

# LA INFORMÁTICA FORENSE COMO HERRAMIENTA PARA LA APLICACIÓN DE LA PRUEBA ELECTRÓNICA<sup>1</sup>

*Alejandra Montoya Rojas<sup>2</sup>*

**Resumen:** El auge de las comunicaciones y la informática ha traído grandes cambios al mundo entero, cambios que no solo han impactado a la sociedad sino también al sistema de Administración de Justicia como escenario idóneo para la solución de controversias. La informática forense ha sido una de las herramientas creadas para motivar el uso de los medios electrónicos.

Esta investigación tiene como objetivo principal mostrar el reconocimiento y aceptación de las tecnologías de la información y comunicación en el desarrollo del proceso judicial, sobre todo si se tiene en cuenta los cambios que la ley 1395 de 2010 trae a la Administración de Justicia en Colombia, cambios que no solo modifican la forma de Administrar Justicia, sino de invocar la tutela judicial efectiva, por lo cual se hace necesario, a luz de las tecnologías de informática y la comunicación, implementar un marco de regulación más amplio que permita la aplicación de métodos y técnicas que coadyuven a la utilización de los avances en materia informática y electrónica.

**Palabras clave:** Administración de justicia, informática forense, medios electrónicos, elementos materiales probatorios, documento electrónico.

**Abstract:** The height of the communications and computer science has brought great changes to the entire world, changes that not only have impacted society but also are an impact to the society but also Justice System, as a suitable stage for the solution of controversies. Forensic computer science has been one of the tools created to motivate the use of the electronic means in society, since this science not only looks for support in the work of investigation and collection of probatory elements, but also one of its main aims is, the verification and establishment that the information contained in the electronic document has not been modified or adulterated during the handling, or during the process of investigation. The implementation and use of the laboratories of forensic computation within the judicial courts as a mechanism to make an effective application not only of the principle of procedural economy but also of the effective access to the

---

<sup>1</sup> Este artículo de investigación es el resultado de la investigación socio – jurídica que se ha venido desarrollando al interior del proyecto de investigación titulado “La Prueba Electrónica. Su Aportación y Valoración”.

<sup>2</sup> Abogada e integrante del grupo de investigación *Estudios Jurídicos* de la Universidad CES.  
Correo electrónico: amontoyar@ces.edu.co.

administration of justice, depends on the diffusion given to the procedure, and also to the effectiveness of the authenticity of the electronic proof.

**Key words:** Administration of justice, forensic computer science, electronic media, material proof elements, electronic document, forensic computer science laboratories, judicial courts.

## **Introducción**

Los desarrollos que en materia de informática se han venido presentando en el mundo entero han dado surgimiento a las tecnologías de información y comunicación, tecnologías que para su utilización requieren de conocimientos técnicos y métodos que propendan por su utilización.

El primer paso que al interior de los países se ha dado es la creación de la normatividad<sup>3</sup> que implementa el uso y coadyuva a la solución de las contingencias que como consecuencia de la utilización de la tecnología se presentan, contingencias que a pesar de estar reguladas por una norma jurídica desbordan el marco de su regulación y requieren de nuevos instrumentos.

Lo anterior es la razón por la que estamos en un constante llamado a la evolución técnica y tecnológica, a la nueva generación de métodos innovadores que se ajusten a los cambios del día a día.

A pesar de ser el Estado el principal convocado a gestionar y generar las capacitaciones necesarias para el conocimiento de las tecnologías, no es el único que se beneficia de su uso, es toda la comunidad la que debe difundir el manejo y utilización de los mecanismo previstos actualmente y estar abierta a acoger los nuevos métodos.

El Estado como depositario del "ius puniendi", esto es, el derecho de velar por el cumplimiento de las normas jurídicas e imponer sanciones cuando se incumplen los preceptos que estas consagran, es el principal encargado de guiar el uso de estos medios, sobre todo en materia de Administración de Justicia, pues sería este el escenario idóneo para equilibrar y poner a la par el derecho con las conductas de los coasociados.

## **Desarrollo**

No es adecuado a la luz del derecho moderno hablar de nuevas tecnologías de información y comunicación porque su creación y uso en países desarrollados no se remonta a este siglo, por el contrario desde ya entrado el siglo XIX se han presentado significativos avances tecnológicos e invenciones técnicas que permiten hacer alusión a métodos de comunicación y recaudo de información diferentes a los comunes. Colombia no ha sido un país ajeno a esta implementación de mecanismos tecnológicos, por el contrario desde 1982<sup>4</sup> ha tratado de regular el tema.

