*Si la inseguridad jurídica es la norma en un mundo interconectado, la administración de la evidencia digital debería ser la constante.*

*Jeimy J. Cano*

# *Valoración de la evidencia digital: Análisis y propuesta en el contexto de la administración de justicia en Colombia*

*Andrea Rueda Plazas*[1]
*Jeimy J. Cano*[2]

## Resumen

El siguiente escrito tiene por objetivo hacer un análisis de la situación actual de la admisión y valoración de la prueba electrónica en el contexto jurídico colombiano. Es así, como se estudiarán las prácticas actuales de la evidencia digital, su regulación y las herramientas jurídicas que tiene el juez, en su tarea de admitir y valorar pruebas que cumplan con requisitos de seguridad y legalidad, tales como la confidencialidad, autenticidad e integridad de la información. Por ello, el siguiente escrito planteará una propuesta de buenas prácticas, bajo los preceptos estipulados por el documento HB171:2003 *Guidelines for the management IT Evidence*[3], el cual servirá para que la evidencia digital sea valorada ya no sólo a la luz de los criterios de la sana crítica y de la razón, sino por elementos y estrategias propias de la seguridad de la información en cada una de las etapas de vida de la evidencia digital.

---

1 Abogada de la Universidad de los Andes, Correo electrónico: and-rued@uniandes.edu.co

2 Ingeniero de Sistemas y Computación de la Universidad de los Andes, graduado del Magíster en Ingeniería de Sistemas y Computación de la misma universidad y Doctor en Filosofía de la Administración de Empresas de Newport University, California en los Estados Unidos. Se ha desempeñado como profesor de cátedra en la Facultad de Ingeniería de la Universidad de los Andes en el área de la seguridad informática y la computación forense, así como de la Facultad de Derecho de la misma universidad, donde hace parte del GECTI. Es actualmente miembro de la Red Iberoamericana de Criptología y Seguridad de la Información – CriptoRED (http: //www.alfa-redi.org). Correo electrónico: jcano@uniandes.edu.co

3 HB 171 – 2003. Handbook of Guidelines for the Management of IT Evidence. Publicado por Standards Australia International Ltd. Página 13.

## ABSTRACT

The following document is the result of an analysis of the current situation of the admission and valuation of digital evidence in Colombia's legal context. In this sense, this paper reviews digital evidence practices and procedures and their legal regulations. It also explores the tools that judges have to take into account in order to admit and value digital evidence, that is, evidence that has to fulfill legal and information security requirements, such as confidentiality, authenticity and integrity. In this line of work, the authors have conceived a proposal based on best practices documented in HB171:2003 *Guidelines for the management IT Evidence*, which will serve not only to value digital evidence by healthy critic and reason standards, but also by strategies and elements that are inherent to information security in every stage of the digital evidence life cycle.


**KEYWORDS**: Digital evidence, functional equivalent, confidentiality, authenticity, integrity. Evidencia digital, equivalente funcional, confidencialidad, autenticidad, integridad.

# 1. Introducción

Con la llegada de las nuevas ciencias aplicadas que controvierten y modifican en gran medida la actividad humana, es claro que el derecho y la tecnología son dos conceptos inherentes a las sociedades modernas. La revolución en el campo de las telecomunicaciones, se ha dado gracias al advenimiento de nuevas redes de comunicación por medios informáticos, los cuales le han otorgado al hombre la disposición de novedosos canales de transmisión de información, como el correo y el comercio electrónico. Es así, como conceptos tales como Internet, mensaje de datos, firma electrónica y demás, están tomando cada vez más fuerza, relevancia y aceptación en las constantes relaciones y negocios celebrados entre particulares.

En Colombia, tal problemática no es ajena a la realidad jurídica. En la actualidad su sistema legal cuenta con normas como la ley 527 de 1999, que incursiona el nuevo concepto del equivalente funcional y la ley 962 de 2005 - conocida también como ley antitrámites - la cual agiliza los procedimientos judiciales; normatividades que dan respuesta a una práctica social creciente entre comerciantes y entre ciudadanos del común. Lo anterior, con el objetivo de generar un mínimo de seguridad jurídica a la hora de efectuar transacciones y negocios, ya no por el medio escrito tradicional, sino mediante correos electrónicos, páginas web y demás campos de acción ofrecidos por la Internet.

A pesar de contar con normatividades que regulan la materia, en Colombia sigue latente la problemática sobre la valoración de las pruebas digitales aportadas en un proceso en cuanto generan dudas sobre la confidencialidad, la integridad y la autenticidad de la información, que se presenta en un formato de mensaje de datos.

Lo anterior, arroja como consecuencia principal que, en la mayoría de los casos, dichas pruebas sean valoradas como meros indicios o por el concepto técnico de un perito. Ambos, a pesar de ser idóneos a la hora de brindarle certeza al juez sobre los hechos, además de restarle eficiencia y eficacia al proceso judicial, abruman la fuerza probatoria de la evidencia digital, impidiéndole que entre al proceso por la puerta principal, es decir como una prueba en sí.

En el presente documento, se hará un breve recuento de la situación actual de la prueba electrónica en el derecho comparado, especificando las regulaciones con las que cuentan algunos países. Así mismo, se estudiará la problemática de la prueba electrónica en Colombia y se analizarán las posibilidades de valoración de la prueba electrónica. Además, se estudiará la necesidad de un plan de buenas prácticas para la admisión y valoración de la evidencia digital y en consecuencia, se planteará una propuesta de buenas prácticas para la admisión y valoración de la prueba digital para el ordenamiento jurídico colombiano, bajo los preceptos planteados por el documento HB171:2003, que se encuentre acorde con sus propias necesidades. La propuesta representará, por lo tanto, una respuesta para los operadores

jurídicos frente a la evidencia digital en determinado proceso. Finalmente, se harán unas breves conclusiones.

## 2. *La prueba electrónica en el derecho comparado*

En todos los países del mundo se ha vuelto indispensable adaptar las leyes vigentes a las nuevas concepciones técnicas y tecnológicas, con el fin de dar respuestas a las necesidades derivadas de la práctica jurídica[4] y a las exigencias propias de un mundo globalizado, en los asuntos comerciales, civiles, entre otros. Lo anterior, tiene como objetivo principal que cada uno de los sistemas jurídicos tenga la capacidad de regular los cambios de sus sistemas económicos y sociales permitiendo, con ello, que el propio derecho no se vuelva arcaico e ineficaz.

Es claro que tanto la Internet, como los medios electrónicos, se han convertido en los medios más rápidos para realizar negocios a nivel nacional e internacional, por cuanto a través de los mismos se pueden perfeccionar y concretar transacciones en cuestión de segundos; transacciones que traen consigo efectos e implicaciones jurídicas.

Las pruebas electrónicas de dichas transacciones, susceptibles de ser aportadas a un proceso determinado, se pueden ver afectadas por una valoración deficiente por parte del juez. Esto, en cuanto no existen criterios o requisitos que guíen la actividad valorativa de la evidencia digital a nivel nacional e internacional, dejando tal acción al libre albedrío de la razón y de la sana crítica. Éstos si bien son útiles y suficientes en determinados casos, en el campo de la informática y más específicamente, de la evidencia digital, dada su especialidad, requieren una valoración más clara y detallada que cualquier otro medio probatorio.

Los países pioneros en regular la materia en la Comunidad Europea fueron Alemania, Italia y España. En éste último, se sancionó el Real Decreto Ley 14 sobre la firma electrónica en el año de 1999[5] en donde se le otorgó a dicha firma el mismo valor jurídico de la firma manuscrita. El decreto, a su vez, recaudó los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica.

Sumado a lo anterior, también se expidió el Real Decreto Ley 1906 de 1999[6], que regula la contratación telefónica o electrónica general. Este se justifica por "la necesi-

4 La práctica jurídica hace alusión al diario vivir de los abogados y los operadores jurídicos, que se enfrentan constantemente con casos expuestos a la luz del derecho y de su normatividad.

