Ratio Juris
ISSN: 1794-6638
ISSN: 2619-4066
Universidad Autonoma Latinoamericana

Gómez-Agudelo, Dany Steven
Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano
Ratio Juris, vol. 15, núm. 30, 2020, Enero-Junio, pp. 220-240
Universidad Autonoma Latinoamericana

DOI: https://doi.org/10.24142/raju.v15n30a11

Disponible en: http://www.redalyc.org/articulo.oa?id=585764837011

Cómo citar el artículo
Número completo
Más información del artículo
Página de la revista en redalyc.org

Sistema de Información Científica Redalyc
Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Ratio Juris

PUBLICACIÓN SEMESTRAL DE LA FACULTAD DE DERECHO
UNIVERSIDAD AUTÓNOMA LATINOAMERICANA

Vol. 15, N.° 30 enero junio pp. 15-282. Medellín-Colombia, 2020, ISSN 1794-6638 / ISSNe: 2619-4066
DOI: 10.24142/raju

Revista *Ratio Juris* Vol. 15 N.º 30, 2020 pp. 220-240 © UNAULA

TIPO DE ARTÍCULO DE INVESTIGACIÓN

Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano

Legal implications of digital evidence in the Colombian judicial process

Implicações legais da evidência digital no processo judicial colombiano

Dany Steven Gómez-Agudelo[1]

Recibido: 20 de enero de 2020 – Aceptado: 20 de abril de 2020 – Publicado: 30 de junio de 2020
DOI: 10.24142/raju.v15n30a11

Resumen
Este artículo identifica los principales antecedentes legislativos y jurisprudenciales de la evidencia digital en Colombia, con miras a detallar su tratamiento en el proceso judicial; así mismo, pretende evidenciar cómo opera la cláusula de exclusión, y de qué manera se protege el derecho a la intimidad, en la obtención de evidencia digital, desde distintos medios de almacenamiento. La metodología es cualitativa y se utilizó la técnica de la revisión documental y la entrevista a expertos, para mostrar una realidad respecto a una problemática de valoración de las pruebas tecnológicas, en los casos de ilicitud, y brindar aportes para mejorar la comprensión y la dimensión de su práctica en el proceso judicial. La principal conclusión es que no se le puede negar eficacia y validez probatoria por estar en forma de bytes, siempre y cuando se pueda establecer la autenticidad del contenido y la correspondencia con el autor.
Palabras clave: Autenticidad; búsqueda selectiva en base de datos; cláusula de exclusión; documento electrónico; intimidad.

[1]Abogado egresado de la Universidad Católica Luís Amigó. Especialista en Derecho Administrativo de la Universidad de Antioquia. Abogado litigante. Docente de las áreas de Metodología de la Investigación, Argumentación Jurídica e Informática Jurídica de la Corporación Universitaria de Colombia IDEAS. Docente de Derecho Informático de la Universidad Católica Luís Amigó. Orcid. https://orcid.org/0000-0003-2687-0146 Google Scholar: https://scholar.google.com/citations?user=YaysRIIAAAAJ&hl=es Email: dany-gomez@hotmail.com

Abstract
This article identifies the principal legislative and jurisprudential history of digital evidence in Colombia, with a view to detailing their treatment in the judicial process; It also aims to show how the exclusion clause operates, and how the right to privacy is protected in obtaining digital evidence from various storage media. The methodology is qualitative, a documentary review technique and the interview with experts were used to show a reality regarding a problem of assessment of technological evidence, in cases of illegality, and to provide contributions to improve understanding and its dimension in the judicial process. The main conclusion is that it cannot be denied effectiveness and probative value to be in the form of bytes, if they can establish the authenticity of the content and correspond with the perpetrator.
Key words: Authenticity; selective database search; exclusion clause; electronic document; privacy.

Resumo
Este artigo identifica os principais antecedentes legislativos e jurisprudenciais da evidência digital na Colômbia, com vistas a detalhar seu tratamento no processo judicial; Da mesma forma, o objetivo é demonstrar como a cláusula de exclusão opera e como o direito à privacidade é protegido, na obtenção de evidências digitais, de diferentes mídias de armazenamento. A metodologia é qualitativa e a técnica de revisão documental e a entrevista com especialistas foram utilizadas para mostrar uma realidade sobre um problema de avaliação de evidências tecnológicas, em casos de ilegalidade, e fornecer contribuições para melhorar o entendimento e a dimensão de sua prática no processo judicial. A principal conclusão é que não se pode negar a eficácia e a validade probatória porque está na forma de bytes, desde que seja possível estabelecer a autenticidade do conteúdo e a correspondência com o autor.
Palavras-chave: Autenticidade; busca seletiva de banco de dados; cláusula de exclusão; documento eletrônico; privacidade.

Sumario

Introducción
El avance de la tecnología ha generado que cada vez sea más común su incidencia constante en la sociedad, aspecto del que no es ajeno el ámbito legal, en el que se utiliza la evidencia digital, para acreditar hechos relevantes en un caso. Sobre el particular, Toro (2019) la define como: "Toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado" (p. 30). Esta se encuentra en distintos medios de almacenamiento, como tablets, computadores,

celulares, y que constituye en un medio de prueba, en el que las personas presentan al proceso un chat, foto, video o conversaciones de WhatsApp.

En este sentido, si bien las disposiciones normativas de la evidencia digital analógicamente están dadas por el medio de prueba documental, esta información digital tiene una naturaleza distinta, al estar compuesta por bytes de información, y ello plantea formas diferentes al momento de incorporarla, controvertirla y valorarla en el proceso judicial.