---

<sup>3</sup> En España se sancionó el Real Decreto Ley 14 sobre firma electrónica en el año de 1995 y en Colombia se promulgó la Ley 527 de 1999.

<sup>4</sup> Se expidió el decreto 2328 "por medio del cual se dictan normas sobre el servicio de transmisión o recepción de información codificada (datos) entre equipos informáticos, es decir, computadoras y-o terminales en el territorio nacional", Luego se expidió el decreto

El Estado Colombiano adecuándose a las realidades actuales y a los avances informáticos que en las mismas se presentan, ha regulado mediante el artículo 95 de la ley Estatutaria de la Administración de Justicia<sup>5</sup> y la ley 527 de 1999<sup>6</sup>, la prueba electrónica, como el mecanismo idóneo para allegar los hechos tipo o causa fáctica objeto de la pretensión a un proceso judicial.

La adecuación de la normatividad Colombiana a mecanismos electrónicos que impulsen el desarrollo tecnológico de la Administración de Justicia y por ende del Estado mismo, es resultado de la ley UNCITRAL<sup>7</sup>, ley modelo de comercio electrónico, expedida por las naciones unidas, que motiva a los países para legislar sobre el denominado documento electrónico contentivo de episodios negociales internacionales e incluso nacionales.

Al interior de nuestro país no ha sido pacífico el tema de los documentos electrónicos, ni muchos menos ha sido tarea fácil la implementación y uso de los mismos en los estrados judiciales, toda vez que a pesar de la regulación normativa que se ha venido dando los funcionarios judiciales y los mismos abogados, encargados de poner a funcionar el aparato jurisdiccional en nombre de sus clientes, se rehúsan a la utilización de métodos innovadores y prácticos y siguen atados a los mecanismos comunes de acceso a la justicia.

Es nuestro ordenamiento jurídico tan adaptable a las nuevas tendencias, que incluso de acuerdo al artículo 175<sup>8</sup> del código de procedimiento civil, que autoriza la práctica de pruebas no previstas normativamente, se considera al

---

148 de 1984 “ por el cual se dictan normas sobre los servicios de transmisión de información codificada (datos) para correspondencia pública y se reglamentan parcialmente los artículos 184 y 186 del decreto ley 222 de 1983” (1982).

<sup>5</sup> El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia... 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.

<sup>6</sup> “Por medio de la cual se define ya 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”

<sup>7</sup> United Nations Commission on International Trade Law - Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional.

<sup>8</sup> Sirven como pruebas, la declaración de parte, el 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.

documento electrónico como un medio de prueba más, que engrosa la lista enunciativa de la legislación procesal colombiana.

Igualmente no solo el ordenamiento jurídico se encuentra abierto a la aplicación de medios informáticos en la estructura administrativa y jurídica del estado, sino que estos nuevos mecanismos también tienen un lugar en la doctrina colombiana<sup>9</sup>, son aceptados y propenden por su uso no solo al interior de las entidades estatales sino también por parte de los particulares, razón de ser de la Administración de Justicia.

De acuerdo a lo anterior no se puede decir que hay ausencia de desarrollos electrónicos, ni que el ordenamiento jurídico colombiano carece de reglamentación jurídica, pues no es este el problema que nos avoca actualmente, es la falta de capacitación y adaptación a las nuevas tendencias la que impide la utilización en nuestro medio de los mecanismos informáticos.

Uno de los temas que ha generado mayor polémica es el de la validez de los documentos electrónicos o mensajes de datos<sup>10</sup>, como los denomina la ley de comercio electrónico, puesto que los operadores jurídicos y en general los abogados y ciudadanos que hacen uso de la Administración de Justicia desconocen que el documento electrónico está en capacidad de otorgar al receptor la misma seguridad que otorgan los documentos consignados en papel, generan incluso un mayor nivel de confianza y rapidez.