5 Ministerio de Industria, Turismo y Transporte de España. Real Decreto Ley 14. Consultado el día 8 de noviembre de 2005 en la World Wide Web: http://www.setsi.mcyt.es/legisla/internet/rdley14_99.htm.

6 Real Decreto Ley 1906 de 1999 de España. Consultado el 8 de noviembre en la World Wide Web: http://www.aeat.es/normlegi/ecomercio/rd171299.htm

dad de desarrollar el artículo 5 de la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación, en su apartado 3 que dice textualmente: "en los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma."

En Estados Unidos, por su parte, gracias a la costumbre y a desarrollos jurisprudenciales, ha sido generalizada la aceptación de la evidencia digital como prueba válida dentro de los procesos judiciales. La codificación de la costumbre fue lograda bajo las Leyes Norteamericanas de las *Uniform Rules of Evidence*[7] y las *Federal Rules of Evidence*.[8] La segunda normatividad regula la introducción de la evidencia en los procedimientos civiles y criminales en las Cortes Federales de los Estados Unidos.

En concordancia con lo anterior, una de la leyes más recientes sancionadas por dicho país, es la *Electronic Signatures in Global and National Commerce Act* del 2000, la cual establece principios generales como: *"i) El desarrollo y uso de los registros electrónicos y la firma electrónica deberían ser regulados por los principios de libre mercado y autorregulación antes que la fijación estatal de reglas; ii) Los principios de neutralidad y no discriminación entre proveedores de tecnología para el registro electrónico y la firma electrónica; iii) Las partes en una transacción pueden establecer requerimientos relativos al uso de la firma electrónica aceptables para esas partes; iv) Las partes pueden determinar los procedimientos de autenticación y ellos deben ser aceptados, dándoles ejecutabilidad y debiendo ser reconocidos como prueba; v) No puede negarse validez y efecto a los registros electrónicos y la firma electrónica otorgados en una forma aceptada por las partes, sobre la base de que no son escritos; vi) No se debe discriminar en favor de una tecnología, proceso, técnica específica de creación, generación, almacenamiento, registro, comunicación o autenticación de firmas."*[9] Las anteriores normatividades fueron expedidas con la intención de lograr una mayor seguridad jurídica para aquellos negocios celebrados por medios electrónicos.

Así las cosas, la comisión de las Naciones Unidas, desde la década del 60, se ha propuesto en la tarea de facilitar los procedimientos del comercio internacional, por medio de normas que agilicen los trámites y disminuyan los requisitos excesivos. Por lo anterior, dicho organismo, desde comienzos de los años 90, ha venido promoviendo la elaboración de leyes modelos para el Intercambio Electrónico de Datos (EDI),

7 Uniform Rules of Evidence. Consultado el día 8 de Noviembre de 2005 en la World Wide Web http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm

8 Federal Rules of Evidence. Consultado el día 8 de Noviembre de 2005 en la World Wide Web http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm

9 Electronic Signatures in Global and national Commerce Act del 2000. Consultado el día 8 de noviembre de 2005 en la World Wide Web http://www.ricardolorenzetti.com.ar/secciones/comercio_electronico1.htm

por medio de la Comisión de la Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI), conocida también como la UNCITRAL.

Tales esfuerzos se vieron materializados con la reciente Ley Modelo de UNCITRAL sobre Comercio Electrónico, "la cual fue inspirada en la convicción de que al dotársele de fundamentación y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros, lo cual, de contera, redundaría en la expansión del comercio internacional, dadas las enormes ventajas comparativas que gracias a su rapidez, estos medios ofrecen en las relaciones de índole comercial entre comerciantes y usuarios de bienes y servicios."[10]

El proyecto tiene como novedad el concepto del *equivalente funcional*, el cual consiste en suplir las exigencias formales como la firma, el requisito que conste por escrito, entre otros, por equivalentes electrónicos que cumplan con la misma función, los cuales son más eficaces para los fines del comercio electrónico. A su vez, resuelve el problema de admisibilidad y fuerza probatoria de los mensajes de datos, ya que suple tal dificultad por *la regla de la mejor prueba*. Dicha solución no opera en los países de corte continental o civil, en cuanto su aplicación no ha sido aceptada por sus tribunales y cortes.

En los países latinoamericanos también se han sancionados leyes que regulan el comercio electrónico. Aunque su llegada ha sido tardía, en la actualidad cuentan con una normatividad sólida y estable del tema. Tal es el caso de Perú, que en el año 2000 sancionó la Ley de firmas y certificados No. 27269;[11] Argentina, que promulgó la Ley 25.506[12] que trata sobre la firma digital; Venezuela, que reguló las firmas digitales, los certificados electrónicos y los proveedores de servicios de certificación; Chile, que sancionó la Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma No. 19.789;[13] Ecuador, que promulgó la Ley No. 57 de 2002 que regula el comercio electrónico, firmas y mensajes de datos; México, que en el año 2000 sancionó la Ley 500 sobre el comercio electrónico; entre otros.

Todas las regulaciones antes mencionadas tuvieron como fuente de derecho y como espíritu la Ley Modelo del Proyecto UNCITRAL que ha inspirado las normatividades nacionales y a su vez, les ha brindado el fundamento necesario y las

10 Sentencia C-662 de 2000. Corte Constitucional. M.P.: Fabio Morón Díaz.

11 Ley de firmas y certificados No. 27269 de Perú. Consultado el día 8 de noviembre de 2005 en la World Wide Web http://www.indecopi.gob.pe/upload/crt/firmasDigitales/reglamentods019-2002-jus.PDF

12 Ley 25.506 de Argentina. Consultado el día 8 de noviembre de 2005 en la World Wide Web http://www.safjp.gov.ar/digesto_2/index/normas/LEY%202424 1/Ley25506.htm

13 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma No. 19.789 de Chile. Consultado el día 8 de noviembre de 2005 en la World Wide Web http://www.cedi.uchile.cl/docs/Ley19799.pdf

herramientas para regular un tema tan novedoso como lo es el comercio electrónico y todos sus derivados.

De la mano de todas las normatividades antes expuestas, se puede decir que el tema del comercio electrónico y en especial, del mensaje de datos, se encuentra debidamente regulado por las normatividades internacionales. Ello por cuanto la práctica electrónica pasó de ser desconocida, a ser promovida por los distintos Estados, en cuanto facilita las transacciones propias del mundo global en el que vivimos en la actualidad.

## *3. Problemática sobre la valoración de la prueba electrónica en Colombia*

Para comprender la problemática de la prueba electrónica en Colombia, será necesario analizar la doctrina general de la prueba y la regulación de la misma, esta última establecida en el Código de Procedimiento Civil. Es así como a continuación se estudiará la normatividad y cada uno de los conceptos desarrollados por la doctrina jurídica.

La prueba judicial, aunque tiene un sentido polifacético, es definida por la doctrina como *"el conjunto de motivos o razones que nos suministran el conocimiento de los hechos, para los fines del proceso, que de los medios aportados se deducen."*[14]

Los principales elementos de la prueba judicial son:

1. El objeto de prueba: Son los hechos susceptibles de ser probados. Estos son esgrimidos por la doctrina como todos los sucesos, acontecimientos, hechos o actos humanos, voluntarios o involuntarios, individuales o colectivos, que sean perceptibles; sus circunstancias de tiempo, modo y lugar; los hechos de la naturaleza en que no interviene actividad humana; las cosas o los objetos materiales y cualquier situación de la realidad material sean o no producto del hombre, incluyendo los documentos; la persona física humana, su existencia y características.[15]
2. El tema de la prueba: "Está constituido por aquellos hechos que son necesarios de probar, por ser los supuestos de las normas jurídicas cuya aplicación se discute en un determinado proceso."[16]

14 DEVIS ECHANDÍA, Hernando. Teoría General de la Prueba Judicial, Tomo I. Primera Edición Colombiana. Editorial Biblioteca Jurídica Dike. Medellín. 1987. Página 25.

