«La verdadera ignorancia no es la ausencia de conocimientos, sino el hecho de rehusarse a adquirirlos» (Karl Popper)

Evidencia Digital: contexto, situación e implicaciones nacionales

José Alejandro Mosquera González[1]
Andrés Felipe Certain Jaramillo[2]
Jeimy J. Cano[3]

RESUMEN

El siguiente escrito tiene como objetivo hacer un análisis de la situación jurídica nacional de la evidencia digital. Por lo tanto, determinar si este tipo de prueba puede ser admitida dentro de nuestro ordenamiento y de serlo así bajo que modalidad se presentaría. Lo anterior nos llevaría inevitablemente a analizar los efectos y las consecuencias de la admisibilidad o no de la evidencia digital y bajo qué modalidad o tipo de prueba esta sería viable. Se analizarán entonces no sólo los códigos de procedimiento sino que se intentará hacer un análisis de la legislación nacional y los pronunciamientos judiciales más relevantes del tema. Del estudio de compatibilidad y aplicabilidad de la evidencia digital y nuestro ordenamiento, una conclusión es evidente, es necesario adoptar un estándar para el manejo de la evidencia digital.

Palabras claves : Evidencia digital, Estándar, equivalencia funcional, autenticidad, requisitos probatorios

ABSTRACT

The following article will analyze the compatibility and applicability of digital evidence within the set of Colombian laws, codes and regulations. We will try to establish if this type of evidence can be admitted as such in our legal system, and if so under what conditions and characteristics. Conclusion on the effects and consequences of the type of admittance under which the digital evidence would be incorporated will also be drawn based on the national laws and jurisprudence. One of such conclusion would be the necessity of adopting and incorporating a standard on managing digital evidence with the objective of having a clear set of legally binding rules and procedures that allow digital evidence to be presented in a court of law or any legal procedure.

Digital Evidence, Standard, functional equivalent, authenticity, evidentiary requisites

---

1 Abogado de la Universidad de los Andes, Abogado Junior, Mosquera y Helo Abogados Ltda. Correo electrónico: jamosquera@mosquerayhelo.com

2 Abogado de la Universidad de los Andes, Correo electrónico: andrescertain@hotmail.com

3 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

Introducción

Para lograr dar una primera aproximación a la situación y estado actual de la evidencia digital y su relación con el ordenamiento jurídico Colombiano, es necesario explicar el porque consideramos como necesario investigar este tema. La importancia y la respuesta a esto se desarrollaran en la introducción de este trabajo. Luego definiremos el concepto de evidencia digital y la equivalencia funcional para después si hacer un análisis de los requisitos probatorios que deben tener todas las pruebas en nuestro ordenamiento, que tipo o medio de prueba sería la evidencia digital, como se valoraría, sus retos y las implicaciones de la misma.

Estamos ya viviendo en lo que muchos consideran como una "aldea global" donde las mejoras en transportes y los avances en las comunicaciones han ayudado a crear una idea de micromundo donde las distancias y las diferencias dejan de existir. Concretada la aldea global, debe reflexionarse sobre lo que ocurre, en términos institucionales, cuando a la vida del hombre entra un nuevo elemento clave a la hora de regular y establecer las relaciones entre gobiernos y la relación que tiene con otros ciudadanos: la tecnología.

Lo anterior tiene efectos tanto positivos como negativos, es innegable que nuestras comunicaciones, nuestra productividad y en general nuestras vidas han mejorado con la tecnología, pero con esta también llegan problemas de crímenes y controversias legales. La existencia del Internet (una red informática mundial abierta a todos), sobrepasa evidentemente la idea del estado moderno para proyectarse hacia algo evidentemente internacional o supranacional, pero con la novedad de que esta al alcance del individuo y no únicamente de los estados.

El dominio indiscutido del Estado sobre las comunicaciones, se ha visto comprometido por el Internet, la red con capacidad de proporcionar todo tipo de comunicaciones a través de un único medio de fácil acceso y relativamente económico. Las dificultades para determinar conceptos como nacionalidad, jurisdicción, domicilio, ley aplicable etc. hasta ahora utilizados en las políticas legislativas se han intensificado, hoy estos conceptos ya son barreras disueltas por una tecnología que permite el acceso virtual, el control de los negocios a distancia, el intercambio de voluntades vía comunicaciones no tradicionales y en fin el hecho que pasamos de una mundo de papel a un mundo de documentos digitales.