En este orden de ideas, el objetivo de este artículo es establecer los antecedentes legislativos y jurisprudenciales de la evidencia digital en Colombia, evidenciando cómo opera la cláusula de exclusión, y de qué manera se protege el derecho a la intimidad, en la obtención de información digital.

La metodología utilizada es de estudio fue de tipo cualitativo, por ser la más pertinente para el objetivo planteado, sobre el particular, Duque, González, Cossio & Martínez (2018) afirman: "su interés está centrado en la cotidianidad que es el espacio para comprender la realidad en el abordaje, de lo subjetivo e intersubjetivo, en los actores y escenarios en los cuales se desenvuelven sus prácticas jurídicas y sociales" (p. 61).

Para la obtención de información, se acudió a la técnica de la revisión documental, acudiendo a información especializada en revistas indexadas, libros nacionales e internacionales, trabajos de grado, bases de datos como Vlex, y sentencias proferidas por las Altas Cortes, realizando un análisis objetivo de la información. Esta se sistematizó en fichas, con algunas palabras clases ligadas a las categorías principales de la investigación.

Así mismo, se acudió a la entrevista semiestructurada a expertos, especialmente a peritos informáticos forenses, con experiencia en el campo forense digital.
El corpus de este artículo se compone de dos capítulos temáticos y un acápite final de conclusiones. En el primer capítulo, se realiza un examen de los antecedentes normativos y jurisprudenciales de la evidencia digital en Colombia. En el segundo capítulo, se lleva a cabo un análisis de la protección a la intimidad y las excepciones a la cláusula de exclusión en la evidencia digital.

I. Antecedentes normativos y jurisprudenciales de la evidencia digital.

El objeto de este acápite busca establecer cómo se ha desarrollado el tema de la evidencia digital dentro del proceso judicial colombiano, iniciando con una conceptualización del tema, luego con las características más relevantes, para finalmente, describir la evolución jurídica del tema.

Para empezar, dados los avances mundiales en materia informática, principalmente con la Internet, siendo esta una red abierta donde cualquier persona, puede a través de un portal publicar información, que fácilmente otros pueden tomar y reproducir, dejando pruebas de su comportamiento, se hace necesario analizar la regulación jurídica ante conductas que afecten la vida, honra y bienes de las personas en el entorno digital, y que pueden derivar en hechos jurídicamente relevantes que se deban llevar al proceso judicial como prueba, apoyándose en otras áreas de la informática. En efecto, el estudio del Derecho Informático es la base fundamental para el conocimiento y regulación de la sociedad respecto de la información digital. Ahora bien, es importante establecer una definición del documento electrónico. Este se debe entender como todo objeto mueble que, teniendo carácter representativo o declarativo, sea aportado al proceso judicial con el propósito de formar una convicción en el Juez, sobre la certeza de los hechos enunciados en la demanda o en su contestación. En este sentido, un documento tradicional consta de la información y el soporte, mientras que un documento electrónico tiene un tercer elemento de contener un mensaje encriptado, es decir, un mensaje cifrado, que debe ser traducido mediante alguna aplicación informática. Al respecto, Reyes (2020) afirma:

> Se ha aludido a los documentos electrónicos como una especie al interior del género "prueba electrónica". Otras manifestaciones de esta última son el correo electrónico, SMS (Short Message Service), y los sistemas de video conferencia aplicados a las pruebas testimoniales. Acerca de los SMS, es fácilmente reconocible el influjo que han tenido en la actualidad como método de comunicación y su empleo habitual en teléfonos móviles. En este escenario es relevante hacer mención de la aplicación WhatsApp, la cual se constituye como un software multiplataforma de mensajería instantánea pues, además del envío de texto, permite la trasmisión de imágenes, video y audio, así como la localización del usuario (p. 15).

Ahora bien, un documento almacenado electrónicamente es todo documento que tiene como soporte un almacenamiento electrónico, es decir, los que se presentan mediante instrumentos informáticos (como memorias USB, discos duros, discos compactos, entre otros), por esto, todo documento electrónico es un documento almacenado electrónicamente, pero no todo documento almacenado electrónicamente es documento electrónico.

Dado lo anterior, todo documento almacenado electrónicamente que se aporte al proceso judicial debe corresponder al contenido en el medio electrónico original, para que tenga valor jurídico probatorio, de acuerdo al artículo 8 de la Ley 527 de la Ley 527 de 1999. Para corroborarlo, existen los conceptos de firma digital y firma electrónica.

De otro lado, la Ley 527 de 1999, que reguló en Colombia el comercio electrónico, estableció los aspectos esenciales para el uso general de los mensajes de datos en

el proceso judicial. En este sentido, el legislador colombiano señaló aquello que debe entenderse como mensaje de datos y señaló los requisitos para que tenga el mismo valor probatorio atribuido a un documento en papel, esto es, el principio de equivalencia funcional. Esta ley definió el mensaje de datos como se expone a continuación:

> 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 (Ley 527, 1999, art. 2).

Ahora bien, algunos doctrinantes también se han ocupado de establecer otras definiciones sobre el documento electrónico. Al respecto Restrepo (2014) afirma:

> Es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, a través del computador, permiten su traducción a lenguaje natural a través de una pantalla o una impresora; otros expertos en el tema como el colombiano Alexander Díaz García afirman que los documentos electrónicos susceptibles de ser valorados como pruebas constan en un soporte material (cintas, diskettes, circuitos, chips de memoria, redes), e insiste en que todo documento requiere para su representación de un soporte, el soporte de este modo es todo substrato material sobre el que se asienta la información; es el elemento que sirve para almacenar la información para su tratamiento, recuperación y reproducción posterior (p. 38).