15 DEVIS ECHANDÍA, Hernando. Compendio de derecho procesal, Pruebas Judiciales, Tomo II. Séptima Edición, Editorial ABC. Bogotá. 1982. Página 46.

16 PARRA QUIJANO, Jairo. Manual de Derecho Probatorio. Séptima Edición. Ediciones Librería del Profesional. Bogotá. 1986. Página 78.

3. El fin de la prueba: Es la creación de la certeza en el juez, es decir la prueba busca indagar la verdad de los hechos ocurridos en el pasado para que en el presente y en la conciencia del juez, se pueda fallar acorde con la realidad de las cosas y no ante hechos hipotéticos.

El artículo 174 del Código de Procedimiento Civil establece que "toda decisión judicial debe fundarse en la prueba regular y oportunamente allegada al proceso", es decir que toda sentencia debe estar soportada por pruebas legales que reposen en el expediente, estableciendo como requisito principal la necesidad de la prueba. Lo anterior, significa que el juez no tendrá la facultad de dirimir la controversia planteada sin pruebas que fundamenten su convicción. Esto con el fin de evitar decisiones arbitrarias y discrecionales.

Acorde a lo anterior, la sentencia del marzo 27 de 1998 de la Corte Suprema de Justicia, desarrolla el artículo 174 del C. de P. C. aduciendo que *"las pruebas producidas, con el objeto de que cumplan con su función de llevar al juez el grado de convicción suficiente para que pueda decidir sobre el asunto materia de la controversia, además de ser conducentes y eficaces, deben allegarse y practicarse en los términos y condiciones establecidos de antemano en el ordenamiento positivo, ya que de lo contrario no es posible que cumplan la función señalada, así lo estipula el artículo 174 del Código de Procedimiento Civil al tenor del cual "toda decisión judicial debe fundarse en pruebas regular y oportunamente allegadas al proceso."*[17]

Siguiendo con la línea argumentativa planteada y teniendo en cuenta el precepto legal del artículo 174 del C. de P. C., el juez debe dirimir toda controversia a partir de las pruebas que consten en el proceso, con base en la valoración que éste haga de cada una de ellas. La doctrina se ha pronunciado al respecto y ha determinado como sistemas para la valoración de la prueba *la tarifa legal* y *la libre convicción.* La primera es aquella donde el legislador señala el valor de la prueba, es decir que determina los parámetros de valoración; mientras que la segunda, es cuando el juez puede y debe libremente valorar la prueba[18] bajo los conceptos de la sana crítica y de la razón.

En tanto lo anterior, en Colombia el artículo 187 del Código de Procedimiento Civil[19] indica que el juez deberá apreciar las pruebas en conjunto, es decir que no podrá fallar por la simple apreciación de una de ellas, sino por el convencimiento derivado de la pluralidad de pruebas que fueron oportuna y regularmente aportadas al proceso. La acción del juez en la valoración e interpretación de las mismas, deberá seguir los criterios de la sana crítica y de la razonabilidad, tal y como lo establece la ley. De lo anterior, se esgrime que el sistema probatorio colombiano se basa en el sistema de la *libre convicción*, por cuanto es el juez quien tiene la facultad de darle valor probatorio a las pruebas del acervo probatorio.

17 Sentencia de marzo 27 de 1998, Expediente 4943. Corte Suprema de Justicia, Sala de Casación Civil. M. P. Carlos Esteban Jaramillo Schloss.

18 Op.cit, PARRA QUIJANO, Jairo. Manual de Derecho Probatorio. Página 109.

Así las cosas, es pertinente mencionar que un determinado proceso no podrá constar de pruebas legalmente prohibidas o ineficaces, ni impertinentes o superfluas, en cuanto el artículo 178 del C. de P. C.[20] lo prohíbe. Al respecto, la sentencia del Tribunal Superior de Bogotá ha dicho que el Código de Procedimiento Civil *ha entendido* por pruebas legalmente prohibidas *"aquellas tendientes a demostrar hechos que la ley prohíbe investigar, como son aquellas en defensa de la moral. (...). Por ineficaces cuando se trata de un medio por el cual es jurídica o legalmente imposible probar el hecho a que se refiere ya sea porque se exige un medio por el cual es jurídica o legalmente imposible probar el hecho a que se refiere ya sea porque se exige un medio determinado de prueba (ej. (Escritura pública o documento privado para determinados actos o contratos). (...). Por impertinentes aquéllas que tratan de probar un hecho que nada tiene que ver con lo discutido dentro del proceso y por superfluas aquéllas que se hacen innecesarias en virtud de haberse practicado ya dentro del proceso suficientes pruebas para darle la plena certeza sobre un hecho determinado."*[21]

Antes de aterrizar toda la teoría y regulación antes planteada a la prueba electrónica, será necesario detenernos en los conceptos básicos del equivalente funcional; conceptos que fueron inmersos al sistema jurídico colombiano por la ley 527 de 1999.

Ahora bien, en este punto es preciso detenerse y comprender el alcance general del principio del equivalente funcional, el cual tiene como finalidad adaptar y darle la misma fuerza probatoria de los documentos consignados en papel a los documentos en formato de mensajes de datos, firmas electrónicas y demás conceptos tecnológicos. Lo anterior, pretende cumplir con los mandatos estipulados por la ley, al incorporarle los requisitos de forma a los documentos electrónicos, como son la fiabilidad, inalterabilidad y rastreabilidad. Es decir, el principio en mención, establece que un mensaje de datos que cumpla con la función de declaración o representación, tendrá los mismos efectos jurídicos propios de los medios de prueba tradicionales.

En conclusión, los documentos electrónicos o mensajes de datos están en la capacidad de brindar equivalentes grados de seguridad que los documentos consignados en papel y en muchos casos, un mayor nivel de confiabilidad y rapidez. Para que se pueda predicar un grado de seguridad confiable, se deberá cumplir con los requisitos

---

19 Código de Procedimiento Civil, Artículo 187: Apreciación de las pruebas. Las pruebas deberán ser apreciadas en conjunto, de acuerdo con las reglas de la sana crítica, sin perjuicio de las solemnidades prescritas en la ley sustancial para la existencia o validez de ciertos actos.

El juez expondrá siempre razonadamente el mérito que le asigne a cada prueba.

20 Código de Procedimiento Civil, Artículo 178: Rechazo in limine. Las pruebas deben ceñirse al asunto materia del proceso y el juez rechazará in limine las legalmente prohibidas o ineficaces, las que versen sobre hechos notoriamente impertinentes y las manifiestamente superfluas.

21 Auto de junio 19 de 1978. Tribunal Superior de Bogotá. Magistrado Ponente: Humberto Rodríguez Robayo.

técnicos y jurídicos plasmados en la ley, cuestión que se hace palpable en el derecho colombiano con la llegada del principio del equivalente funcional.

Es preciso decir que la ley 527 de 1999 surge como una norma interpretativa de la regulación actual, en cuanto los equivalentes funcionales esgrimidos en la ley permiten una interpretación actualizada y acorde con las necesidades de la realidad tecnológica, adaptando las normatividades ya vigentes al mundo contemporáneo.

Así las cosas, el mensaje de datos es definido por la ley 527 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."*[22]

Los requisitos de forma exigidos para las diferentes actuaciones, quedarán suplidos para la información consignada en mensaje de datos de la siguiente forma:

1. Equivalente funcional del escrito: A pesar de que el escrito cumple un sin número de funciones, la ley 527 consideró que la función más relevante es la de permitir el acceso de la información almacenada en el mensaje de datos con posterioridad a su creación. Lo anterior, se deriva del artículo 6 de la ley en cuestión, el cual consagra: *"Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito."*[23]
2. Equivalente funcional de la firma: Las funciones generales de la firma son las de identificar a alguien y vincular a esa persona con el contenido del documento. Para el caso de los mensajes de datos la firma electrónica pretende identificar al iniciador del mensaje de datos y vincular al iniciador con el contenido del documento electrónico firmado. Lo anterior, se interpreta del artículo 7 de la ley 527, el cual dice: *"Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a) Se ha utilizado un método que permita identificar al inicia-*

22 Ley 527 de 1999. Artículo 2°. Definiciones. Para los efectos de la presente ley se entenderá por: a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax; (…).

