

DOCTRINA

Autenticidad y debido proceso en los mensajes de Whatsapp: Una revisión en los casos de divorcio

Authenticity and due process of Whatsapp messages: A review in divorce cases

Dany Steven Gómez Agudelo  Jenny Marcela Acevedo Valencia 
y Juan Esteban Aguirre Espinosa 

Universidad Católica Luis Amigó, Colombia

RESUMEN El artículo analiza la autenticidad de los mensajes de Whatsapp como prueba en el proceso judicial en los casos de divorcio y su incidencia en la protección del principio del debido proceso en Colombia. El estudio se sustenta en un enfoque socio-jurídico y utiliza técnicas de recolección de información como la revisión documental, el grupo focal, la entrevista a expertos y la observación no participante. En los resultados se evidencia que la facilidad para modificar mensajes de Whatsapp, aun sin los mayores conocimientos técnicos, por medio de aplicaciones gratuitas, genera la necesidad de revisar la autenticidad de los mensajes, para evitar desconocer el principio del debido proceso. El código hash sería un factor que contribuye a garantizar la autenticidad de la prueba digital y, por lo tanto, debe ser implementado en los casos de divorcios.

PALABRAS CLAVE Autenticidad, código *hash*, contradicción, debido proceso, documento electrónico, mensaje de datos, prueba digital.

ABSTRACT The article analyzes the authenticity of Whatsapp messages as evidence in the judicial process of divorce cases and their impact on the protection of the principle of due process in Colombia. The study is based on a socio-legal approach and information collection techniques such as document review, focus group, interview with experts and non-participant observation are used. The results show that the ease of modifying Whatsapp messages, even without the greatest technical knowledge through free applications, generates the need to thoroughly review the authenticity of the messages, to avoid disregarding the principle of due process; being the hash code a factor that contributes to guaranteeing the authenticity of the digital proof and therefore, it must be implemented in divorce cases.

KEYWORDS Authenticity, hash code, contradiction, due process, electronic document, data message, digital proof.

Introducción

Las nuevas tecnologías de la información y las telecomunicaciones han generado cambios en las formas de relacionamiento entre las personas, asunto que ha impactado en los aspectos probatorios que se surten al interior de los procesos judiciales. Un ejemplo de ello es el auge de la aplicación de mensajería instantánea Whatsapp, que ha permitido a las personas comunicarse desde un dispositivo móvil y compartir todo tipo de contenido, como mensajes de texto, fotos, videos y audios, los cuales pueden convertirse en posibles pruebas digitales¹ en un proceso judicial. Sobre este asunto, Miguel de Asis Pulido (2020: 187) afirma:

El vertiginoso desarrollo que están protagonizando las nuevas tecnologías desde la segunda mitad del siglo pasado está llevando a la sociedad y, con ella, al derecho, a llegar a las más que necesarias reflexiones sobre su implementación. Hay una sociedad basada en técnicas y dispositivos implementados por los seres humanos donde gran parte de sus procesos se han consumado en la red.

Es así como, con la implementación de las nuevas tecnologías de la información y telecomunicación mediante el uso de teléfonos inteligentes, se permite un mayor flujo de información mediante mensajes de Whatsapp, los que inciden como pruebas en decisiones que adoptan los jueces en las áreas penal, civil, laboral, administrativa y derecho de familia.

Las partes en un caso en ocasiones no tienen la posibilidad de analizar si la prueba digital allegada al proceso ha sido modificada o adulterada, ni determinar en qué fecha se creó, desde dónde se envió el mensaje, quién lo envió, cómo se envió o cómo se archivó, aspectos relevantes para que el juez adopte su decisión con fundamento en pruebas lícitas y legales. Al respecto, Rodríguez (2018: 36) afirma:

La propia naturaleza de las pruebas digitales hace posible la manipulación de las mismas, por ejemplo, podrá manipularse un «pantallazo» aportado en documento impreso bien suprimiendo o añadiendo partes a la conversación mantenida o bien porque esa conversación nunca tuvo lugar.

En este sentido, las conversaciones de Whatsapp son fáciles de modificar, incluso sin conocimientos técnicos avanzados. Sobre el particular, Guzmán afirma: «Existen múltiples plataformas de edición y hasta confección de pantallazos de Whatsapp, por

1. Por *prueba digital*, se va a entender aquella formación con valor probatorio transmitida mediante un medio electrónico, contenida en mensajes de Whatsapp u otras aplicaciones, que permite reconstruir hechos importantes para un caso. Por su parte, el *medio de almacenamiento* será el dispositivo donde queda alojada la información, como un teléfono.

ejemplo Whatsapp Fake Chat,² en la que, se pueden simular los íconos del operador y los mensajes en toda su dimensión».³

Así las cosas, el objetivo de este artículo se centra en analizar la autenticidad de los mensajes de Whatsapp como pruebas en el proceso de judicial de los casos de divorcio, y su incidencia en la protección del principio del debido proceso en Colombia.

Si bien existen antecedentes académicos sobre la prueba digital, la mayor parte hace énfasis en el área penal. Por ello, el objeto de este estudio implica un aspecto innovador desde el estudio de derecho probatorio, puesto que el crecimiento de la tecnología advierte importantes controversias frente a la autenticidad y el debido proceso cuando se utilizan mensajes de Whatsapp en un caso. Es en este contexto en el que surgen las siguientes preguntas: ¿cómo aportan estos mensajes al proceso judicial?, ¿cómo se asegura su autenticidad?, ¿cómo se controvierten estas pruebas? y ¿cómo debe valorarlos adecuadamente el juez para proteger el debido proceso?

Con el propósito de dar respuesta a la pretensión de este artículo, es importante aclarar que este estudio se soportó en los parámetros de una investigación de corte sociojurídico y que, como dicen Duque y otros (2018: 23), permiten reconocer las problemáticas que se detectan «de la dogmática en su relación con la realidad social»; es decir, que esto conlleva a que el investigador se enmarque desde una concepción fáctica o empírica del derecho. Durante el desarrollo del estudio se utilizaron técnicas de recolección de información, como la revisión documental, el grupo focal, la entrevista semiestructurada a expertos y la observación no participante.

En relación con la revisión documental, la investigación se centró en revisar información bibliográfica acudiendo a la literatura especializada en revistas indexadas, libros, sentencias emitidas por las cortes y tesis de posgrado. Se utilizaron motores de búsqueda en bases de datos, como Google Académico, E-Books, EBSCO, Legis Móvil, Notinet y Vlex, bibliotecas digitales, sitios web de entidades públicas y privadas y blogs de expertos en la materia.

En lo que respecta al grupo focal, se creó un evento institucional, llamado «Derecho y Nuevas Tecnologías: La Prueba Digital», en el que se llevó a cabo una mesa de discusión que contó con la participación de varios expertos en el tema, lo que permitió diferenciar y conocer los argumentos de los participantes. También se realizaron cinco entrevistas semiestructuradas a expertos, como jueces, peritos informáticos forenses y abogados litigantes, para obtener información que diera cuenta de los objetivos del proyecto. Como elemento transversal de la investigación, se hicieron observaciones en seminarios, congresos y foros sobre la temática, a fin de sistematizar la información pertinente y registrarla para su posterior análisis.

2. Sitio disponible en <https://www.fakewhats.com/generator>.

3. «Procesalistas estudian el valor probatorio de los “pantallazos” de Whatsapp», *Ámbito Jurídico*, 8 de abril de 2020, disponible en <https://bit.ly/3o71vFl>.

Así, la construcción de este artículo puede resultar trascendental y servir como punto de reflexión para otros países de la región, al desarrollar el aspecto probatorio de los mensajes de Whatsapp, toda vez que precisa cómo se puede garantizar la autenticidad y el principio del debido proceso ante la evolución tecnológica que debe asumir el sistema judicial.