Así las cosas, el documento electrónico tiene una naturaleza diversa al documento tradicional, pues este se materializa a través de un software y un hardware, es inmaterial, por cuanto no tiene un carácter tangible, y cuenta con una serie de características que le otorgan un grado de seguridad jurídica similar a la del documento en papel, debiendo contar con las características de la norma técnica NTC/ISO 15489-1, las cuales son: autenticidad, integridad, fiabilidad y la disponibilidad, características que ha reconocido el Ministerio de Tecnologías de la Información y las Comunicaciones. De acuerdo con Restrepo (2014) se han definido así:

- Autenticidad: hace referencia a que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma.
- Integridad: esta característica se refiere al carácter completo del documento, esto es, que no haya sido modificado o alterado.
- Fiabilidad: aquella en la que su contenido representa exactamente lo que se quiso decir en él. Es una representación completa y precisa de lo que da testimonio y se puede recurrir a él para demostrarlo.

- Disponibilidad: al abordar la disponibilidad como característica del documento electrónico, MINTIC afirma que es aquella que hace posible localizar, recuperar, presentar, interpretar y leer (p. 42).

En este orden de ideas, el Código General del Proceso resulta más innovador que el antiguo Código de Procedimiento Civil, ya que surgió un cambio fundamental con el nuevo código, relativo a la presunción de autenticidad sobre los mensajes de datos, aportados en su formato original, esto es una USB o CD, que ahora no se pregona solo de los documentos públicos sino también de los privados; y también porque el artículo 243 del Código General del Proceso, le brinda pleno valor a los mensajes de datos.

Sin embargo, la impresión en papel de una prueba digital carece de la presunción de certeza. El Código General del Proceso en su artículo 244 del C.G.P precita lo siguiente: "La parte que aporte al proceso un documento, en original o en copia, reconoce con ello su autenticidad y no podrá impugnarlo, excepto cuando al presentarlo alegue su falsedad. Los documentos en forma de mensaje de datos se presumen auténticos" (Ley 1564, 2012, art. 244). Al respecto, Guzmán (2019) afirma:

> El común de los abogados tiene en su mente que la impresión en papel es una representación idéntica del documento electrónico y eso no es real, pues este es complejo y tiene muchas partes, el trasladarlo de manera correcta garantiza el derecho a la defensa de la otra persona, es una garantía del debido proceso (A. Guzmán, comunicación personal, 16 de diciembre de 2019).

De este modo, en el ámbito probatorio, la Ley establece que los mensajes de datos son medios de convicción y su fuerza corresponde a la asignada a los documentos, mediante el Código General del Proceso. Así mismo, la normatividad prohíbe expresamente negar validez jurídica, en cualquier actuación judicial o administrativa, a la información contenida en mensajes de datos, por estar contenida en este tipo de soporte, o no haber sido presentada en su forma original. A continuación, se presenta una descripción de algunos antecedentes normativos sobre la evidencia digital:

Ley 270 de 1996.

La Ley Estatutaria de Administración de Justicia 270 de 1996, reguló el ejercicio de la justicia en el país, y facultó a los jueces y magistrados de todas las jurisdicciones, para valorar los medios de prueba que acarree consigo la innovación de la tecnología, tal como se expone a continuación en el artículo 95:

> Tecnología al servicio de la administración de justicia. El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al

> servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información. Los juzgados, tribunales y corporaciones judiciales *podrán utilizar cualesquier medios técnicos, electrónicos, informáticos* y telemáticos, para el cumplimiento de sus funciones. *Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original* siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales (Ley 270, 1996, art 95).

De la norma expedida por el legislador colombiano, resulta claro que con el nuevo escenario de la tecnología, los operadores de justicia tienen amplias facultades puestas al servicio de la administración de justicia, y de otro lado, incluye deberes para la justicia nacional, para que mejore la práctica de pruebas digitales, mediante el desarrollo de planes que adelante el Consejo Superior de la Judicatura, como organismo administrativo encargado de la Rama Judicial, para estimular la incorporación de la tecnología de avanzada a los procesos judiciales.

Ley 527 de 1999.

Resulta importante conocer los antecedentes históricos de esta ley. A partir del informe de la Sexta Comisión de la Organización de Naciones Unidas para el Derecho Mercantil, la ONU expidió la resolución 51/162 de 1996, por medio de la cual aprueba la Ley Modelo sobre Comercio Electrónico, que tuvo como objetivo la unión entre las leyes internas de los países, sobre los medios de comunicación y almacenamiento de la información, que sustituían la información consignada en el papel.

Dado lo anterior, esta resolución de la ONU fue incorporada a la legislación interna colombiana por medio de 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. Esta ley trajo el principio de equivalente funcional, según el cual el documento electrónico tendrá el mismo valor probatorio que el documento en papel, siempre y cuando se cumplan los requisitos de originalidad, firma y posibilidad de acceso posterior.

En principio, fue aplicable al campo de las transacciones comerciales que se hacían por medios electrónicos, para que esos mensajes de datos tuviesen fuerza obligatoria, concediendo un reconocimiento y valor probatorio a los documentos electrónicos. Al respecto, en la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (1996) se afirmó que:

> La documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos (p. 21).