23 UMAÑA CHAUX, Andrés Felipe. Algunos comentarios sobre el principio del equivalente funcional en la Ley 527 de 1999. Revista de Derecho Comunicaciones y Nuevas Tecnologías. Volumen I. No. ISSN 1794-9254 Ediciones Uniandes. 2005. Páginas 75 a 111.

*dor de un mensaje de datos y para indicar que el Contenido cuenta con su aprobación; b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma."*

3. Equivalente funcional del original: A diferencia de los demás equivalentes, la función del mismo sufre una gran modificación, en cuanto el acceso a la información consignada en formato de mensaje de datos necesariamente implica realizar una copia de la información consignada en ella. Por tal motivo, el original se suple en los mensajes de datos siempre y cuando exista una garantía confiable de que la información almacenada se ha conservado íntegra desde el momento de su creación de forma final. El artículo 8 de la ley 527 es el encargado de regular la materia en los siguientes términos: *"Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si: a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original."*

Los equivalentes funcionales de escrito y firma se armonizan con la realidad gracias al principio de neutralidad tecnológica consagrado en los artículos 6 y 7 de la ley 527, que establecen que no será necesario el uso de una tecnología específica para lograr el equivalente de cada uno de ellos, en cuanto estos quedan satisfechos con el cumplimiento de las funciones establecidas para cada caso en concreto, cuestión que servirá para que un mensaje de datos se entienda firmado y/o que conste por escrito.[24]

Todo lo anterior, nos permite analizar la problemática de la prueba electrónica en Colombia y en especial, la valoración de la misma. Ello, teniendo en cuenta que la prueba electrónica es otro tipo de prueba físicamente concebida, que encuentra su soporte en un medio magnético.

Es así como la valoración de la prueba electrónica además de contener y cumplir las normas consagradas por los artículos 174 y siguientes del Código de Procedimiento Civil, deberá reunir los requisitos establecidos por la ley 527 de 1999, analizados con anterioridad.

24 Op. cit. Revista de Derecho Comunicaciones y Nuevas Tecnologías, Página 88.

Los requisitos de admisibilidad de la evidencia digital se encuentran desarrollados por el artículo 10 de la mencionada ley, que estipula: *"Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original."*

A partir del precepto anterior, el juez no podrá negarle fuerza probatoria ni admisibilidad a los mensajes de datos por el simple hecho de ser mensaje de datos. Esto por cuanto se presentaría una ilegalidad[25] por parte de éste, al contrariar los mandatos establecidos en la ley.

Sabiendo de antemano que las pruebas en el régimen probatorio civil deberán ser valoradas por la sana crítica y la razonabilidad del juez, para el caso de la prueba electrónica, éste también deberá cumplir con la normatividad estipulada por la ley 527 de 1999. Es decir, que sumado a los criterios de la sana crítica y de la razonabilidad, el juez - como consecuencia de la especialidad de la evidencia digital - deberá estudiar y valorar "la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje; la confiabilidad en la forma en que se haya conservado la integridad de la información; y la forma en la que se identifique a su iniciador y cualquier otro factor pertinente."[26]

A continuación, se esgrimirán cada uno de los elementos mencionados, que son también entendidos como las garantías de la información en documento electrónico:

- *Autenticidad:* Hace referencia a la capacidad de determinar si una persona ha establecido su reconocimiento y vinculación sobre el contenido del documento electrónico. Lo anterior, se comprende de dos elementos principales, los cuales son: En primera medida es que "*dicha evidencia haya sido generada y registrada en el lugar de los hechos y la segunda que muestre "la no*

25 La conducta antes descrita se encuentra tipificada por el artículo 230 de la Constitución, en cuanto el juez en sus providencias solo está sometido al imperio de la ley y deberá cumplir a cabalidad con cada uno de sus preceptos. La normatividad establece: "Los jueces, en sus providencias, sólo están sometidos al imperio de la Ley. La equidad, la jurisprudencia, los principios generales del derecho y la doctrina so criterios auxiliares de la actividad judicial."

26 Ley 527 de 1999, Artículo 11. Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

*alterabilidad de los medios originales" es decir que los registros correspondan efectivamente a la realidad y que son un fiel reflejo de la misma."*[27]

Ello se vislumbra en el sistema jurídico colombiano, a partir de dos normatividades diferentes, ya sean documentos públicos o documentos privados.[28] Los primeros de ellos se entienden auténticos siempre y cuando no obre prueba en contrario o no se hayan tachado de falsos;[29] mientras que los segundos, la ley sólo los considera auténticos en los siguientes casos: "i) *Si ha sido reconocido ante el juez o notario, o si judicialmente se ordenó tenerlo por reconocido; ii) Si fue inscrito en un registro público a petición de quien lo firmó; iii) Si habiéndose aportado a un proceso y afirmado estar suscrito, o haber sido manuscrito por la parte contra quien se opone, ésta no lo tachó de falso oportunamente, o los sucesores del causante a quien se atribuye dejaren de hacer la manifestación contemplada en el inciso segundo del artículo 289. Esta norma se aplicará también a las reproducciones mecánicas de la voz o de la imagen de la parte contra quien se aducen, afirmándose que corresponde a ella; iv) Si fue reconocido implícitamente de conformidad con el artículo 276; v) Si se declaró auténtico en providencia judicial dictada en proceso anterior, con audiencia de la parte contra quien se opone en el nuevo proceso, o en la diligencia de reconocimiento de que trata el artículo 274."*[30]

A su vez, se presume la autenticidad de los documentos firmados con firma electrónica autorizada, tal y como lo establece el artículo 17 de la

27 Mosquera Gonzalez, José Alejandro. Certain Jaramillo, Andrés Felipe. Cano, Jeimy J...Evidencia Digital contexto, situación e implicaciones nacionales. Revista de Derecho Comunicaciones y Nuevas Tecnologías. Volumen I. No. ISSN1794-9254. Ediciones Uniandes. 2005. Página 186.

28 Para comprender con precisión la terminología jurídica en este caso el documento, la ley y más exactamente el artículo 251 del Código de Procedimiento Civil, lo define de la siguiente forma: "Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares. Los documentos son públicos o privados. Documento público es el otorgado por funcionario público en ejercicio de su cargo o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumentos público; cuando es otorgado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública. Documento privado es el que no reúne los requisitos para ser documentos públicos.

29 Código de Procedimiento Civil, artículo 252, modificado por la ley 794 de 2003: "Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado. El documento público se presume auténtico, mientras no se compruebe lo contrario mediante tacha de falsedad. (…)."

30 Código de Procedimiento Civil, artículo 252, modificado por la ley 794 de 2003, inciso 2, numerales 1, 2, 3, 4 y 5.

ley 527.[31] Mientras los demás documentos, por el momento, son aptos para el estudio realizado por un perito experto en la materia, quien por medio de habilidades técnicas podrá determinar su autoría y su autenticidad.

- *Originalidad:* Se entiende por original cualquier obra literaria, artística, científica, entre otras, emanadas de la creación e imaginación de su autor. Tal y como se mencionó en el equivalente funcional de original, una de las dificultades más grandes en el campo electrónico e informático es que el original del documento electrónico en realidad es aquel que se encuentra en el equipo o en el computador donde su autor digitó o creó dicho escrito. Por tal motivo, cualquier copia, impresión y demás, son reproducciones de éste, es decir, copias que ya pierden la garantía de ser originales.