El corpus de este artículo se compone de varios apartados y un acápite final de conclusiones. En la primera sección se examinan los aspectos generales y la autenticidad de los mensajes de Whatsapp; la segunda sección se ocupa de una descripción de los elementos estructurales del principio del debido proceso en la valoración de este tipo de intercambio de datos e información; y la última sección se centra en dar cuenta de la vulneración del debido proceso, con la práctica de mensajes de Whatsapp en casos de divorcio.

Nociones generales y autenticidad de los mensajes de Whatsapp

En este acápite se abordará una conceptualización sobre la prueba digital en los mensajes de Whatsapp, y las formas de aportarla al proceso judicial en Colombia, con la finalidad de comprender su naturaleza tecnológica y cómo funcionan los mecanismos que existen para garantizar su autenticidad, como el código *hash*, dentro del marco del derecho fundamental y el principio constitucional al debido proceso (Salt, 2017).

El objeto de conocimiento de este estudio sobre la prueba digital se enmarca en unos antecedentes legislativos, en principio, la Ley Estatutaria de Administración de Justicia 270 de 1996, que reguló el ejercicio de la justicia en el país y estableció el requisito de autenticidad de las pruebas digitales que fuesen practicadas en los procesos judiciales. Luego, la Ley 527 de 1999 reguló el mensaje de datos, estableció su definición y señaló los elementos del principio de equivalencia funcional, esto es, los requisitos técnicos que hacen que un documento electrónico cumpla el mismo fin atribuido a un soporte en papel, para que pueda considerarse como su homólogo para efectos jurídicos.

Más tarde, la Ley 1.564 de 2012, por medio de la cual se expidió el Código General del Proceso, permitió que se realizara la valoración probatoria del mensaje de datos, tanto desde el material disponible en medios tecnológicos como desde el documento impreso en papel, y otorgó la presunción de autenticidad a los documentos aportados a los procesos en forma de mensaje de datos. Asimismo, la sentencia C-604 de 2016, de la Corte Constitucional, resolvió una demanda de inconstitucionalidad en que los demandantes consideraban que el inciso segundo del artículo 247 de la Ley 1.564 no se ajustaba a la Carta Política, y por tanto solicitaron la exequibilidad de la norma. Sin embargo, la Corte decidió declararse inhibida por falta del requisito de certeza, uno de los requisitos mínimos para que pueda ser adoptada una decisión de fondo dentro de una acción pública de inconstitucionalidad.

Para empezar, se deben plantear algunos significados del concepto de *prueba digital*, con miras a establecer sus características particulares que la diferencian de los medios de prueba tradicionales, pues cada vez es más su utilización en las relaciones humanas. La importancia de este estudio la explica Guimaraes (2019: 536) quien afirma: «Toda actividad humana está conectada. Consecuentemente, la forma de concretización de las relaciones jurídicas también va a cambiar y con ella el medio de registrárselas». En relación con otras definiciones del concepto de *prueba digital*, Tobal afirma: «Es un contenedor de información digital que pueden ser utilizada como prueba en un procedimiento judicial».⁴ De otro lado, Toro (2019: 30) destaca los conceptos de la «Guía de prueba electrónica del Consejo de Europa» que indica: «La prueba electrónica es aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial».

De esta manera, el término *prueba digital* incluye rastros digitales representados en mensajes de Whatsapp, chats, fotos, correos electrónicos, grabaciones, videos o audios que se almacenan en dispositivos tecnológicos. Por tanto, cuando una persona o un software ejecuta una acción con uno de estos dispositivos ocurre un *hecho electrónico*, en el que informáticamente quedan rastros, evidencias de hechos en los sistemas informáticos.

Ahora bien, frente a la regulación del tema, el Código General del Proceso de Colombia regula la prueba digital mediante el medio de prueba documental, sin que se refiera al concepto de prueba digital. Sobre el particular, Mesa afirma: «Desde ahí no se reconoce como medio autónomo sino subordinado, eso ha hecho que ellos no entienden que es un mensaje de datos, y lo valoran como un documento cualquiera».⁵ De este modo, el Código General del Proceso menciona en su artículo 243 que son documentos los mensajes de datos, situación que hace necesario acudir a las disposiciones de la Ley 527 de 1999 para determinar los antecedentes normativos del tema por remisión expresa del Código. En dicha Ley se estableció la definición de un *mensaje de datos*, entendido como «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» (artículo 2). Así, el legislador colombiano incluye una conceptualización innovadora del término, puesto que la expresión «ópticos o similares» incluye los adelantos tecnológicos que se generen en el futuro, teniendo en cuenta que la aplicación Whatsapp periódicamente presenta actualizaciones.

4. Javier Tobal, «Análisis forense de evidencias digitales», *Blog de Javier Tobal*, 13 de octubre de 2015, disponible en <https://bit.ly/3wy69bv>.

5. Comunicación personal con Ana María Mesa Elneser, 15 de noviembre de 2019. Mesa es abogada, perito, doctora en derecho procesal, docente en pregrado y posgrado, líder y representante legal de Law Tic, empresa de tecnología y derecho.

Dentro de esta noción se encuentran dos principios para el tratamiento del mensaje de datos: i) *neutralidad tecnológica*, que se refiere a que no importa cuál es la tecnología que se use para la generación del mensaje de datos, que sea conocida o por conocerse; y ii) *equivalencia funcional*, que se refiere a que el documento electrónico tendrá el mismo valor probatorio que el documento contenido en papel, si se cumplen algunos requisitos técnicos. En este sentido, la jurisprudencia de la Corte Constitucional le ha brindado pleno valor al principio de equivalencia funcional, y ha planteado pautas para los funcionarios judiciales acerca de cómo valorar estas pruebas tecnológicas:

La incorporación al proceso del documento electrónico supone, también se advirtió, los «equivalentes funcionales» a los que hacen relación los artículos 6, 7 y 8 de la Ley 527 de 1999, que homologan la exigencia escritural del documento, la necesidad de la firma y la obligación de su aportación en original. Y, por otro lado, presupone también que tales mensajes deben ser valorados con arreglo, además de la sana crítica, a su confiabilidad, derivada de las técnicas empleadas para asegurar la conservación de la integridad de la información, su inalterabilidad, rastreabilidad y recuperabilidad, así como de la manera de identificación del iniciador del mensaje.⁶

Asimismo, la sentencia C-604 de 2016 también se refirió a los requisitos técnicos bajo los cuales un documento electrónico tendrá el mismo valor probatorio que el documento contenido en papel, precisando que,

cuando la ley exija que un contenido conste por escrito, el mensaje de datos puede ser análogo al papel, siempre que la información sea posteriormente consultable; en los casos en que se requiera la firma, cumplirá esa exigencia si se utiliza un método que permita identificar el iniciador del mensaje y asegurarse de que aprueba su contenido; y en los supuestos en que las normas requieran la versión original del documento, podrá satisfacer el requerimiento bajo condición de que se halle técnicamente garantizada la integridad de la información, es decir, que haya permanecido completa e inalterada, a partir de su generación por primera vez y en forma definitiva.⁷

Del pronunciamiento anterior, la Corte se refiere al requisito del mensaje de datos, consagrado en el artículo 12 de la Ley 527 de 1999, que implica la necesidad de acudir al mensaje de datos original. Esto significa que, si la prueba original ya se perdió o se eliminó, en síntesis, no es posible su acceso posterior y se podrá ver afectado su valor probatorio. Además, el legislador colombiano ha determinado que la presentación de una prueba en forma de mensaje de datos se presume auténtica. Sobre el particular, el artículo 247 del Código General del Proceso indica:

6. Corte Constitucional de Colombia, sentencia C-604, 2016.

7. Corte Constitucional de Colombia, sentencia C-604.

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 1.564, artículo 247).