Es pertinente de acuerdo a lo anterior citar al Doctor Hernando Devis Echandía, quien define la prueba como “los motivos que sirven para llevarle al juez la certeza de los hechos” (Echandía: 1970, página 28), definición en la cual encaja perfectamente el documento electrónico, entendido como aquel contenido de los episodios fácticos sustento de la pretensión y que de acuerdo al artículo 175 del Código de Procedimiento Civil tiene la calidad de medio de prueba y por lo tanto esta en la capacidad, como un documento consignado en papel, de llevar al juez la convicción de certeza y seguridad sobre las circunstancias acaecidas, sometándose para tal fin, a las mismas reglas de contradicción que el documento escrito, permitiendo que se verifique tanto su contenido como autoría. Es por esto que no cabe duda sobre la validez del mensaje de datos, toda vez que los mismos

---

<sup>9</sup> “Los medios informáticos son verdaderos documentos pues poseen corpus y docet. El corpus comprende la grafía y el soporte material. El docet está integrado por la intencionalidad y la expresividad del lenguaje. Si un medio electrónico posee estos elementos se puede considerar documento en un proceso”. (Bergel, Salvador. Informática y responsabilidad civil. Informática y Derecho, vol.2, pag.213 y sgts. Buenos Aires, 1988).

<sup>10</sup> Ley 527 de 1999, Artículo 2° Definición: “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; (...).”

no solo son considerados medios de pruebas sino que también se puede ejercer respecto de ellos el derecho de contradicción, que a su vez garantiza el debido proceso consagrado en nuestra Carta Política.

Otro de los aspectos polémicos al interior de nuestro ordenamiento jurídico, en lo que respecta a la utilización de la prueba electrónica, es el de la seguridad jurídica que ofrece este mecanismo a los funcionarios judiciales encargados de aplicar el derecho al caso concreto y plasmarlo en la sentencia judicial, pues a pesar que el régimen probatorio colombiano cuenta con un soporte jurídico que permite la valoración y aceptación de la prueba electrónica, en la práctica judicial se desconoce por parte de los jueces las técnicas e instrumentos que permiten rectificar la veracidad de la información contenida en el documento electrónico, razón por la cual esta herramienta para llevar los hechos al proceso no adquiere la misma fuerza probatoria que cualquier otro medio de prueba.

Como consecuencia de lo anterior no se admite como prueba plena la prueba electrónica, por el contrario al momento de su valoración se hace uso de alternativas jurídicas como los indicios y el peritazgo, que a pesar de ser medios de prueba idóneos para llevar los hechos al proceso, no fueron los elegidos por las partes o dilatan más el proceso mismo, restando a su vez fuerza probatoria al mensaje de datos.

Darle una valoración a la prueba electrónica como meros indicios, disminuye el valor probatorio que ella, como medio de prueba independiente a los demás, tiene, y por ende cuando suceda esto, la prueba electrónica no sería medio idóneo para llevarle al juez la certeza sobre los hechos acaecidos. La justificación que se ha dado para la ocurrencia de este fenómeno, es que la información contenida en el mensaje de datos no logra llevar al juez la seguridad jurídica necesaria sobre la autenticidad y autoría del documento.

Lo anterior ha llevado a que el funcionario judicial nunca fundamente sus decisiones en una prueba electrónica como medio de prueba autónomo, que evite incluso darle el carácter de medio de prueba idóneo, conducente y pertinente al mensaje de datos, igualmente con la tendencia de vincular al proceso la prueba electrónica a través de indicios y peritazgo se está anulando la eficacia de este mecanismo probatorio.

Las anteriores formas de introducir la prueba informática al proceso judicial, se pueden explicar desde el desconocimiento de los funcionarios judiciales, la falta de capacitación y la ausencia de herramientas técnicas que permitan ponerse a la vanguardia de los avances tecnológicos, claro está que no se puede generalizar la vinculación de la prueba electrónica por medio de indicios o peritazgo al proceso, porque también hay funcionarios judiciales que la valoran como un medio de prueba con autonomía propia.

Como primera medida para evitar que los funcionarios judiciales impulsen el uso de la prueba electrónica como una prueba secundaria, desprovista de autonomía, el Consejo Superior de la Judicatura ha implementado en la rama judicial capacitaciones tanto para los operadores jurídicos como para el público en general (abogados – particulares) que les permita conocer y utilizar los mecanismos técnicos y tecnológicos. En el mismo sentido este organismo de control ha expedido unos acuerdos donde reglamenta e impone pautas para el uso de los documentos electrónicos como medios de prueba, estos acuerdos se encuentran consignados en el Centro de Documentación Judicial del Consejo Superior de la Judicatura de Colombia (CENDOJ).