  Una excepción a la regla anterior para el caso colombiano, se encuentra consignada en el artículo 254 del Código de Procedimiento Civil, el cual establece que las copias tendrán el mismo valor que el original, en los casos taxativamente señalados por el mismo, los cuales son: *"i) Cuando hayan sido autorizadas por notario, director de oficina administrativa o de policía, o secretario de oficina judicial, previa orden del juez, donde se encuentre el original o una copia autenticada; ii) Cuando sean autenticadas por notario, previo cotejo con el original o la copia autenticada que se le presente; iii) Cuando sean compulsadas del original o de copia autenticada en el curso de inspección judicial, salvo que la ley disponga otra cosa."* Siempre y cuando se cumplan con cualquiera de los casos descritos, las copias se tomarán como originales y por tal motivo, pierden la calidad de copias. Las anteriores situaciones no podrán ser aplicadas en los documentos electrónicos, en cuanto carecen de la formalidad de escrito que presupone la norma antes citada.

- *No repudio:* Es definida por la doctrina como *"la capacidad de probar a una tercera parte que una determinada comunicación ha sido originada, admitida y enviada a una determinada persona."*[32] El *no repudio* permite establecer el vínculo que existe entre la voluntad de la persona y el contenido del

31 Ley 527 de 1999, artículo 17: "Presunción del origen de un mensaje de datos. Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando: 1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o 2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio."

32 Ramos Suárez, Fernando Revista electrónica ALFA-REDI Eficacia jurídica de una transacción electrónica. La figura del no repudio, Edición Número 12. (1999, julio). Consultado el día 1 de diciembre de 2005 en la World Wide Web http://www.alfa-redi.org/rdi-articulo.shtml?x=300

documento. La diferencia principal entre la autenticidad y el *no repudio*, es que el primero logra establecer quien es el autor y cual es su destinatario, mientras que con el *no repudio* se prueba que el emisor envió la comunicación y el destinatario la recibió sin error alguno.

A pesar de la escasez de regulación sobre la *no repudiación* del contenido del documento, la ley 527 de 1999 en su artículo 23 establece que sin pacto en contrario entre el emisor y el receptor, el tiempo del envío de un mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.[33] En ese instante, el mensaje queda por fuera de la esfera del emisor, cuestión que no le permite desistir del contenido del mismo.

A su vez, el artículo 24 de la ley 527[34] consagra el tiempo de la recepción de un mensaje de datos, el cual será determinado a partir de la consecución de cualquiera de las siguientes hipótesis: *"a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar: 1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o 2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario. Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente."*

33 Ley 527 de 1999, artículo 23: "Tiempo del envío de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste."

34 Ley 527 de 1999, artículo 24. Tiempo de la recepción de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue: a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar: 1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o 2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario. Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

Tal garantía es cumplida cuando se prueba que la información emitida por el emisor, fue satisfactoriamente recibida por el receptor y que éste tiene una estrecha relación con el contenido del mensaje de datos.

- *Integridad*: Un documento se considera íntegro cuando *"contiene toda la información que constaba al momento de su emisión, y que desde entonces no ha sido alterado."*[35]

  Al respecto, la legislación colombiana no ha regulado la materia a cabalidad. Su normatividad se encuentra más encaminada a proteger la originalidad de los documentos, sin hacer mayores alusiones sobre la integridad de los mismos. Sin embargo, sin importar la falta de normatividad al respecto, se puede decir que un documento por el simple hecho de ser auténtico goza de integridad, pero no necesariamente un documento que se considere íntegro tendrá la característica de auténtico. Lo anterior, significa que una de las características principales de la autenticidad es la integridad.

- *Confidencialidad*: Dicha característica "*garantiza que un documento solo pueda ser leído por su destinatario, nos asegura que nadie más sabrá su contenido."*[36]

  Esta garantía es propia del campo de las telecomunicaciones debido a que se trata de un medio en donde el usuario pretende realizar comunicaciones privadas, a diferencia de los medios de comunicación masivos, que tienen por fin comunicar a la mayor cantidad de personas posible. Es por esto, que quien realiza la comunicación es el que le da el carácter de privado o público a la información que pretende transmitir.

  En el caso de los mensajes informáticos, que tienen como soporte una firma electrónica, ésta *"por tener una clave privada combinada con la pública, naturalmente ofrece un grado muy alto de confidencialidad que no le debe pasar inadvertido al juez."*[37]

En conclusión, el régimen probatorio colombiano en la actualidad cuenta con un soporte jurídico apto para la aceptación y valoración de la evidencia digital o prueba electrónica. No obstante, vale la pena indicar que en la práctica jurídica, tales preceptos legales son de difícil aplicación o son desconocidos por los jueces. Lo anterior, por cuanto en el ordenamiento jurídico aquellas pruebas, como es el caso del mensaje de datos, no adquieren la misma fuerza probatoria o consistencia que cualquier otro medio de prueba, ya que el juez decreta peritazgos o simplemente lo valora como

35 Riofrío, Juan Carlos La Prueba Electrónica. Primera Edición. Bogotá, Colombia. Editorial Temis. 2004. Página 105.

36 Ibíd. La Prueba Electrónica, Página 117.

37 Ibíd. La Prueba Electrónica, Página 122.

indicios graves, para su admisión y tratamiento. Esto, sabiendo de antemano que la prueba digital en sí, ya se constituye como un medio probatorio idóneo para otorgarle al juez el convencimiento necesario sobre los hechos fundamento de la demanda y del proceso.

## 4. Análisis de posibilidades

Una vez analizada la problemática de la prueba electrónica en Colombia, es preciso mencionar que el sistema de medios probatorios colombiano está compuesto por un catálogo abierto. Lo anterior, significa que los medios referidos por el mismo, simplemente son enunciados o enumerados. Esto permite la incursión de nuevas técnicas probatorias pertinentes para cada caso en concreto. Tal interpretación se desprende del artículo 175 del Código de Procedimiento Civil, el cual menciona *"sirven como pruebas, la declaración de parte, juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez. El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio."*

Al ser el artículo 175 del C. de P. C. un catálogo no taxativo, la ley faculta al juez para decretar nuevos medios probatorios que no estén contemplados por dicha lista, los cuales, en determinado momento, pueden llegar a ser más eficaces a la hora de esclarecer los hechos objeto del litigio.

En concordancia con lo anterior, es pertinente mencionar que el equivalente funcional es simple y llanamente una norma interpretativa de las leyes ya vigentes. Permite, por lo tanto, expandir la concepción humana a nuevas posibilidades tecnológicas igual de idóneas a las tradicionales. Es así, como es posible asemejar las normas jurídicas a los hechos provenientes del mundo actual, permitiendo que estos se encuentren debidamente regulados por el derecho y brindándole a las nuevas prácticas soporte y seguridad jurídica.

Sin embargo, en la actualidad Colombia cuenta con dos alternativas jurídicas de valoración de la prueba electrónica que, a pesar de ser idóneas y eficaces para esclarecer los hechos de un caso, cuentan con problemas de tiempo, costos, especialidad y uso de tecnología especial para la identificación y valoración de este tipo de prueba; problemas que pueden llegar a obstruir la eficiencia en la resolución del litigio.

En primer lugar, los hechos pueden ser valorados a través de un peritazgo decretado por el juez, el cual no es obligatorio y es susceptible de ser objetado por cualquiera de las partes. El peritazgo es un medio de prueba tradicional enunciado en el catálogo abierto del artículo 175 del C. de P. C. La segunda alternativa que tiene el juez recae en la valoración de las pruebas electrónicas como meros indicios, por cuanto el mensaje

de datos, que determina la existencia de un hecho dentro del proceso, no llega a cumplir con los requisitos mínimos de seguridad jurídica, cuestión que no le proporcionaría al juez la confianza en la autenticidad de la información almacenada en un documento electrónico. Lo anterior, trae como consecuencia catastrófica, el restarle fuerza probatoria a la evidencia aportada en formato de mensaje de datos, sin tener en cuenta que ésta es una prueba apta para darle certeza al juez sobre los hechos del caso en particular.