Esta regulación es relevante toda vez que, con el antiguo Código de Procedimiento Civil, solo los documentos públicos tenían una presunción de autenticidad; pero ahora, con el Código General del Proceso, dicha presunción se aplica también a los documentos electrónicos de carácter privado. En este sentido, no ocurre lo mismo cuando en un proceso se imprime en papel una prueba digital, como un mensaje de Whatsapp o correo electrónico, en que se deberán aplicar las reglas tradicionales de los documentos. Así las cosas, la forma de presentar el documento electrónico genera cambios en la forma como el juez debe valorar la prueba digital, quien deberá tener en cuenta los criterios desarrollados por la Ley 527 de 1999, como la sana crítica, la confiabilidad en la forma en la que se haya generado, archivado, conservado o comunicado el mensaje, si se identifica al iniciador del mensaje y demás factores pertinentes. Sobre el particular, Delgado (2018: 78) afirma:

El juez valorará la prueba electrónica conforme a las reglas de la sana crítica según la naturaleza del soporte en el que se haya aportado los datos, en definitiva, una valoración conforme a las reglas de criterio racional, es decir, de forma ajustada a las reglas de la lógica, los principios de experiencia y los conocimientos científicos.

Según lo expuesto, es importante abordar las maneras posibles de aportar las pruebas digitales al proceso. En la aportación o presentación de los mensajes de Whatsapp, se admite su incorporación como prueba documental, prueba pericial o en su formato original, en virtud de los artículos 245 y siguientes del Código General del Proceso. En cualquier caso, la legislación otorga libertad a las partes en la forma de aportar la prueba al caso, como se explica a continuación:

- Formato original: En este caso, sin necesidad de acudir a un perito, la misma persona descarga el mensaje con el archivo original y lo guarda en un CD o memoria USB, que anexará a la demanda y la relacionará en el escrito en físico que se presenta para dar inicio al proceso.
- Impresión del archivo electrónico en papel o *screenshot*: Se toma una fiel copia del mensaje de datos original, lo que equivaldría a una foto.
- Extracción forense con perito forense certificado: En este caso, la prueba se compone de un informe pericial, un testimonio de experto y documentos físicos y digitales. Además, se debe aplicar la cadena de custodia.

Es necesario establecer cómo se lleva a cabo el dictamen pericial informático. Al respecto, Cardona afirma:

El dictamen pericial se hace con la preservación de la prueba, al demandante se le toma un consentimiento informado para recolectar la información, dado que es el dueño de ese bien mueble. Posteriormente, se preserva la evidencia digital, se somete a cadena de custodia, se lleva al laboratorio, haciendo la extracción de la información, con protocolos y herramientas forenses, se genera el informe y vuelve mediante una evidencia resultante, deja de ser el celular para ser el Whatsapp, que se entrega en DVD o USB, en un almacenamiento digital que no pueda ser modificado —se somete a cadena de custodia— con su respectivo informe, con el análisis y el cálculo *hash*.⁸

En este orden de ideas, de acuerdo con la doctrina, los eventos en que también resulta procedente la práctica del dictamen solicitado por las partes y decretado por el juez son:⁹

- Cuando la autoridad estime que puede establecerse con dictamen el hecho que el interesado pretende demostrar mediante inspección.
- Cuando el operador jurídico estime necesario ordenar de oficio la práctica de la peritación.
- Cuando sea solicitada mediante amparo de pobreza.
- Cuando, por disposición expresa de la ley, se debe practicar el dictamen pericial en el curso del proceso.

Para que el juez decrete de oficio una prueba digital, a la parte a quien le favorece dicho decreto le corresponde entregar antes un derecho de petición, en que haya intentado recoger esa prueba y no se haya obtenido respuesta, o que, habiéndose obtenido, el destinatario no hubiere accedido a radicar la información. Además, la doctrina también se ha referido al tema de cómo se aporta la prueba digital al proceso, la cual es la pieza fundamental sobre la que el juez va a sustentar su decisión. En este sentido, Martínez (2018: 133) indica:

- Aportación que se logra mediante pedimento del juez: Dentro de un proceso, una de las partes pide como prueba un documento que se encuentre en una oficina pública. En ese caso, el juez, si lo estima pertinente, ordenará a la en-

8. Comunicación personal con Juan David Cardona Pérez, exfuncionario en delitos informáticos y cómputo forense, perito en informática forense, analista en cibercriminalidad y director de Laboratorio en Informática Forense, 15 de octubre de 2021.

9. «Prueba pericial: Dictamen, controversia y contradicción», *Uniacademia Leyer*, Faceta Jurídica, julio-agosto de 2019, p. 61.

tidad respectiva que expida una copia para que pueda servir de prueba documental durante el proceso.

- Documentos incorporados durante diligencia de inspección judicial: Durante la práctica de una diligencia se recibe un documento a petición de parte o de oficio por el juez, que se refiera a los hechos objeto de la inspección.

En otros eventos puede surgir el inconveniente de que para facilitar el aporte o valoración del documento al proceso, se presente la evidencia física que contiene la información digital, como el disco duro de un computador o un celular. Sobre el particular, Aige (2014: 94) afirma: «Cuando dice que se deberán aportar en su “soporte papel original”, da por hecho que todos los documentos tienen un soporte original, cuando hoy en día puede que no sea así y que el soporte original sea directamente electrónico». Así las cosas, la parte debe aportar la información contenida en forma electrónica y no la evidencia física.

En relación con la presentación de la prueba digital en estos procesos, es frecuente que los abogados aporten la prueba digital mediante documentos impresos en papel. De este modo, el medio de prueba del documento electrónico que está compuesto por bytes de información. En posición doctrinal de Guzmán: «No se puede someter a contradicción ni a ningún estudio pericial, por lo cual se vulneran garantías de la defensa y contradicción, al momento de presentar pruebas como mensajes de chats en documentos impresos, variando la naturaleza tecnológica del mensaje de datos original».¹⁰ De esta manera, la forma de presentación de la prueba digital también incide en las disposiciones normativas con las que cuenta el juez para valorar el mensaje de datos presentado.

A partir de lo anunciado, es necesario profundizar en cómo garantizar la autenticidad de los mensajes de Whatsapp, asunto que se abordará en el siguiente apartado.

Elementos estructurales de la autenticidad en la presentación de los mensajes de Whatsapp

En este acápite se abordará lo relacionado al concepto, conservación y manejo de la autenticidad en el proceso, con miras a establecer si existen mecanismos jurídicos y tecnológicos que permitan garantizar la igualdad de la prueba recogida del soporte informático respecto de aquella que finalmente es aportada, controvertida y valorada por el juez.

Para empezar, la Ley Estatutaria de Administración de Justicia 270 de 1996, que reguló el ejercicio de la justicia en el país, facultó a los jueces y magistrados de todas

10. Comunicación personal con Andrés Guzmán, abogado, experto en tecnología y certificado por la Unión Europea en manejo de crimen informático y evidencias digitales, 17 de julio de 2017.

las jurisdicciones para valorar los medios de prueba que trajera consigo la innovación de la tecnología, pero sujetos a unos requisitos especiales, como se expone en el artículo 95:

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.

De la norma expedida se pueden establecer deberes para la justicia nacional de mejorar 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. Asimismo, resulta claro que con los avances tecnológicos, los operadores judiciales tienen amplias facultades para aprovechar las bondades de las tecnologías de la información y la comunicación, para darle valor a las pruebas digitales, incluyendo especialmente la autenticidad como requisito de validez del documento electrónico. Sobre la importancia de la autenticidad en el proceso judicial, Guimaraes (2019: 534) 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».

En cuanto a la autenticidad, Guimaraes (2019: 534) señala: «Es auténtico, según la doctrina, aquel documento que identifica a su autor». En este orden de ideas, la autenticidad es uno de los elementos de la cadena de custodia que se aplica a cualquier clase de evidencia física o electrónica, aun con la posibilidad de que se altere, se modifique o sea manipulada.