Otro de los mecanismos para lograr el uso de la prueba electrónica como un medio de prueba que tiene la misma seguridad jurídica, en cuanto a la inalterabilidad y veracidad de su contenido, que los demás medios de prueba, específicamente el documento escrito, es el principio de equivalente funcional consignado en la ley de comercio electrónico. Este principio tiene por finalidad adaptar y concederle la misma fuerza probatoria de los documentos consignados en papel a los documentos en formato de mensajes de datos.

Para alcanzar la finalidad anterior, la ley 527 de 1996 que consagra el principio de equivalente funcional establece unos requisitos formales que la información contenida en el mensaje de datos tiene que satisfacer para ser considerada por el destinatario jurídico como medio de prueba capaz de llevar la certeza de los hechos objeto del proceso. Los requisitos que la información debe cumplir se circunscriben al equivalente funcional a escrito<sup>11</sup>, equivalente funcional a firma<sup>12</sup> y el equivalente funcional a origina<sup>13</sup>.

Así mismo, es importante resaltar que el equivalente funcional no es una forma de valoración, es simplemente un patrón de interpretación que consagra la ley de comercio electrónico para darle mayor posibilidad al juez de constatar la

---

<sup>11</sup> La Ley 527 de 1999 establece en su artículo 6. “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...”

<sup>12</sup> La Ley 527 de 1999 establece en su Artículo 7. “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 iniciador de un mensaje de datos 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...”

<sup>13</sup> La Ley 527 de 1999 establece en su artículo 8: “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...”

veracidad de la información contenida en el documento electrónico, permitiéndole a su vez expandir la concepción humana a nuevas posibilidades tecnológicas igual de idóneas y eficaces a las tradicionales.

La ley 527 de 1999 tratando de dar seguridad jurídica a los funcionarios judiciales sobre la información contenida en el mensaje de datos ha incluido en el marco de su regulación las entidades de certificación<sup>14</sup>, que tienen como una de sus funciones principales “emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos”. Estas funciones de certificación en Colombia las cumplen las Cámaras de Comercio, son entidades de fácil acceso al público y permiten llevar al juez la seguridad sobre la autenticidad, no alterabilidad de la información y firma digital del remitente del documento electrónico.

Como tema central de este artículo y sin restarle importancia a los demás mecanismos que buscan darle seguridad jurídica a la información contenida en el documento informático, se encuentran los laboratorios de computación forense o la denomina informática forense; rama de la investigación forense que se encarga de la investigación y búsqueda de pruebas en medios electrónicos.

A pesar que en nuestro país los desarrollos de esta rama de la investigación han sido muy precarios y se han dado casi todos en la actualidad, no se puede decir, en estricto sentido, que apenas ha venido surgiendo, puesto que sus orígenes se remontan a 1984, cuando el FBI y otras agencias de Estados Unidos comenzaron a desarrollar programas para examinar evidencia informática.

La informática forense está construida sobre una serie de metodologías diseñadas para guiar las investigaciones y los procesos de búsqueda de pruebas, de forma tal que se pueda asegurar que la información no ha sido modificada o dañada en el proceso o durante la investigación.

En la actualidad se ha venido impulsando la utilización de medios electrónicos, sobre todo con los dispositivos digitales de almacenamiento de información<sup>15</sup>, los cuales son utilizados para la ejecución de negocios, implementación de sistemas de trabajo y en general para el desarrollo de

---

<sup>14</sup> La Ley 527 establece en su artículo 2, literal d): es una entidad de certificación “ aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales”.

<sup>15</sup> Los medios de almacenamiento digital son aquellos que permiten almacenar información tales como: medios ópticos CD, DVD, Discos BlueRay, entre otros, medios electromagnéticos como: Discos duros, diskettes y cintas electromagnéticas.

cualquier conducta. Esta época ha sido conocida como la era de lo digital, era que ha traído consigo consecuencias que no se encuentran reguladas por una norma jurídica o si se encuentran exceden el marco regulatorio, como lo ejemplifica un informe presentado por el periódico el tiempo:

...se han denunciado casi 180 casos de fraude electrónico, que en total han costado más de 349.000 millones de pesos a personas naturales y cerca de 6,6 billones de pesos a empresas, según cifras que reveló la Dijín durante el lanzamiento de la Semana de la Seguridad...<sup>16</sup>

Las actuaciones anteriores, que cada día son más frecuentes, hacen necesaria la implementación de medios de análisis, como los laboratorios de investigación forense, máxime si se tiene en cuenta que esta clase de conductas desbordan la metodología y técnica empleada por los tradicionales métodos de investigación y recolección de datos.