Así las cosas, el tema del documento electrónico se ha venido abordando en la academia especialmente desde el Derecho Informático. Si bien la Ley 527 de 1999 en un principio, pretendió regular el comercio electrónico, fue mucho más allá, al punto de convertirse en una ley transversal aplicable a los procesos judiciales de distintas áreas. Conforme a lo señalado anteriormente, es pertinente detallar cómo opera la evidencia digital en el proceso contencioso administrativo.

La prueba tecnológica en el derecho administrativo.

En este acápite se expondrá que desarrollo normativo tiene la prueba digital dentro del proceso administrativo. Algunos estudios como el de Ana María Restrepo (2014) explican algunas características del documento electrónico en el proceso que lo hacen disímil del documento tradicional, tal como se expone a continuación:

> El documento electrónico debe contar con un sistema de verificación que garantice su integridad y la identidad del originador. Lo anterior, por cuanto debe contar con ciertas características que le otorguen una seguridad jurídica semejante a la del documento en papel, así como mecanismos para determinar su origen, destinatario, fecha y hora de la creación y la exactitud de la información contenida (p. 40).

Ahora bien, es importante resaltar que el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, reconoce el valor probatorio de las pruebas electrónicas, de la siguiente manera: "será admisible la utilización de medios electrónicos para efectos probatorios, de conformidad con lo dispuesto en las normas que regulan la materia y en concordancia con las disposiciones de este Código y las del Código de Procedimiento Civil" (Ley 1437, 2011, art. 216).

Así las cosas, en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, no se discrimina este tipo de prueba por el hecho de estar contenida en el mensaje de datos, sino que por el contrario se le reconoce como un medio probatorio válido, para llevar al juez el convencimiento sobre los hechos objeto de controversia en el proceso. De igual manera, se ha abordado el problema de la eventual falta de autenticidad de la prueba digital, Restrepo (2014) afirma:

> Al tratarse de un documento electrónico, este debe tener ciertos requisitos que permitan esclarecer judicialmente su veracidad. Estas características también han sido dadas por la Ley y la Jurisprudencia. En ocasiones, es posible pensar que el material presentado ha sido alterado, y por ello el documento electrónico no ha sido bien recibido por algunos despachos judiciales. A pesar de ello, la Ley y la evolución tecnológica permiten a quienes pretendan hacer valer este tipo de prueba

> en sede judicial, al juez e incluso a la parte contra la que se aduce este tipo de documento, una gran variedad de garantías para asegurar su confiabilidad (p. 58).

Adicionalmente, la incorporación al proceso de las pruebas digitales puede tener algún grado de confusión para las partes, ya que la norma deja en libertad a los abogados que pretendan usar estos medios tecnológicos, en escoger la opción de cómo allegarlos al juez. Si se presentan de forma impresa, tienen presunción de autenticidad, mientras no se realice tacha de falsedad o sea desconocido por la parte contra la cual se aduce; en este caso, la persona debe demostrar que no fue el iniciador del mensaje de datos, a través de un dictamen pericial.

Pero también existe la opción de aportarlos en su formato original, esto es, en CD o USB, con previa descarga del archivo original. O incluso mediante la intervención de un perito en informática forense, con los conocimientos técnicos necesarios, para descartar cualquier falta de autenticidad de alguna de las pruebas digitales aportadas al proceso, lo cual implica mayores gastos para las partes, sobre el particular, Abel, X. (2019*)* afirma:

> Si es objeto de impugnación la falta de integridad del mensaje o la conversación se está impugnando que el mensaje ha sido manipulado, mediante la mutilación, sustitución o añadido de palabras o expresiones. En tal supuesto, lo procedente sería una prueba pericial informática sobre el dispositivo electrónico de la parte proponente de la prueba y, si fuera posible, sobre el dispositivo de la otra parte interviniente en el proceso de comunicación (p. 575).

En consecuencia, el papel del perito es fundamental para evitar el sacrificio de los intereses de alguna de las partes en el proceso, por lo que es importante que cuente con certificación en manejo de herramientas forenses, y con una experiencia en el campo forense digital, al momento de establecer la autenticidad de la evidencia digital. Sobre el particular, Guimaraes, D. (2019) afirma: "El valor del documento electrónico está directamente relacionado, como cualquier otro medio de prueba, con la seguridad y la autenticidad, porque cuanto más seguro y auténtico sea el documento, mayor será el grado de credibilidad que disfrutará en el proceso" (p. 534).

En este orden de ideas, la fácil manipulación de pruebas digitales hace que cobre relevante la cadena de custodia, incluso, la posibilidad de que por el carácter volátil del medio tecnológico este resulte modificado, por este motivo, existen protocolos aceptados en la comunidad internacional como la norma ISO 27.037, que exigen garantizar la autenticidad y la cadena de custodia de las pruebas digitales, al respecto la norma ISO 27.037 (2012) indica:

> Esta Norma Internacional también tiene la intención de informar a los tomadores de decisiones que necesitan determinar la confiabilidad de la evidencia digital que se les presenta. Es aplicable a las organizaciones que necesitan proteger, analizar

> y presentar evidencia digital potencial. Debido a la fragilidad de la evidencia digital, es necesario llevar a cabo una metodología aceptable para garantizar la integridad y autenticidad de la potencial evidencia digital (p. 1).

Es relevante aclarar que la norma ISO 27.037 es aplicable al proceso para recoger la evidencia digital, mientras que la norma ISO 27.042 se utiliza para analizar la información digital recogida.
A continuación, se presenta una gráfica que explica la metodología del perito en informática forense:

***Figura 1*. Diagrama Del Proceso De Evidencia Digital**

Gráfica número 3. Fuente: Guía número 13 sobre seguridad y privacidad de la información (MinTic, p. 12).