Dado lo anterior, el proceso de divorcio no es ajeno a la posibilidad de alterar el estado original de la prueba digital al presentarla en un papel para tratar de demostrar o desvirtuar un hecho ante el juez, lo que deja a un lado el requisito de autenticidad. Al respecto, Toro (2019: 62) afirma:

Llama la atención que posiblemente, amparado en la neutralidad tecnológica permita que se pueda utilizar otro formato «que permita demostrar que reproduce con exactitud la información generada»; pero ¿cómo sabe el juez que realmente reproduce con exactitud el mensaje de datos original, si no conoce el original para poder determinar dicha exactitud? En nuestra legislación, lo que importa en el documento no es el medio, sino la representación de un hecho, esto cambia drásticamente lo que puede llevar a decisiones judiciales equivocadas.

En este orden de ideas, en el caso de un divorcio, la parte interesada debe convencer al juez de familia de que la información aportada no es inventada sino, por el contrario, obtenida bajo los lineamientos en materia de cadena de custodia, cuyo objetivo es básicamente demostrarle al funcionario judicial que las pruebas obtenidas del lugar de los hechos son las mismas de aquellas que se le presentaron en el caso y que luego serán el fundamento de la sentencia. El juez decidirá si, con base en las pruebas practicadas, se configura o no una causal de divorcio para, en caso afirmativo, decretar la decisión de forma obligatoria para las partes.

En este orden de ideas, se abordará si es posible establecer mediante herramientas tecnológicas la autenticidad de los mensajes de Whatsapp, o si por el contrario no es posible garantizarla debido a su volatilidad. Sobre el particular, Abel (2019: 570) afirma: «Para verificar la integridad —al igual que la autenticidad— de la prueba electrónica deberá partirse de un código *hash*». Es claro entonces que se debe precisar el significado de esta herramienta informática; para ello, Delgado (2018: 71) afirma: «El *hash* es una función basada en un algoritmo que permite afirmar que los datos que se encontraban en el dispositivo en el momento de su ocupación no han sido objeto de manipulación posterior».

El código *hash* es un medio idóneo para asegurar las evidencias digitales. Se trata de un algoritmo matemático que hace un cálculo dependiendo de la información, y genera una cadena de caracteres, asegurando la evidencia para certificar que no ha sido modificada respecto de la original.

En la actualidad, las herramientas forenses permiten llevar a cabo el código *hash*, lo cual es una imagen, una copia bit a bit¹¹ o una copia exacta del contenido que tiene el dispositivo, e inmediatamente se calcula el *hash*, lo que permite extraer todo o solo una parte de la información. Por ejemplo, se pueden extraer solo las conversaciones de Whatsapp de un teléfono celular, en lugar de todos los demás archivos. Respecto de lo anterior, si una persona escribe un documento en Word, se calcula el *hash* y el software brinda unos caracteres; si luego se le agrega una coma o cualquier clase de letra al mismo documento, al calcular nuevamente el *hash* con el archivo modificado, este no resultará igual al anterior, lo que actúa como evidencia de que el archivo fue manipulado, con consecuencias desfavorables en el proceso para la parte que aportó dicha prueba. Al respecto, Delgado (2018: 80) afirma: «Si concurren dudas sobre la autenticidad o integridad de los datos, resultará muy probable que el juez deniegue fuerza o eficacia probatoria a la prueba».

Así las cosas, el código *hash* puede ser incorporado al proceso de divorcio mediante un perito en informática forense. Una parte fundamental es empezar por la recolección, hacer una copia bit a bit de la evidencia digital, y así quedan archivos

11. «Copia bit a bit» se refiere al elemento mínimo de memoria de un dispositivo, en el que se hace un clonado forense de discos duros que copia la información a otro dispositivo de almacenamiento.

completamente idénticos, lo cual se denomina «copia espejo» o imagen ISO. Así, después de que se tienen dos elementos idénticos, el perito en informática forense trabaja sobre uno y guarda el otro intacto. Cuando termina, se extrae el código *hash*, el cual equivale a un algoritmo alfanumérico como una huella digital. De este modo, toda manipulación que se haga luego a la evidencia podrá ser identificada de inmediato. Al respecto, Shick y Toro (2017: 465) afirman:

Para ser tan confiable como los archivos originales, la integridad de la evidencia duplicada debe ser verificada. Uno de los métodos de verificación comúnmente aplicado es el *hash*, el cual es una técnica para la identificación única de archivos idénticos. Un *hash* es una huella digital de un archivo o colección de datos, representada como una cadena de datos binarios escrita en notación hexadecimal.

La **figura 1** presenta una imagen que representa el código *hash*, creado a partir de un texto, archivo o contraseña, y que genera una combinación compuesta de letras y números que representa la información.

En este orden de ideas, después de que se obtenga el código *hash*, se crean dos archivos: se guarda uno que se deja intacto, mientras el perito efectúa su labor forense digital sobre otro documento electrónico. En este último caso queda la copia guardada con ese *hash*, que es el mismo que se le entrega a la contraparte, y a esta le debe aparecer igual. Este método es el mismo para la comunidad internacional, y hay herramientas de diferentes proveedores. Por ejemplo, Encase es un software forense utilizado para recoger, preservar información digital y analizar los datos en un dispositivo.

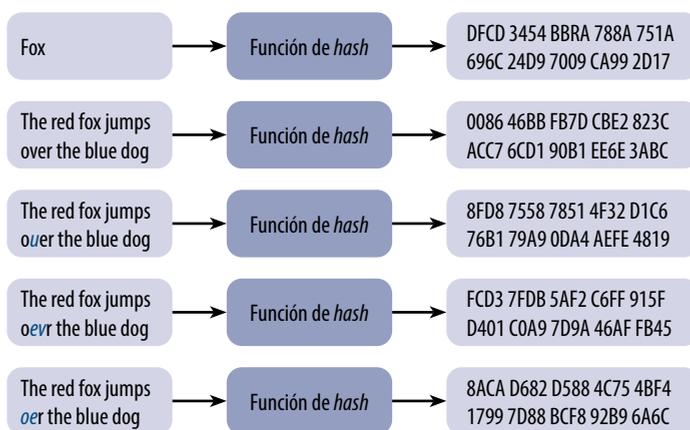


Figura 1. Código *hash*.

Fuente: Pedro Gutiérrez, «¿Qué son y para qué sirven los *hash*?: Funciones de resumen y firmas digitales», *Genbeta*, 15 de enero de 2013, disponible en <https://bit.ly/3HdVbgc>.

También se aplica en estos casos la norma ISO 27.037, «Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital», la cual pretende garantizar la integridad y autenticidad de la prueba digital:

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.¹²

Así las cosas, este es uno de los protocolos conocidos por la comunidad internacional por la creación de la informática, en la cual se ha desarrollado el proceso de clonado de la información, para evidenciar que los datos son exactamente los mismos a los recogidos en los dispositivos. Al respecto, Rodríguez (2018: 31) afirma:

Una vez que se accede o se obtienen los datos del dispositivo, se procede al volcado o clonado de los mismos, que supone realizar una copia espejo o bit a bit de la información obrante en el mismo. Esta podrá hacerse en el mismo lugar en que se encuentra o en un momento posterior. Básicamente, lo que se realiza es una copia física del contenido del mismo. Pero es mediante el hash, una función basada en algoritmos que otorga al contenido de un archivo un valor numérico, como se corrobora que los datos que se encontraban en el dispositivo original no han sido manipulados y, por tanto, son los mismos que los que se hallan en la copia.

Adicionalmente, hay otras pautas que deben garantizarse en este tipo de procedimientos. Sobre el particular, Ángel afirma:

Hay que hacer proceso con cadena de custodia, para garantizar que no hay modificación en la evidencia, toda vez que no es una copia. Por eso son costosos los procesos de captura digital forense, cuando se usan los estándares válidos para que no sean objeto de debate en juicio.¹³

En estos términos, se debe precisar que la falta de autenticidad no impide que se excluya la evidencia, toda vez que en derecho la consecuencia de la falta de autenticidad es distinta a la de ilicitud, ya que, ante pruebas que puedan resultar modificadas, el juez de familia efectivamente sí puede valorarlas. Sobre el particular, Arango señala:

12. «ISO/IEC 27037:2012(en): Information technology; security techniques; guidelines for identification, collection, acquisition and preservation of digital evidence», Online Browsing Platform, disponible en <https://bit.ly/3BZyU1T>.