---

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.criptored.upm.es) y de la Comunidad Internacional de Derecho Informático, ALFA-REDI (http://www.alfa-redi.org). Correo electrónico: jcano@uniandes.edu.co

Es así como el hombre del siglo 21 vive en un mundo global, en este nuevo mundo el hombre y su relación con este primero ha evolucionado dramáticamente en un sin número de aspectos. Las distancias y las barreras de comunicación se han reducido significativamente, con la ayuda de los computadores somos capaces de resolver procesos matemáticos que antes eran inconcebibles, con el Internet se ha logrado una "democratización" de la información y la ha hecho más accesible a todos, en fin las nuevas tecnologías han simplificado nuestras vidas al convertirnos en seres más eficientes pero a su vez más dependientes en los sistemas y la tecnología misma. Con la llegada de las nuevas tecnologías el hombre se ha visto en la necesidad de adaptarse a estos nuevos cambios, y la dependencia que se ha creado entre el hombre y la tecnología es tal que inclusive podríamos afirmar que hoy son inseparables e intrínsecos. Es así como según autores como el profesor Nicholas Negroponte, Director del laboratorio de medios del MIT, hoy vivimos una verdadera interfaz, donde el hombre y los bits se encuentran, se fusionan y se convierten en uno, conformando una verdadera "Vida Digital". Esta nueva dependencia y necesidad de los hombres en la tecnología ha llevado a que esta haya "invadido" todas nuestras esferas: el trabajo, el estudio, e inclusive nuestra vida personal y familiar. Lo anterior ha llevado a que el hombre del siglo XXI sea considerado el hombre de la era digital ya que muchos de los aspectos de nuestras vidas se han "digitalizado".

Con esta nueva relevancia e importancia que han asumido las tecnologías en nuestras vidas, ha llegado así mismo la preocupación porque estas sean confiables y fiables ya que hacen parte integral de nuestras vidas. Esta preocupación se ha manifestado en dos grandes aspectos uno sistemático y otro jurídico. En el aspecto sistemático se resuelven problemas relacionados con los protocolos de seguridad, la inviolabilidad de los sistemas etc. En el aspecto jurídico, nos preocupamos esencialmente por el valor probatorio de estas nuevas tecnologías y sus productos y sobre la admisibilidad de estas dentro de un proceso judicial. En últimas, en este aspecto jurídico nos concentramos en analizar la evidencia digital, su valor probatorio y su admisibilidad procesal, teniendo en cuenta por supuesto los aspectos sistemáticos analizados por el primer aspecto ya mencionado, como una estrategia adicional para avanzar en la construcción de la seguridad jurídica en Internet.

Esta nueva "Era Digital" ya afecta y afectará mucho más la vida humana en todos sus aspectos: la vida institucional, la economía, la cultura, la información, el entretenimiento etc. Todo estará digitalizado: desde los actos más mínimos hasta los más trascendentes del hombre como su el registro de su nacimiento, su estado civil, sus propiedades, sus transacciones, su salud, el ejercicio de sus derechos civiles y democráticos entre otras. Este nuevo mundo digital será así mismo un mundo de documentos que no sólo tomarán relevancia en esta nueva concepción sino que a su vez serán el eje central del mismo.

La llegada de este nuevo fenómeno tendrá incidencias en el aspecto político se presentara un fenómeno de ciudadanía electrónica que transformara el concepto de ciudadano a netdano (citiezen-netizen), cambios en el concepto del mercado: de lugares a redes, cambios en la banca: sistemas de pagos y/o transacciones electrónicas, las comunicaciones, los derechos intelectuales, los derechos del consumidor, la privacidad: derecho a la intimidad, entre otros. Sin embargo es de resaltar que todos los cambios en las áreas antes mencionadas comparten un elemento esencial en común: un problema probatorio.

