, Sevilla, 2005.

DEVIS HECHANDÍA, Hernando. *Teoría General de la Prueba Judicial*, Editorial Zavalia, Buenos aires, 1981.

DILORIO, Ana Haidée. *Guía Integral de Empleo de la Informática Forense en el Proceso Penal.* Universidad FASTA, Mar del plata, 2016.

DI LORIO, Ana Haydée. "La recuperación de la información y la informática forense: Una propuesta de proceso unificado", memorias del Simposio Argentino de Informática y Derecho (SID 2015)- JAII 44, SADIO. 2015, nº44, págs. 117 a 130.

FERNÁNDEZ ALARCÓN, Vicenc. *Desarrollo de sistemas de información, una metodología basada en el modelado,* Ediciones UPC, Barcelona, 2006.

HOCSMAN, Heriberto Simón. *Negocios en Internet*. Astrea y Universidad del Rosario. Buenos Aires, 2013.

HOEPMAN, Henks y LEENES, Ronald. "Open source intelligence and privacy by Design". *Computer Law and Security Review.* 2013, nº 29.

HUNTER AMPUERO, Iván. "Control judicial de las reglas de la sana crítica (Corte Suprema)", *Rev. derecho (Valdivia)*, 2012, vol.25. nº 1.

IBAÑEZ CARRASCO, Patricia y GARCÍA TORRES, Gerardo. *Informática I con enfoque en competencias,* Cengage Learning, México D.F, 2009.

JOYANES AGUILAR, Luis. *Big Data, análisis de grandes volúmenes de datos en organizaciones, editorial Alfa Omega, México D.F, 2013.*

KNUTH, Donald E. *El arte de programar ordenadores volumen 1, algoritmos fundamentales,* editorial Revreté S.A., Barcelona, 2002.

LLOPIS BENLLOCH, José Carmelo, *Prueba electrónica y notariado*, en: OLIVA LEÓN, Ricardo y VALERO BARCELÓ, Sonsoles, *La prueba electrónica validez y eficacia procesal*, Madrid, 2016, págs. 18 a 24.

LÓPEZ, Valentín Carrascosa. Valor probatorio del documento electrónico. *Informática y Derecho: revista iberoamericana de Derecho informático*, 1995.

MANDADO PÉREZ, Enrique y MANDADO RODRIGUEZ, Yago. *Sistemas Electrónicos Digitales,* 9ª edición*,* Marcombo, Barcelona, 2008.

MIRANDA ESTRAMPES, Manuel. "La prueba ilícita: la regla de exclusión probatoria y sus excepciones". *Revista Catalana de seguretat pública,* 2010.

MORA DÍAZ, Rocío. "La valoración de la prueba en soportes informáticos". *El Derecho, Noticias Jurídicas.* 2004, nº 20.

MORAGA, Ramón. "Argumentación Ideal y falacias Unidad I: Argumentación". *Instituto Nacional José Miguel Carrera. Lengua Castellana y comunicación*, Tercero Medio. Disponible en la url: http://www.scribd.com/doc/17547111/Modulo-3-argumentación-falacias, recuperado el 18 de abril de 2020.

NIEVA FENOLL, Jordy. *La valoración de la prueba,* Marcial Pons, Ediciones Jurídicas y Sociales, Madrid, 2010.

NOTARIO, Enzo, PARRA DE GALLO, Beatriz, VEGETTI, Marcela, LEONE, Horacio. "Herramienta para el Análisis Forense de Correos Electrónicos". RISTI Revista lbérica de Sistemas de Tecnologías de Información. 2019, nº 32, págs. 17 a 32.

OLIVA HABA, José ramón, MANJAVACAS ZARCO, Custodia y MARTIN MÁRQUEZ, Pedro Luis. *Montaje y mantenimiento de equipos, sistemas microinformáticos y redes,* ediciones Parainfo, Madrid, 2014.

PINTO PALACIO, Fernando y PUJOL CAPILLA, Purificación. *La prueba en la era digital,* Wolters Kluwer, Madrid, 2017.

RILEY, Jenn. *Understanding metadata what is metadata, and what is it for?,* National Information Standards Organization (NISO), Baltimore, 2017.