13. Comunicación personal con Byron Ángel, ingeniero de sistemas, perito informático forense, docente universitario y miembro de LawTic, 19 de noviembre de 2019.

La autenticidad y legalidad de la evidencia en el derecho son diferentes: una evidencia sin ser auténtica puede ser valorada en el proceso, el juez mira a cuál le da mayor valor. Si hay una evidencia presentada por un servidor público, se presume auténtica y el juez por error le puede dar mayor énfasis, lo cual es una falacia argumentativa.¹⁴

Dado lo anterior, se puede establecer que los efectos jurídicos de la falta de autenticidad son distintos a los de ilicitud de la prueba digital, además de que el código *hash* es una herramienta que brinda la tecnología para asegurar la autenticidad de una prueba digital, que permite ofrecer un alto grado de confiabilidad y validez en un caso de divorcio, solo en caso de ser efectivamente utilizada. No obstante, en muchas ocasiones su alto costo dificulta su práctica en un proceso, dado que estos deben ser asumidos por la parte que aporta la prueba, sin que ello necesariamente le asegure un resultado favorable.

Elementos estructurales del principio del debido proceso en la valoración de los mensajes de Whatsapp

Este acápite se ocupa de desarrollar la relación de las pruebas digitales con el principio del debido proceso. En este sentido, el objeto de estudio permitió determinar qué situaciones generaban una vulneración del principio del debido proceso presentando un estudio en los juzgados de familia de Medellín, Colombia, al momento de practicarse mensajes de Whatsapp en un caso. Asimismo, se abordará cómo se ejerce el derecho a la defensa y la contradicción de una prueba pericial informática, cómo se conserva la cadena de custodia y cómo se asegura que la labor del perito en informática forense sea creíble y le ofrezca pleno valor probatorio al funcionario judicial.

Para empezar, en Colombia cobra especial importancia el principio del debido proceso, aplicable a cualquier actuación judicial o administrativa. Al respecto, Rojas (2017: 230) afirma:

El concepto de debido proceso sugiere una actividad constitucionalmente incuestionable y ceñida a las instrucciones impartidas por el legislador para su realización, lo cual descarta el recuerdo a cualquier actividad ilegítima aun cuando con ella se asegure alcanzar el resultado anhelado que de otra manera sería incierto, o se garantice su realización más rápida y fácil.

Por lo anterior, conviene resaltar una definición del concepto del *debido proceso*, el cual contiene múltiples acepciones. De acuerdo con la Corte Constitucional

14. Comunicación personal con Andrés Felipe Arango, abogado especialista, magíster en Derecho Penal y candidato a doctor en Derecho de la Universidad de Medellín, defensor público y docente universitario, 19 de noviembre de 2019.

consiste en «el conjunto de garantías previstas en el ordenamiento jurídico, a través de las cuales se busca la protección del individuo incurso en una actuación judicial o administrativa, para que durante su trámite se respeten sus derechos y se logre la aplicación correcta de la justicia».¹⁵

Además, el principio del debido proceso cobra mucha más relevancia en el derecho internacional, según afirman autores como Salmón y Blanco (2012: 24):

El proceso es un medio para asegurar en la mayor medida posible, la solución justa de una controversia, a lo cual contribuyen el conjunto de actos de diversas características generalmente reunidos bajo el concepto de debido proceso legal.

Es claro, entonces, que la importancia del debido proceso radica en ser un límite para la actuación del Poder Judicial en las democracias actuales, y es la base de la justicia en un caso, pues sería un contrasentido adelantar un proceso sin el fiel cumplimiento de este principio cometiendo injusticias, situación que hace necesario determinar en qué aspectos de la vida cotidiana podría vulnerarse con la práctica de una prueba digital. Por tanto, es necesario analizar de qué manera se protege el debido proceso y qué incidencia tiene la carencia de su protección sobre la validez o credibilidad de la prueba digital incorporada en los casos de divorcio.

La vulneración del debido proceso con la práctica de mensajes de Whatsapp en casos de divorcio

Se pretende detallar cómo se dan los mensajes de Whatsapp en el proceso de divorcio y en qué tipo de casos se puede vulnerar el principio del debido proceso. Para empezar, dada la libertad de aportar la prueba al proceso, la legislación colombiana permite que se presente la prueba digital de forma impresa en un papel, situación que, a diferencia de otras formas de aportación en el caso, sí varía su estado original e incide en la protección del debido proceso de la parte sobre la cual se aduce. Al respecto, Guzmán (2017) 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.¹⁶

En este orden de ideas, de acuerdo con los peritos en informática forense que fueron entrevistados en la investigación, en los procesos de divorcio se han encontrado casos con pruebas digitales que fueron convertidas en impresiones de correos

15. Corte Constitucional de Colombia, sentencia C-341, 2014.

16. Comunicación personal con Andrés Guzmán, 16 de diciembre de 2017.

electrónicos o de conversaciones de Whatsapp, que se transcriben manualmente con un computador; en otros casos, fueron introducidas fotografías impresas, en las que no era posible validar si se había modificado la foto original; también se refirieron a casos de divorcio en los que se han aportado videos sin definir la fuente original, o sin determinar si se vulneró la privacidad de alguna de las partes, aspectos que debieron evitarse para no sacrificar el debido proceso.

En otros casos, cuando un usuario quiere evidenciar relaciones sexuales extra-matrimoniales por un mensaje de Whatsapp, es necesario que le acredite al juez de familia cuál es el número de su cónyuge. Dado lo anterior, es necesario que, con un derecho de petición al operador de comunicaciones, se indique quién es el titular o suscriptor de esa línea telefónica, pues este aspecto no debe quedar en duda en el proceso. Además, puede ocurrir que llegue la respuesta del operador en que se certifique que efectivamente esa línea si es del cónyuge o que el operador indique que no puede dar esa información, porque está protegida por protección de datos personales (intimidad). En este último caso, se debe esperar que el juez admita la prueba de oficio, con previa solicitud desde el escrito de demanda o en su contestación. En Colombia, el Código General del Proceso le otorga amplias facultades de oficio a los jueces de familia; no obstante, en principio les impone la carga a las partes del caso de presentar las pruebas ante el juez, para que decida conforme a derecho; en este tipo de procesos, cuando una de las partes no logre obtener una prueba, el juez podrá disponer oficiosamente la autoridad o parte que tiene la información, que la envíe al despacho judicial para examinar su contenido.

Además, ante la eventual necesidad del juez de obtener una copia de las conversaciones de la aplicación de mensajería instantánea para validar si se acredita o no la causal de divorcio, estas comunicaciones se almacenan en los dispositivos, pero no en los servidores. Sobre el particular, Mesa (2017: 241) afirma:

La ausencia de respaldo de información transmitida en el servidor de WhatsApp pareciera ser una amenaza para lograr el propósito del reconocimiento como mensaje de datos, porque la funcionalidad del cifrado con protocolo Signal impide a Whatsapp que los datos y la información transferidos por su canal de procesamiento de datos quede almacenada en su servidor propio, solo queda respaldo en cada dispositivo (extremo), hecho que obliga a contar con el dispositivo tanto del remitente y destinatario si se quiere una trazabilidad fiable, íntegra y auténtica de la comunicación, evitando desconocimiento o nulidades de la prueba, salvo, eso sí, que se logre el reconocimiento de parte sobre quien se alega la existencia de los mensajes transferidos en el proceso.