Aunque en Colombia estas nuevas transformaciones ya se están manifestando, nuestro ordenamiento no le ha dado todavía un tratamiento adecuado al mismo y con contadas excepciones nuestro país esta atrasado a la hora de legislar sobre aspectos de trascendencia nacional e internacional como la evidencia digital. Destacamos la reciente Ley 906 del 31 de Agosto de 2004 la cual permite reconocer como documento entre otros, a los mensajes de datos y las grabaciones computacionales. Esta ley no define que se entiendo por los anteriores, y tampoco lo hace su decreto reglamentario 2770 de 2004, por lo tanto nos debemos remitir entonces al literal A y siguientes del Artículo 2 de la ley 527 de 1999 que define los mensajes de datos, y propone una definición quizás adecuada para la evidencia digital como tal. El punto es que no se ha promulgado un vínculo directo entre el concepto genérico de evidencia digital y las definiciones legislativas. Tampoco contamos con un procedimiento detallado del manejo a otorgar a estos documentos para que puedan "nacer, tener vida y ser tratados" al interior de un proceso. Este vacío legal permite la aplicación del segundo parágrafo del articulo 175 del Código de Procedimiento Civil el cual reza: "El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejante o según su prudente juicio". Este artículo que le da rienda suelta a la creatividad de los jueces es sin duda alguna, peligroso en cuanto disminuye el nivel de seguridad jurídica en las decisiones y procedimientos de los mismos. Lo anterior no solo afectaría el concepto de seguridad jurídica sino que a su vez afectaría el concepto de igualdad procesal ya que al no estar consagrada la evidencia digital como un medio de prueba en el código de procedimiento entonces el juez podría practicar esta prueba "a su prudente juicio". Es bien sabido que la complejidad técnica propia de la evidencia digital, le dificultaría al juez practicar este tipo de pruebas sin la ayuda de una serie de procedimientos y lineamientos que lo guíen a la hora de hacerlo, ya que el no es un conocedor del aspecto técnico de la evidencia digital y de la problemática de la misma.

Entendida ya la necesidad de contar con mecanismos y herramientas que nos permitan tener claros una serie de de criterios o procedimientos claros y precisos que permitan orientar a los órganos competentes a admitir o no pruebas digitales en los procesos que estos estudian, es necesario tener claro que el objetivo de este escrito es realizar un análisis de la evidencia digital y su compatibilidad con nuestro ordenamiento. Para lograr lo anterior hemos visto como requisito necesario no solo estudiar el tema de la evidencia digital como aspecto esencial de los delitos informáticos sino que a su vez consideramos indispensable ampliar el concepto a todo tipo de delito o investigaciones judiciales (laborales, civiles, administrativas etc.)

¿Qué es la evidencia digital?

Una definición uniforme y universal de este concepto no es fácil de encontrar, sin embargo consideramos acertada la definición que nos ofrece el profesor Cano quien nos manifiesta que la evidencia digital es un tipo de evidencia física. Continúa definiendo a la misma como aquella evidencia que esta construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Encontramos así mismo acertada la definición ofrecida por el estándar norteamericano de "*searching and seizing computers and obtaining electronic evidence in criminal investigations*" quien nos ofrece una definición un poco mas práctica y menos conceptual del mismo, según este estándar la evidencia digital que contiene texto puede ser dividida en 3 categorías:

1. Registros generados por computador.
2. Registros no generados sino simplemente almacenados por o en computadores.
3. Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos.

La diferencia entre las 3 categorías mencionadas radica en el factor humano. Es decir lo determinante es si una persona o un computador crearon o generaron el contenido del registro.

Los registros almacenados en computadores son documentos que contienen escritos o información creada por una persona en forma y formato electrónico, ejemplos de lo anterior son correos electrónicos, documentos generados por procesadores de palabras, etc. Lo esencial en este tipo de registros es demostrar plenamente la identidad del generador, vinculándolo directamente a la creación de los datos. De no ser así, al igual que con cualquier otra prueba testimonial o documental que contenga afirmaciones humanas, la prueba debe cumplir con el "*hearsay rule*". Si la evidencia es admitida para demostrar o probar hechos o afirmaciones contenidas en la evidencia misma, quien propone dicha evidencia (quien pretende hacerla valer) debe demostrar circunstancias que indiquen que las afirmaciones humanas contenidas en la evidencia o registro son fiables y confiables.