Adicionalmente, se debe mencionar una serie de requisitos técnicos en el procedimiento, sobre el particular Guzmán (2020) afirma:

> En la práctica, el requisito legal es que, en primer lugar, el archivo se pueda abrir, es decir que podamos ver tanto su contenido como sus metadatos; en segundo lugar, es requisito que exista una firma electrónica del documento que cumpla con los parámetros establecidos en la Ley 527 de 1999 y el Decreto 2364 del 2012. Finalmente, que el documento sea original, es decir que exista una garantía confiable de que se ha preservado en su formato original, esto de conformidad con

> las mejores prácticas internacionales (ISO 27037) que obligan a la existencia de un código hash, más la evidencia de la fecha y hora del recaudo que, hoy, incluso, están en el manual de cadena de custodia (p. 1).

En este orden de ideas, desde una perspectiva jurídica, se han establecido algunas fases de un dictamen pericial en el campo informático, al respecto Delgado (2018) afirma:

a. Obtención de los datos (acceso a la información).
b. Clonado de los datos y cálculo del hash.
c. Elaboración del dictamen.
d. Presentación del dictamen pericial al Tribunal.
e. Valoración por el Tribunal (p. 70).

Además, la impresión en papel de la prueba digital puede generar dudas frente al documento electrónico, sino se genera la certeza de que no ha sido modificado o de quien es su autor. Al respecto, Fernández (2018) afirma:

> Se debe conservar un proceso denominado cadena de custodia, la evidencia tecnológica tiene sus propias peculiaridades, pues no sólo hay que conservar el mismo dispositivo, sino también garantizar que esa información desde un origen hasta un fin no se ha vulnerado, y eso se concibe calculando firmas electrónicas o códigos hash, garantizando que esa información es la misma de origen a fin (J. Fernández, comunicación personal, 22 de marzo de 2018).

En este orden de ideas, hay que diferenciar los eventos donde un documento lleva firma digital y otros en que no la lleva, en el primer supuesto el documento electrónico cuenta con un mayor nivel de confiabilidad; mientras que en el documento electrónico sin firma digital, que es más usual en la internet, contiene signos que permitan establecer quién es el iniciador del mensaje. Sobre el particular, estos signos que permiten identificar al iniciador del mensaje de datos muestran el remitente, el destinatario, la hora de envío del email y permiten rastrearlo en caso de que sea necesaria una prueba adicional, concepto que deberá ser emitido a través de peritos. Al respecto, Restrepo (2014) afirma:

> En estos casos, si la persona contra la que se aduce la prueba niega su autenticidad, será esta quien deba demostrar que no fue el iniciador de dicho mensaje de datos. Otro escenario es presentar el documento electrónico presumiéndolo autentico, y en caso de ser desconocido por la persona contra la que se aduce, será entonces el aportante quien deba demostrar a través de peritazgos, porque el iniciador que indica en la prueba si es el autor de dicho mensaje de datos. Sobre este punto también puede suceder que la persona contra la que se aduce dicha prueba guarde silencio y, en este caso, dicho documento gozara de una presunción de autenticidad por la aceptación tácita del iniciador del mensaje de datos (p. 68).

Así las cosas, el Código de Procedimiento Administrativo y de lo Contencioso Administrativo le atribuye un papel protagónico a las partes, toda vez que estas debe ser activas en impugnar la credibilidad de las pruebas digitales, en caso de estar modificada en relación a la original, toda vez que, en caso contrario, la prueba podrá ser apreciada y valorada por el funcionario judicial, sin perjuicio, de la facultad del juez, de forma oficiosa, de restarle valor probatorio a las pruebas digitales que resulten manipuladas o modificadas, por las partes o terceros. Conforme a lo señalado anteriormente, es pertinente mencionar uno de los principales fallos de la Corte Constitucional sobre la evidencia digital.

Sentencia C 604 de 2016.

Es importante destacar la sentencia C-604 de 2016, de la Corte Constitucional, donde se resolvió una demanda de inconstitucionalidad en contra del artículo 247 del Código General del Proceso.

En este caso, los demandantes consideraban que el inciso segundo del artículo 247 de la Ley 1564 de 2012 por medio de la cual se expide el Código General del Proceso, no se ajustaba a la Carta Política y por tanto solicitaron la inexequibilidad de la norma que se presenta a continuación:

> El artículo 247 del Código General del Proceso. 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 (Ley 1564, 2012, art. 247).

Con relación a esta acción de inconstitucionalidad, los impugnantes señalaron que los mensajes de datos son medios probatorios, como lo son también los documentos impresos en papel, de manera que ambos se encuentran en igualdad de condiciones, además, explicaron que la sola impresión del mensaje de datos no refleja los requisitos de escritura, firma y originalidad. Al respecto, los demandantes indicaron:

> No se podría "acceder" a una impresión para su posterior consulta, como lo exige el artículo 6 de la Ley 527; no podría identificarse el iniciador del mensaje de datos, como lo impone el artículo 7 ídem., y tampoco podría considerarse original, en los términos del artículo 9 ídem, debido a que no existiría garantía de que el mensaje no fue modificado o se ha conservado inalterado desde que se creó. La "*volatilidad*" de esta clase de documentos los haría susceptibles de ser modificados, al momento de ser consultados, copiados, impresos o comunicados (Corte Constitucional, Sentencia C 604, 2016).