Asimismo, con algunos permisos de la aplicación Whatsapp es posible borrar mensajes enviados, sin que le quede registro al otro usuario de que se eliminó parte de la conversación, mientras que en otros teléfonos sí queda el registro de la infor-

mación; de este modo, la cadena de conversación con estas herramientas puede presentar alteraciones, lo que trae como consecuencia que la prueba pierda integridad, que es un requisito esencial de la Ley 527 de 1999 para ser valorada y practicada en el proceso. Además, pueden borrarse por distintos factores, Aguirre (2019: 75) afirma: «Pueden ser destruidos o alterados a través de virus informáticos». Como consecuencia de lo anterior, el problema detectado se traduce en que se han incorporado estas pruebas a algunos procesos de divorcio y algunos jueces las han admitido, brindándole valor legal. Incluso expertos como Fernández afirman: «Hay que evitar presentar estas evidencias de forma impresa, este medio de prueba no se puede someter a contradicción ni a ningún estudio pericial».¹⁷

Este tipo de dificultades en parte se deben a que la Escuela Judicial Rodrigo Lara Bonilla «no había incluido el tema de las pruebas digitales dentro de los planes de formación en tecnologías de la información y las comunicaciones. Solo hasta 2020 este tema se incluyó en las capacitaciones a funcionarios judiciales».¹⁸ Este aspecto evidencia la casi nula capacitación por parte de expertos a los jueces de familia en esta temática, quienes han tenido que aprender sobre el manejo de pruebas tecnológicas por sus propios medios.

La Corte Constitucional se ha pronunciado sobre los casos en que se modifica el formato digital a un soporte físico, en atención a la protección del debido proceso, regulado como derecho de rango fundamental en el artículo 29 de la Carta Magna. La Corte ha indicado que

la información pasa de estar contenida en un dispositivo electrónico, que asegura la integridad, autenticidad e inalterabilidad de la información, a un soporte de papel sin esa capacidad técnica, por lo cual, el elemento material probatorio resulta modificado y se convierte en una mera reproducción de su original.¹⁹

Respecto de este problema probatorio, la Corte Constitucional también se pronunció en sentencia T-043 de 2020, en un caso en que se aportaron unos Whatsapp impresos y la Corte, en un confuso fallo, cita doctrina argentina de hace 30 años y afirma que por haber sido aportada la prueba impresa en papel, esta tiene carácter de prueba indiciaria. De este modo, desconoce su propio precedente y el hecho de que, en su regulación, el Código General del Proceso le asigna el carácter de prueba documental. Al respecto, el magistrado Reyes afirma:

17. Comunicación personal con Juan Fernández, abogado, gerente y fundador de Tecnogados, 22 de marzo de 2018.

18. Comunicación personal con Mary Lucero Novoa, abogada especialista en derecho administrativo, derecho penal y criminalística, magíster en Filosofía del Derecho y Teoría Jurídica, directora de la Escuela Judicial Rodrigo Lara Bonilla, 4 de mayo de 2020

19. Corte Constitucional de Colombia, sentencia C-604, 2016.

Los operadores judiciales diariamente deben analizar elementos extraídos de aplicaciones de mensajería instantánea, sobre estas últimas, la doctrina especializada les ha concedido el valor de prueba indiciaria ante la debilidad de dichos elementos, frente a la posibilidad de realizar alteraciones en el contenido, por lo cual deben ser valoradas de forma conjunta con los demás medios de prueba.²⁰

Por consiguiente, diversos expertos se han manifestado en torno al fallo de la Corte Constitucional con algunas críticas académicas. En este contexto, Otero afirma: «Los pantallazos deberían considerarse pruebas documentales, y como cualquier otro documento gozan de la presunción de autenticidad, salvo que sea cuestionada por la parte contra la que se aduce»;²¹ mientras que Garzón afirma: «Es correcto que la Corte tenga en cuenta el WhatsApp como medio de prueba, pero en lo que se equivoca es en indicar que es una prueba indiciaria, el medio electrónico en este caso es documental».²² En síntesis, para diversos autores, la Corte Constitucional confunde el medio de prueba aplicable, toda vez que en principio sería aplicable las reglas de la prueba documental.

En este sentido, otros autores presentan una posición en torno al principio constitucional de la buena fe. Al respecto, Canosa afirma:

Se garantiza la contradicción, porque se podrá tachar o desconocer, es inaceptable sostener que porque un documento pueda ser alterado, se pueda exigir autenticaciones con prueba periciales, esto puede desconocer el artículo 83 de la Carta Política y trasgredir el artículo 11 del Código General del Proceso, que prohíbe realizar formalidades innecesarias para no incurrir en excesos rituales manifiestos.²³

Otras posiciones de expertos se encargan de referirse a los requisitos legales para acreditar un hecho mediante un Whatsapp. Sobre el particular, Toscano afirma: «Para valorar adecuadamente estas pruebas es imprescindible tener en cuenta su confiabilidad, en cuanto a su generación, archivo, integridad y procedencia».²⁴ Además, se deben tener en cuenta los requisitos técnicos de las pruebas digitales, establecidos en los artículos 6, 7, 8 y 9 de la Ley 527 de 1999. Al respecto, Guzmán afirma:

20. Corte Constitucional de Colombia, sentencia T 043, 10 de febrero de 2020.

21. Comunicación personal con Liliana Otero, abogada egresada de la Universidad del Rosario, con especialización en derecho procesal, Universidad Colegio Mayor de Nuestra Señora del Rosario, 8 de abril de 2020.

22. Comunicación personal con Fabián Garzón, abogado y filósofo, magíster en Derecho Procesal Constitucional, doctor en Derecho, profesor universitario, 8 de abril de 2020.

23. Comunicación personal con Ulises Canosa, abogado de la Universidad Libre. Se ha desempeñado como conjuer de la Sala Civil del Tribunal Superior de Bogotá, 8 de abril de 2020.

24. Comunicación personal con Fredy Toscano, abogado de la Universidad Externado de Colombia, conciliador extrajudicial en derecho, especialista en derecho procesal de la Universidad Externado de Colombia, 8 de abril de 2020.

La Ley 527 de 1999 trae unos requisitos de validez jurídica para que aquello que está electrónicamente presentado ante el juez tenga el mismo valor de un medio físico, los cuales son: 1) que esté escrito, o sea, que la información se pueda abrir para su posterior consulta; 2) que esté firmado, mediante cualquier forma de identificar el iniciador de un mensaje de datos; 3) que sea original, es decir, que no ha sido alterado desde que se generó en su forma definitiva. Esto se garantiza con un sistema de cadena de custodia, que brinda un laboratorio en informática forense certificado, y dotado con herramientas forenses.²⁵

Dado lo anterior, la Corte Constitucional, en sentencia T-043 de 2020, incurre en una confusión al afirmar que la prueba impresa en papel tiene carácter de prueba indiciaria, toda vez que el legislador desde el antiguo Código de Procedimiento Civil, y ahora con la regulación del Código General del Proceso, le ha mantenido el tratamiento normativo de medio de prueba documental. Las pruebas indiciarias tienen una naturaleza distinta.

Además, es importante exponer otros casos, como la sentencia T-916 de 2008, con magistrada ponente Clara Inés Vargas, en la que se analiza la exclusión de unas pruebas digitales dentro de una diligencia de interrogatorio de parte, en un proceso de divorcio en curso. En el caso ocurrió que el apoderado de la parte demandante le presentó al interrogado unos correos electrónicos que no se encontraban dentro del expediente, y a partir de ellos hizo preguntas al testigo.

Así las cosas, la parte contraria objetó la pregunta efectuada, pero la jueza de familia no accedió favorablemente, por lo cual interpuso el recurso de reposición y en subsidio apelación, argumentando que se viola el debido proceso al no tener la oportunidad de controvertir esa prueba documental, que se adujo dentro de la diligencia. Es de resaltar que los correos electrónicos que se le exhibieron al testigo no habían sido aportados antes en la demanda, ni eran conocidos en el caso, situación que resultó sorpresiva para el apoderado del demandado.

En este caso, el problema jurídico que se planteó es si los mecanismos resultan idóneos y eficaces para garantizar la protección de derechos fundamentales como el debido proceso, el acceso efectivo a la administración de justicia y el derecho a la intimidad.