Por oposición a lo anterior, se encuentran los registros generados por computadores que contienen el producto de la programación de los mismos, inalterados por el hombre. Aquellos serán, archivos de registro (*log files*), registros telefónicos, registros de transacciones bancarias, informes de datos de SWIFT, donde no hay afirmaciones generados por humanos sino por sistemas o computadores. Lo anterior implica un vuelco en el tema probatorio pues ya no se tratara de demostrar que una afirmación humana por fuera de la corte (sin juramento) sea veraz y acertada sino que el objetivo probatorio será demostrar o comprobar el correcto funcionamiento del programa generador de registro.

En la tercera y última categoría, la mixta o híbrida al combinar tanto afirmaciones humanas como registros producto de programas o computadores, quien pretende hacer valer una prueba típica de esta categoría debe entonces cumplir con los dos requisitos antes mencionados: el *hearsay rule* y lograr demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

Entendiendo entonces que en Colombia no existe una definición clara a nivel legislativo o jurisprudencial del concepto de evidencia digital es claro que existe una necesidad de crear una legislación nueva o la modificación de la ya existente para dar claridad sobre las condiciones requeridas para la admisibilidad de la evidencia digital y la necesidad de establecer una serie de procedimientos de valoración de pruebas digitales que protejan y garanticen los derechos de las partes de un proceso judicial proporcionándole al funcionario herramientas claras para su adecuada valoración. Por tanto, para poder lograr esto es necesario no solo estudiar el contexto normativo y jurisprudencial nacional y su situación actual para rescatar y proponer modificaciones a este, sino también recurrir a la utilización de un estándar para cumplir con los objetivos antes mencionados.

Antecedentes y situación actual

Entendido entonces que es la evidencia digital, es necesario ahora estudiar la situación actual de la misma en Colombia. Comencemos entonces por analizar, ¿Hasta dónde remontan las incursiones legislativas colombianas por velar por aquel anhelado pero tan difícil paralelismo entre la tecnología y la normatividad?

Quizás el primer gran paso legislativo relevante para nuestra investigación se presenta con la promulgación de la Ley 98 del 20 de Diciembre de 1993, también conocida como la Ley del Libro. En dicha ley se realizó una analogía entre las publicaciones en papel (o en materia) con aquellas realizadas por medios electromagnéticos en su artículo segundo al afirmar que: " Para los fines de la presente Ley se consideran libros, revistas, folletos, coleccionables seriados, o publicaciones de carácter científico o cultural, los editados, producidos e impresos en la República de Colombia, de autor nacional o extranjero, en base papel o publicados en medios electro-magnéticos ".

Como siguiente escalón en la tecnificación de la ley nacional, la Ley Estatutaria de la Administración de Justicia en su artículo 95 reza: ¨ Tecnología al servicio de la Administración de Justicia. El Consejo Superior de la Judicatura debe propender por **la incorporación de tecnología de avanzada al servicio de la administración de Justicia**. Ésta noción se enfocará principalmente a mejorar la **práctica de pruebas**, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información. Los juzgados, tribunales y corporaciones judiciales **podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y temáticos, para el cumplimiento de sus funciones**. Demás circulares y decretos han mencionado tangencialmente el tema de manera similar.

Es necesario mencionar el Decreto 2150 de 1995, - por medio del cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios, existentes en la Administración Pública -, dispuso en su artículo 26, que las entidades de la Administración Pública deberían habilitar sistemas de transmisión electrónica de datos para que los usuarios enviaran o recibieran información requerida en sus actuaciones frente a la administración y que en ningún caso las entidades públicas podrían limitar el uso de tecnologías para el archivo documental por parte de los particulares, sin perjuicio de sus estándares tecnológicos. Recordemos la Ley 527 de 1999 como elemento interesante en el tema de los documentos electrónicos que son considerados como pruebas. En esta ley en su artículo 37 se establecen como documentos equivalentes a la factura, el documento conocido como la factura electrónica La Factura Electrónica es la representación informática de un documento tributario generado electrónicamente, que reemplaza al documento físico en papel, pero con idéntico valor legal a éste.