Así las cosas, los demandantes explicaron en su demanda contra la norma del Código General del Proceso, que los mensajes de datos no deben ser valorados a

partir de su impresión en papel y conforme a las reglas de los documentos, sino a la luz de sus características técnicas propia, toda vez que en caso contrario se haría imposible controvertirlos y la norma desconocería el derecho a la contradicción probatoria. En estas condiciones un perito en informática forense no podría analizar la prueba impresa, desde el punto de vista técnico.
Ahora bien, los demandantes también explicaron que la confiablidad de un mensaje de datos depende de que se garanticen los mecanismos técnicos de integralidad, inalterabilidad, rastreabilidad, recuperabilidad y conservación. Al respecto, se señaló:

> La integralidad asegura que el contenido transmitido electrónicamente sea recibido en su totalidad; la inalterabilidad garantiza la permanencia del mensaje en su forma original, mediante sistemas de protección de la información; la rastreabilidad permite al acceso a la fuente original de la información; la recuperabilidad posibilita su posterior consulta y de la conservación depende su perdurabilidad en el tiempo, contra deterioros o destrucción por virus informativos (Corte Constitucional, sentencia C 604, 2016).

Finalmente, aducen que la simple impresión en papel de un mensaje de datos, debe ser apreciada con base en las reglas generales de los documentos, por ello el legislador ordena la valoración de esa impresión con arreglo a las normas generales sobre los documentos, otorgándole un tratamiento diferente en atención a su esencia como prueba, ya que el mientras el documento electrónico se puede reproducir con exactitud, la simple impresión en papel podría generar un mensaje distinto al original, y dejando de lado el lleno de los requisitos de la equivalencia funcional, con criterios que no son aplicables al documento en papel.

En este sentido, la Corte Constitucional explicó los requisitos de fondo y forma de la acción pública de inconstitucionalidad, indicando que, en la presente demanda, no se cumplió con el requisito de certeza para poder emitir una decisión de fondo, toda vez que los demandantes atacaron una interpretación no susceptible de ser inferida de su texto, por tanto, la Corte resolvió declararse inhibida.

Dado lo anterior, el fallo aclara que el legislador si otorgó un tratamiento diferenciado a la valoración de los mensajes de datos en el artículo demandado. Allí estableció un aspecto relevante, señalando que si una información es generada, enviada o recibida a través de medios electrónicos, ópticos o similares, finalmente es allegada al trámite, en el mismo formato o en uno que lo reproduzca con exactitud, como un verdadero mensaje de datos, deberá valorarse conforme a sus criterios técnicos, con las reglas de la sana crítica, y finalmente su confiabilidad, que viene de los mecanismos empleados para garantizar la integridad de la información, su inalterabilidad, rastreabilidad y recuperabilidad, así como de la forma de identificar el iniciador del mensaje.

Adicionalmente, el Consejo de Estado se ha pronunciado sobre la validez del documento electrónico, en virtud de los adelantos tecnológicos y el impacto en el sector público. En Sentencia 2000-00082 del 13 de diciembre de 2017, con Magistrada Ponente Dra. Stella Conto Díaz del Castillo, se pronunció respecto al valor probatorio de las pruebas digitales:

> En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la no admisión como prueba de un mensaje de datos: a) Por la sola razón de que se trate de un mensaje de datos; o b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta (Conto, 2017, p. 6).

Así las cosas, en este fallo la Sección Tercera del Consejo de Estado precisa que la copia de una prueba digital que haya sido aportada al proceso de forma impresa podrá ser valorada por el juez administrativo, salvo que contra dicha prueba prospere la tacha de falsedad, en contra de quien la trae al caso. Por este motivo, su valoración será a partir de la apreciación conjunta y la sana crítica. Así mismo, se le brinda validez a las copias de pruebas digitales, en razón al principio de la buena fe constitucional, lo cual es una interpretación garantista, en favor de quienes desconocen la facilidad con que pueden ser modificadas estas pruebas, al presentarse de forma impresa al proceso.

II. Protección a la intimidad y excepciones a la cláusula De exclusión en la evidencia digital.

El presente acápite pretende exponer cómo se protege el derecho fundamental a la intimidad, cuando se presenta una evidencia digital en un proceso judicial, así mismo, que tipo de excepciones existen en la cláusula de exclusión, cuando se presentan pruebas obtenidas con violación a derechos fundamentales.

Para empezar, en distintos medios de almacenamiento, como tablets, USB, correos electrónicos, celulares, se conserva información digital, que sirve para probar hechos relevantes en un proceso judicial.

En este sentido, el acceso no autorizado a esta información personal vulnera el derecho a la intimidad del titular, salvo que este lo autorice expresamente o que medie una orden de una autoridad judicial competente. La intimidad es un derecho inhato al ser humano, de acuerdo con Sarmiento, Ardila & Báez (2016): "para que el hombre se desarrolle y geste su propia personalidad e identidad, es menester que disponga de un área que comprenda aspectos de su vida individual y familiar" (p. 47).

En este sentido, la intimidad se configura en dos dimensiones: "como secreto que impide la divulgación ilegítima de hechos o documentos privados, o como libertad,

que se realiza en el derecho de toda persona a tomar las decisiones que conciernen a la esfera de su vida privada" (Corte Constitucional, Sentencia C 881, 2014).

La consagración del derecho fundamental a la intimidad permite que los particulares exijan que los particulares ni el mismo Estado, invadan la órbita privada del ser humano, salvo con propósitos constitucionalmente justificables, toda vez que no se trata de un derecho absoluto.