Como respuesta a este problema jurídico, la Corte Constitucional señaló en sentencia T-916 de 2008 lo siguiente:

El correo electrónico, por tratarse entonces de un dispositivo que tiene un ámbito privado, es que la regla constitucional prevista en el artículo 15 superior, referida a la inviolabilidad de la correspondencia y demás formas de comunicación privada, tiene total aplicabilidad cuando se trata de correos electrónicos, pues se trata de una

25. Comunicación personal con Andrés Guzmán, 8 de abril de 2020.

forma de comunicación entre personas determinadas, siendo solamente posible su interceptación o registro: i) mediante orden de autoridad judicial, ii) en los eventos permitidos en la ley y iii) con observancia estricta de las formalidades que la misma establezca.

En este sentido, a juicio de la Corte Constitucional, los mensajes de datos que fueron allegados por el apoderado de la parte demandante al caso de divorcio son pruebas ilegítimas, por cuanto fueron obtenidas de la cuenta personal del accionante, sin su consentimiento. En este sentido, se aplicó el precepto constitucional de que una comunicación privada por regla general es inviolable. Al respecto, Abel (2019: 572) afirma: «Sería una prueba electrónica ilícita la del exmarido que se introduce en el nuevo domicilio de la exesposa y graba conversaciones de ella con un tercero a partir de un dispositivo móvil».

En consecuencia, la Corte Constitucional ordenó a la jueza Once de Familia de Medellín excluir del proceso de cesación de los efectos civiles de matrimonio católico los correos electrónicos allegados por el apoderado de la parte demandante, en la diligencia de interrogatorio de parte iniciada, con el fin de que no fueren tenidos en cuenta al momento de proferir sentencia.

Así, la Corte reafirma que, en casos de divorcio, interceptar un sistema informático ajeno de uno de los miembros del grupo familiar constituye una clara violación del derecho a la intimidad, toda vez que no está de por medio el consentimiento del afectado.

Las formas de ejercer el derecho a la defensa y la contradicción de los mensajes de Whatsapp

En este acápite se pretende exponer algunas figuras jurídicas que podrán invocarse en el proceso, si la parte contra la cual se aduce detecta que existe alguna alteración, modificación o manipulación de la información digitales, las cuales se explican a continuación.

La *tacha* será procedente, de conformidad con el artículo 269 del Código General del Proceso, frente a mensajes de datos en formato original que contengan firma digital. En este caso, la carga de demostrar la falsedad del documento es de quien lo tacha, es decir, contra quien se aduce.

El *desconocimiento por mensaje de datos*, de acuerdo con el artículo 272 del Código General del Proceso, será procedente para aquellos datos presentados en formato original, pero no firmados, mientras que para aquellos impresos se puede solicitar el cotejo con el original. En este sentido, si la prueba digital se presenta como impresión, se puede solicitar el cotejo con el original, es decir, ir a la fuente, que pudo ya haberse perdido o de que no haya manera de acceder a la misma, por tanto, ese documento no podría ser valorado.

La *cláusula de exclusión* hace referencia al párrafo final del artículo 29 de la Constitución Política de Colombia, que establece: «Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso». Tal nulidad no debe entenderse como aquella propia del derecho privado, sino como aquella exclusión del material probatorio con el que cuenta el juez para decidir con respecto a pruebas ilícitas o legales, es decir, que hayan sido obtenidas con violación a derechos fundamentales, lo que no ocurre frente a aquellas pruebas donde se discuta la autenticidad o la cadena de custodia, que tiene efectos jurídicos distintos, esto es, se ve afectada su credibilidad dentro del caso. En los casos de divorcio es mucho más evidente la difícil labor probatoria de acceder a la información del cónyuge. Al respecto, Ezurmendia Álvarez (2020: 4) afirma: «Gran parte de la evidencia disponible está en el límite de la vulneración de la privacidad, la honra, la inviolabilidad del hogar, de un sujeto, pudiendo caer en la tentación de la sobreexclusión».

Teniendo presente lo anterior, se cuentan con diversos mecanismos para hacer efectivo el derecho a la defensa y la contradicción en casos en que se practican mensajes de Whatsapp. Mientras los dos primeros mecanismos se diferencian por la forma del documento electrónico, la cláusula de exclusión alude a la obtención de pruebas tecnológicas en que se vulneraron derechos fundamentales.

También es importante mencionar que el legislador colombiano autoriza a que se presente la prueba digital en formato en papel. Sin embargo, la parte contra la cual se aduce la prueba tiene la obligación de impugnar, en caso de que la prueba esté adulterada o modificada; de lo contrario, en caso de permanecer en silencio, la prueba produce plenos efectos jurídicos. Incluso el juez tiene la obligación de revisar la autenticidad de la prueba, de forma oficiosa, sin necesidad de que una de las partes la alegue, determinando si ha sido modificada, si el contenido original aún existe en el medio informático, de dónde se envió el mensaje, cómo se envió, y si se pudo establecer su autor; de lo contrario, con su omisión se puede vulnerar el principio del debido proceso de la parte contra la que se adujo la prueba digital.

Por tanto, es importante abordar el concepto, alcance y situaciones en que se debe impugnar una prueba digital, en atención al ejercicio de defensa y contradicción, que debe efectuar la parte contra la cual se aduce la prueba. Sobre el particular, Martínez (2018: 138) afirma: «La impugnación de la autenticidad se da cuando se presume o se tiene certeza de que el autor del documento no es realmente o se tiene certeza de que el autor del documento no es realmente la persona a la que se atribuye tal autoría».

En este sentido, tal impugnación no debe ser planteada por una de las partes en cualquier fase del proceso, sino en momentos específicos; de lo contrario, la prueba será considerada auténtica y deberá ser valorada por el juez, con las demás pruebas aportadas válidamente al proceso. De allí la particularidad de nuestro sistema judicial, que exige abogados activos en la defensa de los intereses de su poderdante. Al respecto, Martínez (2018: 138) afirma:

Lo común es que el demandado se pronuncie sobre la autenticidad de los documentos presentados por el actor y que lo haga en la contestación de la demanda; lo mismo cabe decir cuando exista reconvencción; cabe recalcar que en la audiencia cada parte debe pronunciarse sobre los documentos presentados, manifestando si los admite o impugna o reconoce o si, en su caso, propone alguna prueba acerca de su autenticidad.

En relación con las pautas que deben observarse al momento de impugnar la prueba digital, Abel (2019: 577) afirma:

Precisar el motivo de la impugnación, esto es, si es por falta de autenticidad, de integridad, de exactitud o por ilicitud, evitando la impugnación genérica. Precisar el motivo de la impugnación, esto es, si va referida a una palabra o una expresión concreta y determinada, o varias palabras o expresiones y, en este último caso, el contexto en que se pronuncian tales palabras o expresiones.

Así las cosas, la misma legislación traslada la carga de impugnar a la parte contra la cual se aduce la prueba, su inactividad o descuido por impugnar si resultare aplicable alguna de las circunstancias mencionadas, genera que resulte afectado el derecho a la defensa y contradicción de una de las partes en el proceso, por lo que el juez también debe actuar en procura de la legalidad en estos casos de forma oficiosa.

Conclusiones

Sin duda, en los casos en los cuales los jueces le dan pleno valor probatorio a mensajes de Whatsapp aportados de forma impresa en papel (en atención a la presunción del artículo 244 del Código General del Proceso y el principio constitucional de la buena fe), y sin verificar la autenticidad del mensaje de datos (pese a que existe la tecnología y los procedimientos técnicos mediante peritos en informática forense que garantiza la mismidad de las pruebas tecnológicas), se vulnera el debido proceso. Los jueces deben valorar la prueba de acuerdo con las reglas de la sana crítica, revisando la configuración de los requisitos del mensaje de datos, esto es, si la información es accesible, si se puede identificar su autor, si es íntegra y si es confiable (Ley 527 de 1999, artículo 11). El argumento recae no desde el punto de vista formal —pues los jueces pueden conservar las formalidades propias de los casos y excluir las pruebas ilegalmente obtenidas—, sino desde el punto de vista material, toda vez que la parte contra la cual se aduce la prueba, desde cuestiones técnicas, no tiene cómo ejercer el derecho a la defensa y la contradicción mediante un estudio pericial, puesto que no se puede establecer la originalidad e integridad del mensaje de datos (si eventualmente fue modificado por la parte que lo aporta o terceros).