Así mismo, el concepto de factura electrónica es definido por el decreto 1094 de 1996 al establecer que se debe entender "por factura electrónica el documento computacional que soporta una transacción de venta de bienes o. prestación de servicios, transferido bajo un lenguaje estándar universal denominado Edifact de un computador a otro", se establece además que todos los equipos de computación, comunicaciones, almacenamiento y software utilizados para administrar la red de valor agregado y sus buzones electrónicos deben estar en Colombia. Los conceptos antes mencionados son desarrollados y reafirmados nuevamente por el decreto 1165 de 1996, quien reglamenta las aplicaciones y requisitos de la factura electrónica. Es importante mencionar que estas 3 disposiciones son las primeras disposiciones legales que le otorgan a un documento electrónico específico, como lo es la factura electrónica un valor probatorio importante pues le otorgan al documento electrónico la facultad de ser prueba para efectos tributarios.

Respecto a los avances legales ya mencionados, en estos momentos, el Ministerio de Comercio adelante un proyecto sobre el Documento Tributario Electrónico

(DTE), la factura electrónica, la nota de crédito electrónica y la nota de débito electrónica que soportan una transacción de venta de bienes o prestación de servicios, transferidos de un dispositivo electrónico a otro bajo un lenguaje estándar XML adoptado por el gobierno nacional según recomendación que emita para el efecto el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Así mismo es importante mencionar que el ICONTEC adelantará un proceso de normalización del estándar técnico XML adecuado para que los DTEs tengan un soporte tecnológico que permita mantener la originalidad, integridad, no repudiación y seguridad de los mensajes de datos. El estándar deberá incluir la posibilidad de presentar y transmitir el DTE por medios electrónicos a usuarios finales. Es así como el gobierno nacional fijará el estándar dentro de los tres meses siguientes a la fecha de la recomendación de ICONTEC y ordenará al mismo Instituto la revisión de los estándares cada tres años. Tal revisión podrá incluir la adopción de un lenguaje estándar distinto al XML si se considera adecuado a la evolución tecnológica. En el mismo proyecto se establece que de cumplir los DTEs con el estándar del ICONTEC este tendrá el mismo valor para todos los efectos legales que la factura en papel.

El reconocimiento de la necesidad de un estándar en este tema, es un paso importante en el desarrollo de conceptos de estandarización de los temas relacionados con los documentos electrónicos y por tanto en el tema de la evidencia digital. Este proyecto claramente sigue la tendencia internacional en los temas de los documentos electrónicos y por tanto es un proyecto clave.

El próximo gran paso de la normatividad colombiana fue la promulgación de la ley 527 de 1999. Esta ley permitió gracias al concepto de la equivalencia funcional equiparar los mensajes de datos a los escritos y por tanto le dio a los mismos la posibilidad de convertirse en pruebas judiciales. Es necesario ahora explicar brevemente el concepto de equivalencia funcional ya que este ha permitido al legislador equiparar conceptos antiguos y en desuso por sus equivalentes modernos, logrando así con la utilización de este concepto modernizar y actualizar las leyes y disposiciones de nuestro ordenamiento jurídico.

Por equivalencia funcional, se entiende la aplicación del sistema jurídico y sus disposiciones a un estadio diferente que por estar encaminado y cobijado por los mismos principios debe gozar de una extrapolación de los mecanismos y dispositivos jurídicos existentes aunque en el momento de la creación de éstos no se hayan consentido la existencia de aquellos. Más adelante se discutirá en jurisprudencia de la Corte Suprema el anterior planteamiento.

Según la ya mencionada 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, cumplidos ciertos requisitos, los mensajes de datos, los mensajes de datos y demás se entienden como escritos y originales y además 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.

Lo anterior de acuerdo al siguiente articulado de la Ley:

"**Artículo 10**. *Admisibilidad y fuerza probatoria de los mensajes de datos.*

Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

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".

Si bien lo anterior es un gran paso, no está orientada la ley a la evidencia digital como tal, sin embargo debemos entender su bagaje de creación histórico, al comprender que dicha ley fue una respuesta más a una necesidad mercantil global que a una preocupación jurídica por actualizar el derecho probatorio.

La Ley 527 de 1999, sigue los lineamientos del proyecto tipo de Ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional -CNUDMI y la intención de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil fue la de promover la gestación de un proyecto de ley tipo en materia de comercio electrónico, inspirada en la convicción de que al dotársele de fundamento y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros, repercutiendo así necesariamente en la expansión del comercio internacional ya que trae consigo ventajas comparativas por su velocidad y acercamiento de las relaciones entre comerciantes y usuarios de bienes y servicios.