Colombia no ha sido un país ajeno a los cambios tecnológicos, y por esto para adaptarse a las consecuencias que los mismos traen ha creado no solo un marco de regulación normativa, sino que también cuenta con equipos de respuesta de seguridad de cómputo, los cuales se encargan de la investigación de delitos en la red o de cualquier anomalía que al interior de la misma se dé y sea debidamente reportada, estas investigación que hace este grupo no son automáticas, debe mediar entre el inicio de la investigación y la conducta realizada en la red una especie de denuncia o informe por parte del afectado.<sup>17</sup>

Independiente de las consecuencias desfavorables que pueda traer consigo la utilización de mensajes de datos o documentos electrónicos, igualmente este mecanismo de almacenamiento, a diferencia de los medios físicos de almacenamiento de información, permite que la información que se borra, no se eliminada realmente del dispositivo, sino que sea registrada en un archivo (MTF o FAT) que no tiene acceso directo, pero que igual se conserva dentro del dispositivo y si se requiere puede ser recuperada. Esta es una ventaja, que siendo reiterativa, no ofrece la evidencia física, puesto que en está no hay posibilidad de obtener una copia exactamente igual a un Elemento Probatorio original.

Casi siempre la información que se genera a través de dispositivos de almacenamiento digital o documentos electrónicos son Elementos Materiales

---

<sup>16</sup> Los Delitos Informáticos, En Aumento [online]. [Bogotá, Colombia]: ciencia y tecnología, 7-mayo-2007 [Cited 8 noviembre 2008]. Puede ser consultado en: <http://www.eltiempo.com/archivo/documento/MAM-2485829>.

<sup>17</sup> El mayor Fredy Bautista, jefe del grupo de delitos informáticos de la Dirección de la Policía Judicial de Colombia, señala que *“muchas de las conductas realizadas en la Web no son investigadas porque la mayoría de empresas no denuncian sus casos, pues temen perder credibilidad, o sufrir consecuencias de tipo económicas u otras similares”*.

Probatorios, que dadas las circunstancias pueden servir como medios de prueba en un proceso.

El análisis que se realiza a la información eliminada del dispositivo de almacenamiento digital, no es un simple análisis de datos, sino que implica una serie de pasos, y se puede desarrollar a través de diferentes métodos, que no solo sirven para recuperar el archivo eliminado, sino también para verificar que la información no haya sido adulterada en su contenido y remitido.

Los métodos más conocidos son el de la copia Bit a Bit y los Algoritmos. La copia bit a bit es una herramienta que originalmente no fue creada para ser utilizada por la informática forense, sino para la administración de sistemas y para hacer respaldo de datos, pero dados los resultados se comenzó a utilizar, específicamente el programa "dd" que permite hacer el proceso de copia de la información contenida en el medio de almacenamiento desde cualquier computador y tiene un porcentaje de efectividad del 100%. Hoy ha avanzado tanto la ciencia de la informática forense, que se han diseñado equipos especializados para hacer copias bit a bit de medios de almacenamiento que pueden haber sufrido daños, sin influir estos daños en el resultado o la veracidad de la información contenida en el dispositivo de almacenamiento.

Vale la pena señalar que la información contenida en el documento electrónico, no es solo una combinación de átomos sino que también existen documentos conformados por Bits, lo que hace más fácil la copia bit a bit y da mayor confianza el resultado del proceso de copia, en lo que atañe a la veracidad e inmodificabilidad de la información.

El medio donde se encuentra la evidencia material probatoria no es el elemento al que se le realiza la réplica, sino a los bits que están contenidos en él y son los bits los que forman el Elemento Material Probatorio. Los pasos que se deben realizar para analizar la información que se encuentra dentro del medio de almacenamiento, es en primer lugar realizar la copia bit a bit para no trabajar sobre la información contenida en el dispositivo de almacenamiento, adicional a la copia, es recomendable, realizar otra copia bit a bit de la copia, de forma tal que hay una imagen de referencia de la original, hay una réplica y una copia se está última, que servirá para realizar los procedimientos de análisis, con este proceso no solo se verifica que la información contenida no haya sido alterada, sino que también se podría recuperar archivos e información borrada.