Los mensajes de Whatsapp que no son auténticos en los casos de divorcio, por ejemplo, cuando se cambió una parte de la conversación original, sí pueden ser va-

lorados por el juez de familia. En este sentido, la falta de autenticidad no genera la exclusión de la prueba. Sin embargo, en el mundo ideal, debería ser un presupuesto para la aducción válida al proceso de la prueba digital que esta sea auténtica, siguiendo el enfoque inicialmente planteado por la Ley 270 de 1996, toda vez que la credibilidad de las pruebas tecnológicas se ve reducida en la medida en que se desacredite su seguridad y autenticidad. En cualquier caso, los efectos jurídicos de la falta de autenticidad son distintos a los de la ilicitud de la prueba digital, ya que, en caso de ser obtenida con violación de derechos fundamentales, deberá ser excluida por parte del juez.

El código *hash* es un algoritmo matemático que garantiza que las pruebas digitales no están alteradas ni modificadas, que puede ser verificada en cada copia, y que puede ser incorporado al caso de divorcio mediante el dictamen pericial de un experto en lo forense digital. Así las cosas, si se le aplica el código *hash* a un archivo digital, y luego se le suprime o añade alguna letra, el código *hash* cambiará. No obstante, la utilización de esta herramienta es muy poco frecuente en los procesos, dados los altos costos de los laboratorios y peritos en informática forense, que debe ser asumido directamente por la parte que aporta la prueba, lo cual implica abordar en otros estudios cómo garantizar el acceso a la administración de justicia y al derecho a probar de quien no cuenta con los medios económicos para asumir estos costos.

El caso analizado en sentencia T-043 de 2020, en que se aportaron unos mensajes de Whatsapp impresos, generan confusión en la aplicación del precedente judicial, toda vez que la Corte Constitucional cita doctrina argentina de hace treinta años, y afirma que por haber sido aportada la prueba impresa en papel esta tiene carácter de prueba indiciaria, desconociendo su propio precedente jurisprudencial, desarrollado a partir de las sentencias C-662 del 2000, C-831 de 2001 y C-604 de 2016, y que en su regulación normativa, el Código General del Proceso le asigna el carácter de medio de prueba documental a los mensajes de datos. Por último, la facilidad para modificar mensajes de Whatsapp, aun sin los mayores conocimientos técnicos por medio de aplicaciones gratuitas, genera la necesidad de revisar minuciosamente la autenticidad de los mensajes, para evitar desconocer el derecho de defensa y contradicción, de la parte contra la cual se aducen en el proceso.

Referencias

- ABEL, Xavier (2019). «La impugnación de la prueba tecnológica». *Justicia: Revista de Derecho Procesal*, 1: 217-266. Disponible en <https://bit.ly/3qsOL76>.
- AGUIRRE, Juan (2019). *Implicaciones de la valoración probatoria del documento electrónico en Colombia*. Tesis de Maestría, Universidad Santo Tomás, Tunja. Disponible en <https://bit.ly/3oiDS53>.
- DE ASIS, Miguel (2020). «La incidencia de las nuevas tecnologías en el derecho al de-

- bido proceso». *Ius et Scientia*, 6 (2): 186-199. DOI: [10.12795/IETSCIENTIA.2020.102.12](https://doi.org/10.12795/IETSCIENTIA.2020.102.12).
- DELGADO, Joaquín (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: Wolters Kluwer.
- DUQUE, Sandra, Flor González, Nora Cossio y Sandra Martínez (2018). *Investigación en el saber jurídico*. Medellín: Universidad de Antioquia.
- EZURMENDIA ÁLVAREZ, Jesús (2020). «Problemas relativos a la prueba en cada etapa de la actividad probatoria en el procedimiento de familia». *Revista Chilena de Derecho*, 47 (1): 101-118. DOI: [10.4067/S0718-34372020000100101](https://doi.org/10.4067/S0718-34372020000100101).
- GUIMARAES, Darci (2019). «La prueba digital». En Dimaro Agudelo (compilador), *La prueba: Teoría y práctica* (pp. 521-539). Medellín: Universidad de Medellín.
- MARTÍNEZ, Pedro (2018). *La valoración y motivación de la prueba y su procedimiento en la jurisprudencia*. Lima: Grijley.
- MESA, Ana (2017). «Cifrado de extremo a extremo de Whatsapp: Un análisis a partir de la prueba documental». En Dimaro Agudelo (compilador), *La prueba: Teoría y práctica* (pp. 221-253). Medellín: Universidad de Medellín.
- RODRÍGUEZ, Marta (2018). *La prueba digital en el proceso penal*. Tesis de Maestría, Universidad de La Laguna, Madrid. Disponible en <https://bit.ly/3qvp3yH>.
- ROJAS, Miguel (2017). *Eficacia de la prueba obtenida mediante irrupción en la intimidad*. Bogotá: Universidad Externado de Colombia.
- SALMÓN, Elizabeth y Cristina Blanco (2012). *El derecho al debido proceso en la jurisprudencia de la Corte Interamericana de Derechos Humanos*. Lima: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú.
- SALT, Marcos (2017). «Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos». Buenos Aires: Ad-Hoc.
- SHICK, Kyung y Marlon Toro (2017). *Cibercriminología: Guía para la investigación del cibercrimen y las mejores prácticas en seguridad digital*. Bogotá: Antonio Nariño.
- TORO, Néstor (2019). *Los mensajes de datos y la prueba electrónica*. Bogotá: Leyer.

Reconocimiento

Este artículo es resultado de la investigación «Acceso a la justicia digital en el derecho público. Análisis de derecho comparado: El caso de Brasil y Colombia», la cual fue financiada por la Universidad Católica Luis Amigó, Sede Medellín, Colombia.

Sobre los autores

DANY STEVEN GÓMEZ AGUDELO es abogado titulado en la Universidad Católica Luis Amigó, Colombia. Especialista en Derecho Administrativo, Universidad de Antioquia, Colombia. Magíster en Derecho, Universidad Católica Luis Amigó. Docente

de Derecho Informático y Nuevas Tecnologías, Derecho Administrativo, docente del semillero en Técnicas de la Oralidad en el Proceso y coordinador del área de derecho público de la Universidad Católica Luis Amigó. Adscrito al Grupo de Investigación Jurídicas y Sociales. Su correo electrónico es dany.gomezag@amigo.edu.co.  <https://orcid.org/0000-0003-2687-0146>.

JENNY MARCELA ACEVEDO VALENCIA es socióloga. Magíster en Estudios Políticos, docente e investigadora del grupo Laboratorio Universitario de Estudios Sociales (LUES), adscrito a la Facultad de Educación y Humanidades de la Universidad Católica Luis Amigó, Colombia. Su correo electrónico es jenny.acevedova@amigo.edu.co.  <https://orcid.org/0000-0001-8971-9975>.

JUAN ESTEBAN AGUIRRE ESPINOSA es titulado en la Universidad de San Buenaventura Seccional Medellín, Colombia. Especialista en Derecho Tributario Internacional en la Universidad Externado de Colombia. Magíster en Ciencias Políticas, Magister en Derecho Universidad Católica Luis Amigó, Colombia. Decano de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó. Investigador adscrito al grupo de investigación DEHJUS Derecho, Justicia y Desarrollo Humano, categorizado A, también de Jurídicas y Sociales, categorizado en C. Investigador categoría asociado Minciencias. Su correo electrónico es aguirreespinosaesteban@gmail.com.  <https://orcid.org/0000-0001-9012-9585>.

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipografía
(www.tipografica.io).