En 1996 La Asamblea General de la ONU mediante Resolución 51/162 aprueba la Ley Modelo sobre Comercio Electrónico elaborada por la CNUDMI y recomienda su incorporación en los ordenamientos internos como un instrumento útil para agilizar las relaciones jurídicas entre particulares.

En Colombia según sentencia C-662 de 2000 del Magistrado Fabio Morón Díaz se surtió dicha implementación así, comienza como un estudio de temas de derecho mercantil internacional en el seno de una Comisión Redactora de la que formaron parte tanto el sector privado como el público liderado por el Ministerio de Justicia y con la participación de los Ministerios de Comercio Exterior, Transporte y Desarrollo para concluir con la ya mencionada ley 527. La justificación según la misma sentencia:

> "Obedece a la necesidad de que existiese en la legislación colombiana un régimen jurídico consonante con las nuevas realidades en que se desarrollan las comunicaciones y el comercio, de modo que las herramientas jurídicas y técnicas dieran un fundamento sólido y seguro a las relaciones y transacciones que se llevan a cabo por vía electrónica y telemática, al hacer confiable, seguro y válido el intercambio electrónico de informaciones."

Así, pues, gracias a la Ley 527 de 1999, Colombia se pone a tono con las modernas tendencias del derecho internacional privado, una de cuyas principales manifestaciones ha sido la adopción de legislaciones que llenen los vacíos normativos que dificultan el uso de los medios de comunicación modernos, pues, ciertamente la falta de un régimen específico que avale y regule el intercambio electrónico de informaciones y otros medios conexos de comunicación de datos, origina incertidumbre y dudas sobre la validez jurídica de la información cuyo soporte es informático, a diferencia del soporte documental que es el tradicional.

De ahí que la Ley facilite el uso del EDI y de medios conexos de comunicación de datos y concede igual trato a los usuarios de documentación con soporte de papel y a los usuarios de información con soporte informático.

La Corte Constitucional respalda la normatividad y muy tempranamente aplica sus disposiciones en sus providencias, así por ejemplo es como el Magistrado Vladimiro Naranjo Mesa en sentencia C-562 de 2000 refiriéndose a la viabilidad de reconocer una información allegada a sedes administrativas y judiciales en forma de mensaje de datos, precisó:

> *"No cuestiona la Corte el hecho de que el documento contentivo de la presente acusación haya sido enviado por telefax a la sede de la Corporación, pues entiende que, gracias a los avances tecnológicos que se han presentado en el campo de las comunicaciones, al orden jurídico interno se han venido incorporando algunas preceptivas que, amparadas también en los principios de eficacia, economía, celeridad y primacía de lo sustancial, le otorgan plena validez a ciertos actos procesales que se realizan bajo esa modalidad de mensaje de datos. Recientemente, se expidió la Ley 527 de 1999, por medio de la cual se define y reglamenta -entre otros- el acceso y uso de los mensajes de datos, en cuyo artículo 10° se le reconoce "fuerza obligatoria y probatoria" a toda información que se allegue a las actuaciones administrativas y judiciales "en forma de un mensaje de datos".*

Podemos concluir entonces, que la situación legislativa y jurisprudencial en Colombia si bien es importante, es así mismo insuficiente a la hora de resolver todas las dudas con respecto al tema de la evidencia digital. Es necesario resaltar como un gran salto que la Ley 906 del 31 de agosto de 2004 y el Decreto 2770 de 2004 introdujeron y reglamentaron el sistema acusatorio adversarial en Colombia. Allí se mencionan en el Art. 424, numerales 6) y 7) la grabación computacional y el mensaje de datos como documentos y que por lo tanto serian estas pruebas documentales. Así mismo en el Art. 426 sobre métodos de autenticación e identificación de documentos, se menciona en el numeral 3 los certificados digitales emitidos por entidades de certificación como instrumentos que permiten lograr dicho fin. En el tema de la autentificación de los documentos la misma ley en su artículo 425. establece que "Salvo prueba en contrario, se tendrá como auténtico el documento cuando se tiene conocimiento cierto sobre la persona que lo ha elaborado, manuscrito, mecanografiado, impreso, firmado o producido por algún otro procedimiento. También lo serán la moneda de curso legal, los sellos y efectos oficiales, los títulos valores, los documentos notariales o judicialmente reconocidos, los documentos o instrumentos públicos, aquellos provenientes del extranjero debidamente apostillados, los de origen privado sometidos al trámite de presentación personal o de simple autenticación, las copias de los certificados de registros públicos, las publicaciones oficiales, las publicaciones periódicas de prensa o revistas especializadas, las etiquetas comerciales, y, finalmente, todo documento de aceptación general en la comunidad."