La seguridad jurídica que otorga este sistema de copia radica en que sobre el medio de almacenamiento solo se realiza una lectura que sirve para extraer la copia o réplica, quedando incólume el Elemento Material Probatorio, esto es, no se modifica o altera la información, por el contrario se verifica que la misma no haya sufrido cambios sustanciales en su contenido. El único inconveniente que ha este sistema se le ha encontrado es que cuando los archivos son más grandes, la

copia bit a bit puede tener cierto porcentaje mínimo error en cuanto a la verificación de inalterabilidad de la información. Es por esta razón que existe otra herramienta, los algoritmos, que no tienen la misma finalidad de la copia bit a bit, pues busca conservar la cadena de custodia, pero que igual otra de sus finalidades va encaminada a la verificación de no adulterabilidad de la información dada en cadena de custodia; su fin mediato no es buscar que la información no haya sido adulterada, sino conservar y evitar que se rompa la cadena de custodia, pero para lograr esto necesariamente se tiene que pasar por la verificación de veracidad de los datos.

De acuerdo al diccionario de la Real Academia de la Lengua Española, un algoritmo es un *“Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema”*, en otras palabras es un conjunto de pasos que si se sigue en un orden específico permite alcanzar un resultado. Todos los programas de computadores son algoritmos programados en los computadores, que se encargan de ir y buscar donde está almacenado el programa, cargarlo al encontrarlo y mostrárselo al usuario.

Adicional a los algoritmos de HASH<sup>18</sup> hay otra clase de algoritmos que también pueden ser utilizados para el análisis de datos, pero que quizás su forma de uso es más compleja y trae el mismo resultado, son igualmente confiables, es por esto que los algoritmos de HASH son la herramienta más usada en seguridad informática a lo largo del mundo, no solo en el sistema de cadena de custodia, sino también para determinar si las evidencias o documentos recuperados de un dispositivo de almacenamiento han sido modificados voluntaria o involuntariamente durante la investigación.

Los algoritmos HASH operan calculando un valor resultante llamado huella digital a partir de un dato o información de entrada, este dato de entrada puede ser una cadena de caracteres, un archivo o hasta una imagen bit a bit, a partir del cálculo de la huella digital, que es la que caracteriza la información, se establece si esta última ha sido o no modificada.

Tanto los algoritmos HASH como la copia bit a bit son herramientas de la ciencia forense para analizar la información contenida en los dispositivos de almacenamiento y verificar que la misma no haya sufrido cambios sustanciales en el contenido. A pesar que los algoritmos busquen conservar la cadena de custodia y la copia bit a bit verificar la autenticidad de la información contenida en cualquier medio de almacenamiento, en estricto sentido, como ya se señaló, su objetivo, a luz del derecho, es servir de medio para garantizar o dar seguridad a los

---

<sup>18</sup> Un HASH es el resultado alfanumérico que se obtiene de procesar un mensaje, texto o cualquier tipo de archivo y uno de sus usos más importantes es verificar que este mensaje, texto o archivo no ha sido modificado.

funcionarios judiciales de la inalterabilidad de la información e idoneidad de la prueba electrónica o mensaje de datos.

Adicional a las herramientas anteriores, la informática forense cuenta con otros sistemas, como por ejemplo los MFT y FAT (File asignment table), que son programas configurados para guardar registro de todo lo que ocurre con los datos de almacenados en el medio, registros que muchas veces el equipo no almacena por dejar evidencia sino porque hace parte del funcionamiento mismo, pero que es un mecanismo muy útil para la ciencia forense y facilita su trabajo de investigación. En el mismo sentido hay programas, como los logs de seguridad de Windows, que permiten que las personas voluntariamente puedan activar el sistema de registro, esto es lo más común en las compañías.

En concordancia con lo anterior, existe un proceso que permite generar un archivo para ver la historia de la información guardada en los MFT y FAT (File asignment table), accediendo a los nombres de todos los registros que están o estuvieron en el medio de almacenamiento, observando cuál de los archivos fue modificado, accesado o creado, este proceso se llama MAC (Media Access Control o Control de Acceso al Medio) time, la única limitación o desventaja que se le ha detectado es que solo se puede ver la historia desde la última vez que se formateó el medio de almacenamiento de manera física.