Así las cosas, la doctrina define el peritazgo como *"una actividad procesal desarrollada, en virtud de encargo judicial, por personas distintas de las partes del proceso, especialmente calificadas por sus conocimientos técnicos, artísticos o científicos, mediante la cual se suministra al juez argumentos o razones para la formación de su convencimiento respecto de ciertos hechos cuya percepción o cuyo entendimiento escapa a las actitudes del común de las gentes."*[38]

De esta forma y como el juez no puede tener conocimiento de todas las ciencias, técnicas o áreas del conocimiento, es necesario recurrir a los peritos como auxiliares de la justicia. Éstos ayudan a resolver un determinado litigio, al esclarecer el saber del juez sobre los hechos objeto del experticio, otorgándole total certeza sobre los mismos.[39]

Como se mencionó anteriormente, el peritazgo a pesar de ser un medio eficaz para brindarle certeza al juez sobre los hechos objeto del proceso, su práctica en el medio informático presenta problemas de costos, tiempo y probabilidades de éxito que llegan a dilatar el proceso. A su vez y de no haber estándares para adelantar el procedimiento forense y valorar las pruebas recabadas en este proceso, se podría caer en la ineficiencia en la resolución de eventuales litigios.

La experiencia norteamericana ha demostrado que a un experto suele tomarse entre diez y cincuenta horas su labor, dependiendo de las habilidades y destrezas del implicado dentro de un proceso en específico, lo que dificulta el desempeño del perito. En cuanto a costos, éstos son de alrededor de dos mil dólares, en los casos pequeños o de menor cuantía y cien mil dólares, en los casos grandes.[40]

Así las cosas, el peritazgo a pesar de ser óptimo a la hora de suplir las necesidades del juez y esclarecer los hechos del caso, es una labor compleja que amerita tiempo y dinero; limitaciones que pueden llegar a perjudicar la eficacia de la justicia y la resolución de los conflictos.

---

38 DEVIS ECHANDIA, Hernando. Teoría General de la Prueba, Tomo II. Tercera Edición. Buenos Aires, Argentina. Editor Buenos Aires. 1974. Páginas 286 y s.s.

39 Parra Quijano, Jairo (1988). Tratado de la Prueba Judicial, "La prueba pericial y la inspección judicial", Tomo V. Tercera Edición. Bogotá, Colombia. Ediciones Librería del Profesional. Página 7.

40 Ob.cit., La prueba electrónica, Página 144.

Como segunda medida, los operadores jurídicos también valoran la prueba electrónica como un mero indicio, definido por la doctrina como *"un hecho del cual se infiere otro desconocido. Debe quedar suficientemente claro que el indicio es, por así decirlo, un hecho especialmente cualificado, porque tiene la propiedad de salirse de sí mismo y mostrar otro."*[41]

En el sistema jurídico colombiano, el artículo 248 y siguientes del Código de Procedimiento Civil, desarrollan el tema de los indicios, indicando que para que un hecho pueda considerarse como tal deberá estar debidamente probado dentro del proceso.[42] A su vez, el juez deberá valorar los indicios en conjunto,[43] junto con las demás pruebas que reposen en el acervo probatorio del caso en concreto.

De esta forma, el indicio es el producto de una deducción lógica que realiza el juez de un hecho demostrado dentro del proceso, que afirma la existencia de uno desconocido del cual no obra prueba alguna en el acervo probatorio. Por tal motivo y en este caso en particular, es claro que los medios informáticos no entrarían como prueba sumaria, ya que queda en manos del juez el otorgarle la fuerza probatoria y el grado de convencimiento a los medios informáticos, bajo los criterios de la razón y de la sana crítica.

Al igual que el peritazgo, es pertinente y necesario aclarar que aunque estos medios de prueba son aptos para esclarecer los hechos de un determinado proceso, es comprensible que si un medio magnético se vincula a un proceso por medio de dichas alternativas, el juez le estaría restando eficacia a la evidencia electrónica.

## *5. Hacia un estándar de valoración de la prueba electrónica.*

De esta misma forma y aunque el peritazgo y el indicio son mecanismos eficientes y eficaces a la hora de esclarecer los hechos de un caso, es claro que estos sufren problemas de costos, tiempo y especialidad, que en determinado momento pueden llegar a dilatar la decisión del juez.

Por tal motivo y con el fin de proporcionarle una herramienta eficiente al operador jurídico, se hace necesario fijar unos parámetros de valoración de la prueba electrónica que tengan como principal propósito evitar que los hechos de un determina-

41 PARRA QUIJANO, Jairo. Tratado de la Prueba Judicial, Indicios y Presunciones, Tomo IV. Tercera Edición. Bogotá, Colombia. Ediciones Librería del Profesional. 1988. Página 21.

42 Código de Procedimiento Civil, artículo 248: "Para que un hecho pueda considerarse como indicio, deberá estar debidamente probado dentro del proceso."

43 Código de Procedimiento Civil, artículo 250: "El juez apreciará los indicios en conjunto, teniendo en consideración su gravedad, concordancia y convergencia y su relación con las demás pruebas que obren en el proceso."

do caso sean valorados como meros indicios o mediante peritazgos largos y costosos y por lo tanto, lograr que el juez los admita como elementos formales.

Lo anterior, tiene como finalidad determinar en que casos una evidencia digital debe ser admitida a un proceso como una prueba plena, es decir, cuando ésta cumple con la totalidad de los requisitos establecidos en la ley[44]; requisitos tanto de seguridad como de legalidad. A su vez, permite que el juez vislumbre cuando se hace necesario acudir a otros medios de prueba, cuando las pruebas no satisfagan la totalidad de los requisitos y por ende, no sean idóneas para crear un pleno convencimiento del juez sobre los hechos bajo estudio.

A continuación se explicarán las razones, tanto legales como de seguridad, que determinan la eficacia, alcance y eficiencia de la evidencia digital. Ello, en concordancia con la fuerza probatoria otorgada a los mensajes de datos por la ley 527 de 1999.

Las pruebas informáticas gozan de una eficacia natural por el simple hecho de ser documentos electrónicos. A pesar del deber que existe en cabeza del legislador y del derecho positivo de regular y de determinar el alcance de cada una de ellas, el alcance probatorio otorgado por el derecho positivo no elimina la aptitud probatoria que reposa en los *documentos* electrónicos. En el caso colombiano, la ley 527 determina el alcance probatorio de la información contenida en forma de mensaje de datos, elevando la eficacia natural de estos a mandatos legales y asimilando su fuerza probatoria a la de los documentos tradicionales.

A su vez y en virtud de los principios de confidencialidad, integridad y autenticidad de los mensajes de datos, será necesario establecer pasos y requisitos mínimos a la hora de recolectar la prueba electrónica y de aportarla al proceso, con el fin de que ésta no sea alterada o modificada por terceros. Ello cumpliendo con una cadena de custodia que vinculará al recolector con el material recopilado y donde éste deberá seguir cada paso, sin omisión alguna. De lo contrario el mensaje de datos podría perder fuerza probatoria.

En este sentido y siempre y cuando se reúnan los requisitos legales y de seguridad informática, el juez podrá valorar los hechos provenientes de una evidencia electrónica como una prueba en sí, sin necesidad de acudir a los auxiliares de la justicia o de otorgarle la fuerza de un indicio. Lo anterior, en la medida en que se cumplirán los requisitos de confidencialidad, integridad y autenticidad que tanto preocupa a los operadores jurídicos.

44 Los requisitos establecidos por la ley para el caso de los mensajes de datos, como son el equivalente funcional de escrito, firma, original, entre otros y las formalidades establecidas para el perfeccionamiento de algunos negocios jurídicos celebrados por particulares, con el fin de que estas sean cumplidas a cabalidad bajo el criterio y parámetros electrónicos.A su vez, la ley determina que un mensaje de datos deberá cumplir con requisitos de confidencialidad, integridad, no repudio, entre otros, que brindan confianza en el juez sobre la veracidad de la información contenida en mensaje de datos.