RIZO GOMEZ, Belén. *La anticipación de la prueba en el proceso civil,* tirant lo blanch, Valencia, 2010.

SEMPRINI, Gastón. "El Análisis integral de la evidencia digital", *Memorias del Simposio Argentino de Informática y Derecho.* 2017, nº 46.

SENTIS MELENDO, Santiago. *La prueba. Los grandes temas del derecho probatorio,* editorial EJEA, Buenos Aires, 1978.

SILVA, Carlos, *Capas sin espesor: aproximación psicosocial a la cibercultura,* en: RANGEL, Ana Lisset y LADRÓN DE GUEVARA, Irene. *Voces digitales ida y vuelta a la cibercultura*, Latina, Caracas, 2003, págs. 37 a 46.

TESONE, Rodolfo, FERRER, Jordi y CABAÑATE, Josep. "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en materia penal". *Economist & jurist.* 2012.

TWINING, William. *Derecho y globalización,* siglo del hombre editores, Bogotá, 2003.

VALHONDO, Domingo. *Gestión del conocimiento, del mito a la realidad,* ediciones Díaz de Santos, Madrid, 2010.

VELASCO SAN MARTÍN, Cristos. Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos. Tirantlo blanch, Valencia, 2016.

REFERENCIAS WEB

https://www.ramajudicial.gov.co/web/noticias-paloquemao/informacion , recuperado el 25 de marzo de 2020, rama judicial república de Colombia. (Etapas del nuevo esquema acusatorio en Colombia).

http://noticias.gti.es/servidores-y-almacenamiento/que-es-un-disco-duro-ssd/ , recuperado el 29 de marzo de 2020, GTI software & networking. (Referente a los discos de estado sólido).

https://cleverdata.io/que-es-machine-learning-big-data/ , recuperado el 14 de abril de 2020, Cleverdata corp. (Referente al Machine Learning).

Informe Explicativo del consejo de Europa sobre el convenio de Budapest contra la cibercriminalidad, pág 1. Disponible en la url: https://rm.coe.int/09000016802fa403 , recuperado el 18 de abril de 2020, Council Of Europe.

https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ , recuperado el 18 de abril de 2020, ESET SECURITY.(Referente al convenio de Budapest sobre la Ciber criminalidad)

Informe Explicativo del consejo de Europa sobre el convenio de Budapest contra la cibercriminalidad, pág 6. Disponible en la url: https://rm.coe.int/09000016802fa403 , recuperado el 18 de abril de 2020, Council Of Europe.

Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos, BOE-A-2019-4244 Disponible en la url: http://www.boe.es , recuperado el 24 de abril de 2020, Boletín Oficial del Estado.

JURISPRUDENCIA

ESPAÑOLA

STC nº 236/2002 de 09 de diciembre de 2002, (RJ 2002/236)

STS nº 777/2013, de 7 octubre de 2013, FJ 7º, (RJ 2013\7891)

STS nº 300/2015 de 19 de mayo de 2015, (RJ 2015\1920)

STS nº 204/2016 de 10 de marzo de 2016, (RJ 2016/11142)

SAP nº 702/2015 de 24 de noviembre de 2015, (RJ 2015/16072)

SAP nº 69/2017 de 31 de enero de 2017, (RJ 2017\106183)

COLOMBIANA

Sentencia nº C-202/2005 de 08 de marzo de 2005, (D-5336)

Sentencia nº C-336/2007 de 09 de mayo de 2007, (D-6473)

Sentencia nº C-334/2010 de 12 de mayo de 2010, (D-7915)

Sentencia nº C-830/2002 de 8 de octubre de 2010, (D-3991)

Sentencia nº C-602/2016 de 02 de noviembre de 2016, (D-11332).

Sentencia 76001-23-33-000-2015-01577-01, del diecisiete 17 de marzo de 2016, Sección quinta de la sala de lo contencioso administrativo del Consejo de Estado Colombiano.

Sentencia nº T-043/20 de 10 de febrero de 2020, (T-7.461.559)

NORMATIVA

COLOMBIANA

Instructivo para el hallazgo, identificación, embalaje de la evidencia de tipo digital, adoptado mediante resolución 0-5017 del 20 de octubre de 2009, publicado en el Diario oficial No 47.510 de 22 de octubre de 2009, por medio del cual se actualizan los documentos del proceso penal, como parte del subproceso de policía judicial y se adopta un documento dentro del mismo subproceso relacionados con la actividad investigativa de la sección de investigaciones y apoyo a unidades nacionales.