Así como hay múltiples herramientas y sistemas de los que se sirve la informática forense, también hay un gran número de fuentes importantes de evidencia, dentro de las cuales se encuentran, como fuente principal, los discos duros de los computadores, los registros en los servidores y como una de las fuentes más utilizada se encuentran las ISP (Internet Service Provider) de las empresas que prestan el servicio de Internet como UNE, TELMEX o ETB.

En nuestro país la aplicación de los procesos y herramientas anteriores se comenzó a dar en el 2004, año en que se creó la Dirección de Investigación Criminal y surgió la ciencia forense como una ciencia de apoyo a las labores investigativas desempeñadas por la Policía Nacional.

Partiendo del surgimiento, a nivel mundial, de la Ciencia forense en el año de 1984, es evidente que el desarrollo colombiano en esta área además de ser tardío ha sido precario, tanto a nivel normativo como jurisprudencial y doctrinario, es por esto que los autores conocedores del tema han llegado a exponer que Colombia no es un país que se encuentre en capacidad de generar conocimientos de informática forense, razón por la cual se hace necesario acudir a países que si

están capacitados y pueden generar no solo conocimientos teóricos sino también prácticos<sup>19</sup>.

Actualmente, de acuerdo a la ley 906 de 2004, el periodo de investigación dentro del proceso penal está a cargo de la Fiscalía General de la Nación, y dentro de ésta la encargada de recopilar la evidencia y presentarla en la audiencia del juicio oral es la Policía Judicial, quien cuenta con un equipo especializado, para garantizar la inalterabilidad de la información sometida a cadena custodia.

La Contraloría General de la República, quien en veces se ocupa de funciones de investigación, fue la primera entidad en Latinoamérica que tuvo a su disposición un laboratorio de informática forense para determinar actos ilícitos o fraudes donde el patrimonio del Estado corriera algún riesgo.

En la actualidad no solo la Contraloría cuenta con laboratorios de computación forense, sino también la Policía Nacional, pues en los últimos años se han creado por parte de la Dijin cinco laboratorios dotados con toda la tecnología necesaria y se han capacitado a 50 policías en el manejo de los mismos, de forma tal que se puedan investigar y combatir los delitos informáticos. En este mismo sentido, debido al incremento de robos y fraudes en la red, el DAS ha fortalecido los mecanismos de defensa en los dispositivos de almacenamiento, para hacer más eficiente la lucha contra estos ataques electrónicos.

A pesar de los esfuerzos y mecanismos implementados por el Departamento Administrativo de Seguridad y la Dijin, la legislación colombiana no tiene al interior de su normatividad penal tipificados los delitos informáticos, lo que impide que las personas que ejecutan dichas conductas en la red sean sancionadas, pues al no adecuarse su conducta a una norma tampoco hay consecuencia jurídica aplicable. El mayor Fredy Bautista expresa al respecto que *“la actual legislación colombiana contempla algunas de estas conductas en cuanto a lo que tiene que ver con acceso abusivo a un sistema informático (art. 195), sabotaje (art. 199), o violación a los Derechos Patrimoniales de Autor (Art. 271 y 272)”*, con la regulación de estos delitos se estaría impidiendo no solo los fraudes electrónicos, sino que se daría mayor seguridad a los usuarios y destinatarios de la información contenida en formato electrónico.

---

<sup>19</sup> La forma de llevar a la práctica la informática forense es a través de los laboratorios forenses uno de los pasos más importantes para llevar a cabo la investigación, puesto que es allí donde se hace el análisis de la información contenida en los medios de almacenamiento digital recolectados como evidencia física.

Ha tenido tanto impacto y trascendencia el tema de la informática forense y sus implicaciones tanto jurídicas como sociales, que en este momento se está tramitando un proyecto de ley sobre la Protección de la Información y de los datos, con la finalidad de regular en forma más amplia el tema e imponer limitaciones al mal uso de este mecanismo.

Es importante, para finalizar, resaltar las palabras del mayor Bautista cuando hace referencia a los logros que en materia informática ha tenido nuestro país: “Colombia tiene la tecnología disponible en el mercado y eso nos pone a la vanguardia en la lucha contra la criminalidad electrónica en Latinoamérica. Hemos implementado servicios de interacción virtual entre la comunidad y la Policía”. Estos avances que la ciencia forense ha tenido no solo al interior de Colombia, sino de muchos países más, han traído consigo grandes logros en materia informática y de telecomunicaciones, pero también han exigido la implementación de mecanismos que permitan la difusión y utilización de los mismos, no solo a nivel de la Administración de Justicia, sino también de los particulares razón de ser de esta última.