## 6. Propuesta para Colombia

Como se mencionó anteriormente, la propuesta pretende otorgarle las herramientas suficientes al juez para la admisión y valoración de la prueba electrónica; pruebas que deberán cumplir con los requisitos establecidos en la ley, en procura de la conservación de la integridad, autenticidad y confidencialidad de la información contenida en el archivo electrónico.

Es pertinente mencionar que la neutralidad jurídica juega un papel de enorme importancia en el caso bajo estudio. Ello por cuanto las normatividades se encuentran redactadas con el ánimo de que éstas no se encasillen a una técnica específica. Lo anterior, permite que sus preceptos queden abiertos a las formas tecnológicas provenientes de nuevos avances científicos. Garantizando, así, que las regulaciones no se limiten a una destreza concreta de seguridad, sino que dejen latente la posibilidad de implementar nuevas pericias, provenientes de la constante evolución del hombre.

De esta forma, el siguiente estándar propondrá un conjunto de buenas prácticas para el sistema jurídico colombiano, que tendrá como fundamento jurídico principal el documento HB171-2003[45]. Este estándar justificará la admisión y la valoración de la evidencia digital que cumpla, en su totalidad, con los pasos o requisitos planteados a continuación. Lo anterior, garantizará que la información se conserve integralmente, es decir protegiendo la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información; señalando la forma en la que se identifica a su iniciador y cómo se realizó la recopilación de la evidencia digital.[46]

A su vez, la propuesta de buenas prácticas recomienda la aplicación de una etapa de recolección de la prueba electrónica, donde se proteja la evidencia por medio de una cadena de custodia a cargo de un informático forense.[47] Esto con el fin de prevenir la alteración del documento por parte de terceros, una vez se haya recopilado y aportado al proceso todo el acervo probatorio digital.

---

45 El documento HB171-2003, es una propuesta para el ordenamiento jurídico australiano, que plantea una serie de buenas prácticas y de requisitos para la admisión de la prueba electrónica en dicho país.

46 Ley 527 de 1999, artículo 11. Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

47 El informático forense funcionaría como un auxiliar de la justicia, encargado de vigilar y proteger la evidencia digital que se pretenda hacer valer dentro de un proceso determinado.

La propuesta es la siguiente:

1. El juez deberá establecer qué pruebas son electrónicas y cuáles no. Ello con el fin de determinar cuáles evidencias digitales se les aplicará el estándar de valoración a proponer.
2. La persona natural o jurídica que pretenda hacer valer pruebas electrónicas dentro de un determinado litigio, deberá diseñar o contar con un sistema computacional para la evidencia electrónica que permita verificar e identificar el documento electrónico y esté disponible a la hora de la creación, alteración y de recolección del mismo.

   Para garantizar la efectividad y eficacia del diseño computacional, éste deberá identificar al autor del documento electrónico, establecer fecha y hora de la creación y/o alterabilidad del documento, establecer la autenticidad del contenido del mensaje de datos mediante la confiabilidad de los programas computacionales que permitan la no incursión de terceros de mala fe en la información contenida en el medio informático.

   Los programas informáticos deberán establecer la autenticidad del documento electrónico mediante la identificación del documento original y de las posibles alteraciones. Es decir, el sistema computacional deberá tener la capacidad de detectar cualquier alteración del documento con respecto a la información del documento original.

   Es así, como el juez deberá entrar a valorar los métodos de seguridad implementados por la parte emisora y la receptora. En este punto juega un papel preponderante el sistema de identificación y autenticación, criptografía, biométricos, entre otras técnicas ya implementadas, así como las que traiga la tecnología en el futuro. Es decir, el juez deberá estudiar si el documento electrónico se encuentra sometido a un determinado método de seguridad para garantizar, con ello, la confiabilidad sobre el contenido del mensaje de datos.
3. En la etapa de elaboración del documento, se deberá contar con un sistema que cumpla con la fase operacional de los pasos que se pretenden plantear, ya que se deberá determinar qué computador en específico fue el instrumento para la creación del mensaje de datos, estableciendo la fecha y la hora de la misma. A su vez, se deberá establecer que el programa computacional, en el momento de la creación o alteración del contenido del mensaje, funcionaba a cabalidad y sin error alguno. Lo anterior, con el fin de no alterar la confiabilidad del documento y la integridad del mismo, sabiendo de antemano si el almacenamiento del mensaje de datos pudo contar con algún inconveniente técnico. De ser así se desvirtuaría la seguridad de la técnica específica utilizada.

   De acuerdo a la técnica de seguridad implementada, el juez deberá establecer el grado de confianza que le brinde la técnica de seguridad efectuada. Es decir, el

juez deberá analizar si el sistema implementado, tanto por el emisor como por el receptor, es confiable. Lo anterior, significa que si el sistema utilizado es el de autenticación y clave, el juez deberá –según su propio criterio y discrecionalidad– evaluar que tan confiable pudo ser la clave y que tan secreta.

4. En la fase de recolección de la evidencia, ésta deberá llevarse a cabo por un informático forense,[48] especializado en la materia. Contar con dicho funcionario le daría mayor fuerza probatoria a la prueba electrónica, ya que el procedimiento le otorgará la confianza suficiente para admitir la prueba como evidencia dentro del acervo probatorio.

   El informático forense deberá hacer un recuento de cada uno de los procedimientos utilizados, los datos de fechas y horas de los documentos del computador. Así mismo, deberá identificar a cada uno de los autores de los mensajes de datos y todos los hechos inmersos en el sistema computacional.

   Sumado a lo anterior, será necesario implementar una cadena de custodia de las evidencias recolectadas y allegadas al proceso, con el fin de evitar posibles intromisiones y alteraciones de terceros. Por tal motivo, parece conveniente seguir con los planteamientos del artículo 288[49] del Código de Procedimiento Penal, el cual establece que se deberá aplicar la cadena de custodia a los elementos físicos materia de prueba, con el ánimo de garantizar la autenticidad de los mismos y acreditar tanto su identidad y estado original, envío, manejo, análisis y conservación de estos elementos, como los cambios hechos en ellos por cada custodio.

---

48 Ley 906 de 2004, artículo 236. Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.

Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen. (…)

49 Código de Procedimiento Penal, artículo 288. Cadena de custodia. Se debe aplicar la cadena de custodia a los elementos físicos materia de prueba, para garantizar la autenticidad de los mismos, acreditando su identidad y estado original, las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos, así mismo, los cambios hechos en ellos por cada custodio. La cadena de custodia se inicia en el lugar donde se obtiene, encuentre o recaude el elemento físico de prueba y finaliza por orden de la autoridad competente. Son responsables de la aplicación de la cadena de custodia todos los servidores públicos y los particulares que tengan relación con estos elementos, incluyendo al personal de servicios de salud, que dentro de sus funciones tengan contacto con elementos físicos que puedan ser de utilidad en la investigación. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, conforme con los avances científicos y técnicos.

Esta cadena deberá iniciarse en el lugar donde se obtiene la prueba y finalizar por orden judicial de la autoridad competente. Todos aquellos que tengan acceso a la evidencia digital serán responsables de llevar a cabo la cadena de custodia y se identificarán con el procedimiento implementado para el mismo.

5. Si se cumplen los pasos antes mencionados, el juez deberá admitir y aceptar el mensaje de datos como una prueba electrónica dentro del acervo probatorio del proceso. Además, dependiendo de la confidencialidad y el cumplimiento de los pasos antes planteados, podrá otorgarle —bajo su discrecionalidad— la fuerza probatoria que estime conveniente.

   A las partes les queda la posibilidad de controvertir la validez de la prueba o de tachar de falsa la información inmersa en el documento electrónico.