En este orden de ideas, la vulneración de la intimidad en las pruebas digitales conlleva necesariamente a que por regla general (salvo algunas excepciones) se deba aplicar la cláusula de exclusión, al obtener una prueba con violación de derechos fundamentales. Este aspecto no es nada nuevo, desde la antigüedad eran muy frecuentes los sucesos donde las pruebas tenían las características de ilícitas, sobre el particular, Laudan (2013) afirma: "En el derecho griego del siglo V, el que interrogaba tenía el derecho de mandar a torturar al esclavo de otro para saber la verdad" (p. 143).

El principal fundamento es esta figura es el artículo 29 de la Constitución Política de Colombia que establece: "Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso" (Constitución, 1991, art. 29). Como ejemplo de lo anterior, Meza (2017) afirma:

- El acopio de mensajes de datos en la modalidad de correos electrónicos – ley 527 de 1999 -, cursados entre una de las partes y un tercero, sin el consentimiento de estos y atentando contra el derecho fundamental a la intimidad de los aludidos.
- El rastreo de computador de una de las partes sin orden de la autoridad penal competente (p. 98).

En este orden de ideas, la sentencia SU 159 de 2002 de la Corte Constitucional, se refirió acerca de los casos donde se debe anular un proceso por violación a garantías fundamentales, señala que, en principio, la nulidad solo afecta el acto probatorio respectivo, a menos que no existan dentro del proceso tras evidencias válidas y determinantes que soporten la sentencia.

Así las cosas, el acceso no autorizado a un medio de almacenamiento de información digital está tipificado como delito, si se realiza sin el debido consentimiento del titular, o sin autorización judicial, al respecto la Ley de delitos informáticos estableció el tipo penal de violación de datos personales:

> El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión

> de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Ley 1273, 2009, art 269F).

Por consiguiente, desde la óptica constitucional, el funcionario judicial debe realizar un análisis de cada prueba digital, para descartar que en su obtención se vulneraron derechos fundamentales, toda vez que en caso de que así ocurra, debe aplicar la cláusula de exclusión y evitar así la vulneración del principio del debido proceso.

En este sentido, en el proceso penal el procedimiento legalmente establecido en la Ley 906 de 2014, es que, si se detecta información de utilidad para la investigación, contenida en dispositivos informáticos, el fiscal del caso emite la orden, con miras a que la policía judicial acuda donde se encuentra el dispositivo, y extraiga una copia bit a bit de la información. Sobre el particular, Shick y Toro (2017) afirman: "El investigador necesita una orden de registro que especifique el alcance de su búsqueda. Debe reconocer que tipo de pruebas digitales deben ser buscadas e intenta averiguar por los aspectos importantes de la investigación" (p. 441).

No necesariamente la copia y extracción debe hacerse en el lugar de los hechos, pues en todo caso es mucho más confiable, desplazarse con los dispositivos desconectados, a un laboratorio en informática forense, evitando la modificación de la evidencia digital. Al respecto, Shick y Toro (2017) afirman: "la mejor práctica como investigador forense digital es hacer la examinación en un ambiente confiable, como un laboratorio forense" (p. 443). En este sentido, el Código de Procedimiento Penal establece:

> El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación, así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación (Ley 906, 2004, art. 235).

Así las cosas, el problema jurídico consiste en determinar si es obligatorio que el fiscal acuda ante el Juez de Control de Garantías, para que apruebe la extracción de datos informáticos, toda vez que es claro que esta facultad está en cabeza del fiscal, desde el criterio establecido por el legislador en la ley 906 de 2004. Mientras que, con la audiencia de control posterior, esto es, una vez obtenido el elemento material probatorio, no hay discusión, toda vez que, si es obligatorio en todos los

casos someter la evidencia digital recogida, a verificación de su legalidad por parte del Juez de Control de Garantías. Al respecto, la Corte Constitucional indicó:

> Pueden identificarse tres cláusulas generales de origen constitucional que sujetan las medidas dirigidas a la restricción de derechos en la investigación penal: (i) en materia del derecho a la libertad personal, en general sus restricciones deben ser autorizadas privativamente por el Juez de Garantías; (ii) en el ámbito de las intervenciones al domicilio, a la intimidad y a la privacidad (diligencias previstas en el Art. 250.2. C.P.), opera el control judicial posterior sobre lo actuado; y (iii) para todos los demás procedimientos restrictivos de los derechos fundamentales, se requiere autorización judicial previa. En suma, el Juez de Garantías ejerce un control previo de todas las diligencias de investigación penal que limitan los derechos fundamentales, salvo las intervenciones a la intimidad contenidas en el artículo 250.2. C.P., cuya revisión de legalidad es posterior y se ejerce tanto sobre el contenido de la orden como en cuanto a su ejecución (Corte Constitucional, C 014, 2018).

En este sentido, resulta claro que aquello que se encuentre dentro del artículo 250 de la Constitución no requiere autorización judicial previa – solo orden de fiscal -, mientras que, para todos los demás procedimientos restrictivos de los derechos fundamentales, el Juez de Garantías ejerce un control previo de todas las diligencias de investigación penal que limitan los derechos fundamentales. Por consiguiente, el artículo 250 de la Constitución establece:

> La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo. En ejercicio de sus funciones la Fiscalía General de la Nación, deberá: 2. Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes (al solo efecto de determinar su validez) (Const, 1991, art. 150).

Adicionalmente, en materia de vulneración a la intimidad, existen excepciones como el consentimiento del titular, y la autorización judicial de funcionario competente, por lo cual es importante analizar si existen otras excepciones.