Decreto 2364 de 2012, sobre la firma electrónica, Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

Ley 527/1999 de 18 de agosto de 1999. (Diario Oficial No. 43.673/ 21 agosto /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.

Ley 1564 del 12 de julio de 2012 por la cual se expide el nuevo Código General del Proceso el cual derogo el código de procedimiento civil colombiano.

Ley 906 de 31 de agosto de 2004 "Por la cual se expide el Código de Procedimiento Penal"

ESPAÑOLA

Constitución Española de 1978.

Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica.

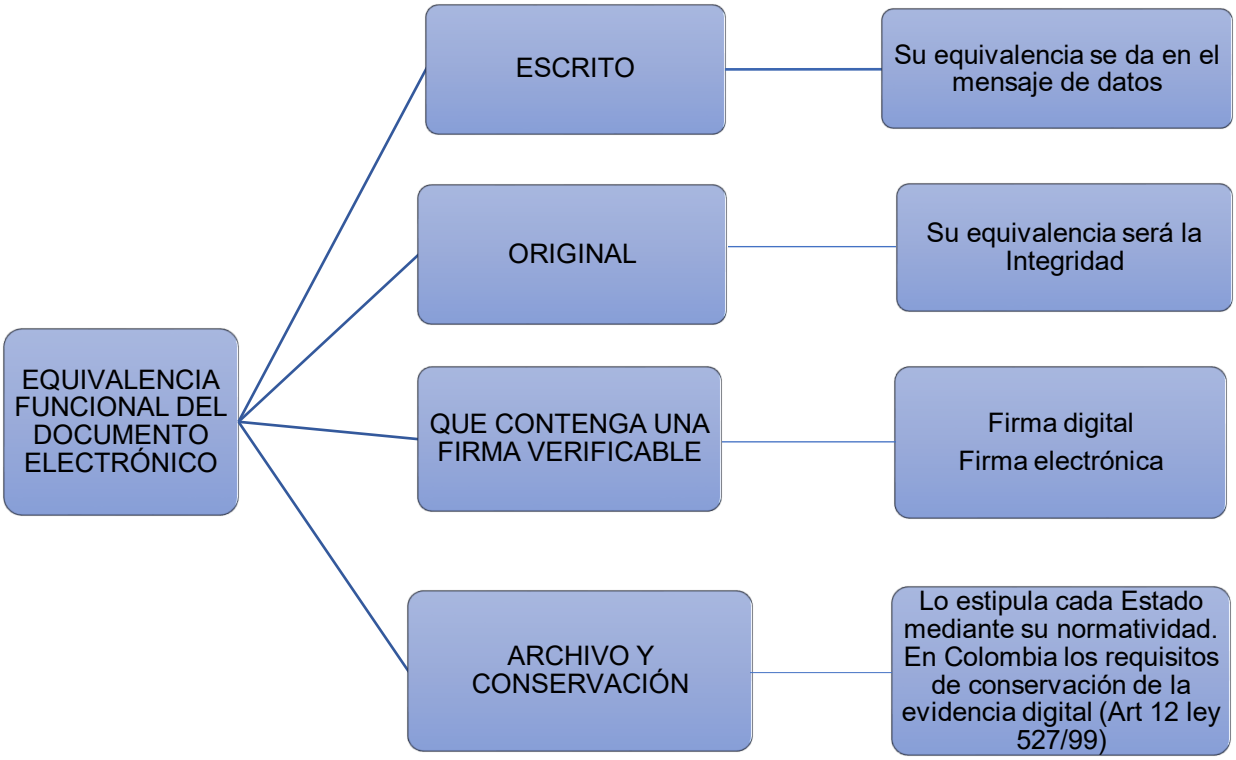
Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Ley 1/2000 del 7 de enero, Ley de Enjuiciamiento Civil.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

ANEXOS



Anexo 1. Equivalencia funcional del documento físico respecto a los documentos digitales, electrónicos y privados.[137]

[137] Elaboración propia.