Cada día es más necesario dar a conocer la ciencia forense como ese mecanismo que permite a los funcionarios judiciales y usuarios del sistema de administración de justicia utilizar los medios electrónicos como herramientas que gozan de plena validez, idoneidad y acogida dentro del sistema actual, que permite a los particulares tener un acceso diferente y más ágil y a los funcionarios tomar sus decisiones fundamentadas en métodos diferentes a los tradicionales pero que ofrecen las mismas garantías, seguridad y certeza sobre los hechos tipo objeto del proceso.

## **Conclusiones**

La investigación que se ha realizado demuestra la importancia y trascendencia del tema objeto de análisis, puesto que los avances tecnológicos crecen cada día más y promueven la realización de las conductas de los coasociados a través de ellos, lo que hace necesario, no solo un marco de regulación normativa más amplio, sino también la aplicación métodos y técnicas que permitan la utilización de los avances electrónicos.

La administración de justicia es la principal avocada a la implementación de herramientas como la informática forense dentro de sus procesos judiciales, no solo para fomentar la aportación y valoración en debida forma de los medios informáticos, sino para difundir entre los actores del proceso el conocimiento de esta ciencia de la investigación.

No basta con la existencia de laboratorios de investigación forense, se requiere que el Estado sea un difusor de los mismos y permita no solo a sus miembros y entidades acceder a ellos, sino también al público en general.

## REFERENCIAS

### Jurisprudencia

Sentencia Consejo de Estado. Sala Contencioso Administrativa, sección segunda. Auto del 19 de diciembre de 1998. Magistrado Ponente: Carlos Arturo Orjuela Góngora.

Sentencia Corte Suprema de Justicia. Sala Laboral. Auto 13015 de Abril 3 de 2000. Magistrado Ponente: José Roberto Herrera Vergara.

Sentencia Corte Constitucional. Sentencia [C-037 del](#) 5 de 1996. Magistrado Ponente: Vladimiro Naranjo Mesa.

Decreto 1094 del 21 de junio de 1996. “Por medio del cual se reglamenta el artículo 612 de 1994 del Estatuto Tributario”.

Decreto 2150 de 1995. “Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública”.

### Legislación

Ley 223 del 20 de diciembre de 1995. “Por la cual se expiden normas sobre racionalización tributaria y se dictan otras disposiciones”.

Ley 527 de 1999 del 18 de agosto de 1999. “Por medio de la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Ley 270 de 1996. “Estatutaria de Administración de Justicia”.

### Doctrina

Artículo (Inédito). (2004). Díaz, A., *Acceso a la administración de justicia por medios electrónicos*. Juez Segundo Promiscuo Municipal. Rovira (Tolima).

Camelo, C. y otros. (2004) El documento electrónico: aspectos procesales. *Revista Chilena de Derecho Informático*. Santiago de Chile: Universidad de Chile, No. 4, páginas 81-106.

Cano, J. J., Pimentel, J. Consideraciones Sobre el Estado del Arte del Peritaje Informático y los estándares de manipulación de pruebas electrónicas en el

mundo. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*. Bogotá: Universidad de los Andes, No. 3, diciembre de 2007.

Cano, J. J. y Pimentel, J. Valoración de la evidencia digital: Análisis y propuesta en el contexto de la administración de justicia en Colombia. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*. Bogotá: Universidad de los Andes, agosto de 2006.

Echandía, D. (1970). *Teoría General de la Prueba Judicial*. Buenos Aires: Nolberth.

Peña, D. (2001). *Aspectos legales de Internet y del comercio electrónico*. Bogotá: Dupré editores. 2001.

Rincón E., Cubillos R. (2002). *Introducción Jurídica al Comercio Electrónico*. Bogotá: Editorial Gustavo Ibáñez. 2002.

Riofrío, J. C. (2004). *La prueba electrónica*. Bogotá: Temis. 2004.

Rincón, E. e Ibáñez. (2009). El acto administrativo electrónico y Las nuevas tecnologías de la información. *Temas Jurídicos*. Bogotá: Universidad Sergio Arboleda, No. 7, enero-junio de 2009, páginas 1-36.

Rueda, A., Cano, J J. (2006). *Valoración de la evidencia digital*. Bogotá: Universidad de los Andes. Facultad de Derecho.