Así las cosas, en materia de derecho de familia, en el proceso de divorcio, se han presentado discusiones probatorias, sobre la causal de "las relaciones sexuales extramatrimoniales de uno de los cónyuges" (Ley 25, 1992, art. 6), por medio de pruebas digitales. En un caso puntual, la prueba de la infidelidad estaba en el celular de la esposa, quien en el caso era la demandada, y ella no accedía a entregar el celular, con el fin de que un perito en informática forense llevara a cabo una

extracción de la información y un análisis forense digital, para acreditar si se configuraba la causal o no. Sobre el particular, Lozada (2019) afirma:

> Las evidencias estaban en el celular de la señora, el dispositivo era de ella y no lo iba a entregar, pero este equipo estaba a nombre de la empresa de los dos cónyuges; entonces en las políticas de seguridad de la empresa, estaba claro que el dispositivo era de la empresa y por ese medio se pudo acceder a practica el peritaje. Ella alegó violación a la privacidad, porque consideraba que era el celular era de su propiedad, pero no le prosperó. En este caso, se encontraron fotos en la memoria del celular, con material en contra de la señora, las cuales acreditaron la infidelidad. En este sentido, el juez de familia admitió la prueba pericial, y la decisión fue en favor del esposo, decretando el divorcio. El proceso no llegó a segunda instancia (A. Lozada, comunicación personal, 15 de septiembre de 2019).

En este sentido, la decisión del Juez de Familia fue avalar la protección del acuerdo en política de tratamiento de datos personales, ordenando la práctica de un dictamen pericial en el celular y finalmente decretando el divorcio, brindándole primacía a la aplicación de las disposiciones de la Ley Estatutaria 1581 de 2012 de Protección de Datos Personales, por encima de aspectos relacionados a la privacidad.

Sin embargo, por regla general, la Ley Estatutaria 1581 de 2012 de Protección de Datos Personales, ordena conservar una autorización previa, expresa e informada al titular de la información, toda vez que los datos: "no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento" (art. 4).

Finalmente, nótese como en el campo judicial existen casos donde se generan tensiones entre el derecho a la intimidad y el tratamiento de datos personales, y el funcionario judicial ha decidido optar por prevalecer las disposiciones de la Ley 1581 de 2012, brindándole pleno valor probatorio a la evidencia digital recogida del dispositivo, por tratarse de información con previos acuerdos suscritos en materia de datos personales.

Conclusiones

La evidencia digital debe cumplir con los requisitos intrínsecos de autenticidad, integridad, fiabilidad y disponibilidad, y extrínsecos de legalidad y licitud, para ser valorada en el proceso.

La valoración de la evidencia digital se realiza a partir de la apreciación conjunta y la sana crítica, sin perjuicio, de la facultad del juez, de restarle valor probatorio a chats, fotos, videos, o correos electrónicos, que resulten manipulados o modificados, por las partes o terceros.

La normatividad y la jurisprudencia ha avalado la aplicación del principio de equivalencia funcional, en el sentido del mensaje de datos no se le puede negar eficacia y validez jurídica y probatoria por el simple hecho de serlo, siempre y cuando se pueda establecer la autenticidad del contenido y la certeza de que quién lo emitió, sea efectivamente la persona que lo firmó.

Bibliografía

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Delgado, J. (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Madrid, España: Wolters Kluwer.

Duque, S, González, F, Cossio, N & Martínez, S. (2018). *Investigación en el saber jurídico*. Medellín, Colombia: Universidad de Antioquia.

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

Guimaraes, D. (2019*). La prueba digital.* En Agudelo, D, Pabón, L, Toro, L, Bustamante, M & Vargas, O. La prueba: teoría y práctica (pp. 521 – 539). Medellín: Universidad de Medellín.

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

Guzmán, A. (17 de julio de 2017). *La prueba electrónica - Entrevista Andrés Guzmán Caballero. Agencia Nacional para la Defensa Jurídica del Estado* [Archivo de Video]. Recuperado de YouTube (16 de diciembre de 2019). Recuperado de https://www.youtube.com/watch?v=8IebLRPkCU4&t=1176s

Laudan, L. (2013). *Verdad, error y proceso penal. Un ensayo sobre epistemología jurídica*. Madrid, España: Marcial Pons. Recuperado de https://www.marcialpons.es/media/pdf/9788415664741.pdf

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

Meza, H. R. (2017). *La iniciativa judicial probatoria. La prueba de oficio en el proceso contencioso administrativo*. Bogotá, Colombia: Leyer.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (17 de mayo de 2018). *Guía número 13 sobre seguridad y privacidad de la información.* [Fotografía]. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Norma ISO 27.037 (2012). *Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.* Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

ONU, (1996) *Ley Modelo de la CNUDMI sobre Comercio Electrónico*. Recuperado de https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

Restrepo, A. (2014). *El documento electrónico como medio de prueba en el procedimiento laboral colombiano.* (Trabajo de grado). Pontificia Universidad Javeriana. Cali, Colombia.

Sarmiento-Verbel, A. R., Ardila-Barrera, J. R., & Báez-Pimiento, A. (2016). *Aportaciones no jurídicas al concepto de "la intimidad": reflexiones interdisciplinarias. DIXI, 18* (23). https://doi.org/10.16925/di.v18i23.1290

Shick, K. y Toro, M. (2017). *Cibercriminología. Guía para la investigación del cibercrimen y las mejores prácticas en seguridad digital.* Bogotá, Colombia: Antonio Nariño.

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