## 7. Conclusiones

1. La propuesta de buenas prácticas para la admisión y valoración de la prueba electrónica y para la incursión de las mismas en el sistema jurídico colombiano, tiene como principal ventaja, el simple hecho de que el juez tendrá una herramienta legal que le proporcionará seguridad, confiabilidad y certeza a la hora de admitir y valorar la evidencia digital, por cuanto tal práctica ya no queda sujeta a los criterios de la sana crítica y de la razonabilidad. Por lo tanto, el juez tendrá que entrar a analizar si la propuesta fue aplicada a cabalidad en la etapa de creación, de almacenamiento y de recopilación de la prueba digital. Pues si alguno de los pasos llegaren a faltar, el juez no le podrá otorgar la misma fuerza probatoria de aquel que haya cumplido a cabalidad con el estándar planteado. Es así como la tarea del juez ya no queda bajo su discrecionalidad, sino bajo los preceptos legales.
2. Una limitante para el sistema jurídico colombiano es que a pesar de que en la actualidad nuestro ordenamiento jurídico cuenta con múltiples normatividades que regulan el nuevo campo de acción entre los particulares y de la actividad estatal, todavía no existe una conciencia ni una cultura informática. Es decir que a pesar de la existencia de regulaciones claras que le otorgan plena seguridad a las transacciones celebradas por medios electrónicos, los operadores jurídicos y los mismos particulares hoy en día no cuentan con un acceso y dominio del tema, convirtiéndolos en personas escépticas a la consecución de este tipo de prácticas.
3. Algunas condiciones esenciales para la aplicación de la propuesta de buenas prácticas para la admisión y valoración de la prueba digital en el sistema jurídico colombiano, es la necesidad que existe de incluirla en el ordenamiento jurídico como ley de la República. Esto con el ánimo de que los jueces estén

sometidos a los preceptos de la misma, tal y como lo establece la Constitución en el artículo 230,[50] el cual estipula que los jueces, en sus providencias, sólo están sometidos al imperio de la ley.

A su vez, será necesario incentivar y propagar el uso de la Internet como campo de acción entre la actividad de los particulares y la estatal, creando una conciencia de seguridad de los negocios celebrados por medios informáticos.

4. Por último, para las personas que estén interesadas en seguir esta investigación, será necesario estudiar permanentemente los avances tecnológicos que innovan en gran medida la actividad humana. A su vez, será necesario estudiar las necesidades provenientes de las prácticas internas, en cuanto la complejidad y la amplitud del campo de la informática será cada vez mayor. Ello le dará mayores retos al derecho y por consiguiente, a sus operadores jurídicos al establecer nuevas necesidades en el contexto en el que se encuentren.

## 8. Referencias

HB 171 – 2003. Handbook of Guidelines for the Management of IT Evidence. Published by Standards Australia International Ltd.

DEVIS ECHANDÍA, Hernando. (1987) *Teoría General de la Prueba Judicial, Tomo I.* Primera Edición Colombiana. Editorial Biblioteca Jurídica Dike. Medellín.

DEVIS ECHANDÍA, Hernando. (1982). *Compendio de derecho procesal, Pruebas Judiciales, Tomo II.* Séptima Edición, Editorial ABC. Bogotá.

PARRA QUIJANO, Jairo (1986). *Manual de Derecho Probatorio*. Séptima Edición. Ediciones Librería del Profesional. Bogotá.

RIOFRÍO, JUAN CARLOS (2004). *La Prueba Electrónica*. Primera Edición. Bogotá - Colombia. Editorial Temis.

DEVIS ECHANDIA, Hernando (*1974*). *Teoría General de la Prueba, Tomo II.* Tercera Edición. Buenos Aires - Argentina. Editor Buenos Aires.

PARRA QUIJANO, Jairo (1988). Tratado de la Prueba Judicial, *"La prueba pericial y la inspección judicial"*, *Tomo V.* Tercera Edición. Bogotá - Colombia. Ediciones Librería del Profesional.

50 Constitución Política de Colombia, artículo 230. "Los jueces, en sus providencias, sólo están sometidos al imperio de la Ley. La equidad, la jurisprudencia, los principios generales del derecho y la doctrina son criterios auxiliares de la actividad judicial."

PARRA QUIJANO, Jairo (1988). *Tratado de la Prueba Judicial, Indicios y Presunciones, Tomo IV*. Tercera Edición. Bogotá-Colombia. Ediciones Librería del Profesional.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en la Legislación Colombiana.

Ley 906 de 2004. Por medio de la cual se expide el Código de Procedimiento Penal.

Ley 446 de 1998. Por la cual por la cual se adoptan como legislación permanente algunas normas del Decreto 2651 de 1991, se modifican algunas del Código de Procedimiento Civil, se derogan otras de la Ley 23 de 1991 y del Decreto 2279 de 1989, se modifican y expiden normas del Código Contencioso Administrativo y se dictan otras disposiciones sobre descongestión, eficiencia y acceso a la justicia.

Código de Procedimiento Civil Colombiano.

Código de Procedimiento Penal Colombiano.

Sentencia C 662 de 2000. Corte Constitucional. M.P.: Fabio Morón Díaz.

Sentencia de marzo 27 de 1998, Expediente 4943. Consejo de Estado, Sala de Casación Civil. Magistrado Ponente: Carlos Esteban Jaramillo Schloss.

Auto de junio 19 de 1978. Tribunal Superior de Bogotá. Magistrado Ponente: Humberto Rodríguez Robayo.

UMAÑA CHAUX, Andrés Felipe (2005, Abril). *Algunos comentarios sobre el principio del equivalente funcional en la Ley 527 de 1999.* Revista de Derecho Comunicaciones y Nuevas Tecnologías. Volumen I. No. ISSN1794-9254. Ediciones Uniandes.

Mosquera González, José Alejandro. Certain Jaramillo, Andrés Felipe. Cano, Jeimy J.. (2005). *Evidencia Digital contexto, situación e implicaciones nacionales.* Revista de Derecho Comunicaciones y Nuevas Tecnologías. Volumen I. No. ISSN1794-9254. Ediciones Uniandes.

Ramos Suárez, Fernando (1999, julio). Revista electrónica ALFA-REDI *Eficacia jurídica de una transacción electrónica. La figura del no repudio*, Edición Número 12. Consultado el día 1 de diciembre de 2005 en de la World Wide Web http://www.alfa-redi.org/rdi-articulo.shtml?x=300

International Association of Chiefs of Police Advisory Committee for Police Investigative Operations. Best Practices for Seizing Electronic Evidence. Consultado el día 8 de noviembre de 2005 de la World Wide Web: http://www.fletc.gov/legal/downloads/bestpractices.pdf

Ministerio de Industria, Turismo y Transporte de España. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.setsi.mcyt.es/legisla/internet/rdley14_99.htm.

Real Decreto Ley 1906 de 1999. Consultado el 8 de noviembre de la la World Wide Web: http://www.aeat.es/normlegi/ecomercio/rd171299.htm

Uniform Rules of Evidence. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm

Federal Rules of Evidence. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm

Electronic Signatures in Global and National Commerce Act del 2000. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.ricardolorenzetti.com.ar/secciones/comercio_electronico1.htm

Ley de firmas y certificados No. 27269 de Perú. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.indecopi.gob.pe/upload/crt/firmasDigitales/reglamentods019-2002-jus.PDF

Ley 25.506 de Argentina. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.safjp.gov.ar/digesto_2/index/normas/LEY%2024241/Ley25506.htm

Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma No. 19.789 de Chile. Consultado el día 8 de Noviembre de 2005 de la World Wide Web http://www.cedi.uchile.cl/docs/Ley19799.pdf

National Institute of Standards and Technology. Computer Security Division. Consultado el día 8 de noviembre de 2005 en de la World Wide Web http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter19.html

National Institute of Standards and Technology. Computer Security Division. Consultado el día 8 de noviembre de 2005 de la World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter19.html

National Institute of Standards and Technology. Computer Security Division. Consultado el día 8 de noviembre de 2005 de la World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter16.html