Se radica entonces el 20 de julio de 2003, el proyecto de ley que intenta la Modificación del Código Penal y del Código de Procedimiento Penal, adecuaciones del estatuto Penal a las exigencias tecnológicas. Se introducen los Delitos contra la seguridad informática y telemática al Código Penal y el artículo 229. Así mismo con la Ley 890 del 07 de julio de 2004 se adicionó al Código Penal, principalmente en el capítulo Noveno, nuevos delitos contra medios de prueba y otras infracciones. *Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes* al Código de Procedimiento Penal. Éste último, introduciendo por primera vez al estatuto un tema de suma importancia, el peritaje técnico-informático. Que si bien no es la materia de investigación del presente escrito, está necesariamente ligado a la evidencia digital, y será únicamente con la ayuda de esta herramienta que se logrará avanzar en el tema y lograr su correcta y completa implementación a nuestro aparato judicial.

Es claro entonces que, la ley 527 de 1999 y la Ley 906 del 31 de agosto de 2004 fueron los últimos grandes y verdaderos aportes legislativos al tema de derecho probatorio y tecnología y si bien con estas leyes se logró un gran avance aún no es claro como la evidencia digital debe ser allegada a un proceso ni como se deberán cumplir los requisitos para que esta sea considerada auténtica, ya que como se mencionó la ley 527 tiene como fundamento razones mercantiles y no de actualizaciones al derecho probatorio y si bien la ley 906 permite admitir ciertos conceptos de la evidencia digital como documentos todavía el procedimiento para su incorporación y valoración en un proceso judicial no son claros. Siendo lo anterior cierto, es claro entonces que careciendo la anterior ley de la certitud necesaria para resolver nuestro objetivo de investigación, es necesario recurrir a las disposiciones de derecho probatorio propiamente dichas para así hacer un estudio de los requisitos legales para la aceptación e incorporación y las modalidades de presentación de las pruebas. Veamos entonces primero cuales son los criterios de admisibilidad de la evidencia digital de manera general para después si entrar en detalle con los requisitos probatorios legales propiamente dichos.

Criterios de admisibiliad de la evidencia digital

El profesor J. Cano basándose en autores como Sommer, y Casey entre otros nos recuerda que en las legislaciones modernas son 4 los criterios que se deben tener en cuenta y analizar al momento de decidir sobre la admisibilidad de la evidencia: la admisibilidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial.

Analicemos entonces cada uno de estos conceptos y su relación con nuestro tema de investigación.

Autenticidad

A continuación ofrecemos una definición doctrinal del concepto, con fines meramente académicos, puesto que más adelante discutiremos el concepto concebido dentro de la legislación que si bien mantiene una estrecha similitud, proporcionará contextualizaciones jurídicas relevantes.

Este aspecto nos obliga a afirmar que una evidencia digital será autentica siempre y cuando se cumplan dos elementos. El primero que dicha evidencia haya sido generada y registrada en el lugar de los hechos y la segunda que muestre “la no alterabilidad de los medios originales” es decir que la los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma. En cuanto a la autenticidad de los documentos la legislación colombiana en el artículo 11 de la ley 446 de 1998 preceptúa que “Autenticidad de documentos. En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados de terceros.”

Nos apartamos respetuosamente del concepto del Dr. Cano quien considera que el artículo antes mencionado solo aplica para documentos y medios no digitales. La razón que sustenta nuestro distanciamiento es que el concepto de documento como lo entiende el Código de Procedimiento Civil en sus artículos 10 y 11 y la doctrina colombiana, sumados y leídos bajo el concepto de equivalencia funcional nos permiten concluir que la evidencia digital es un tipo de documento. Entendido lo anterior concluimos entonces que la presunción de autenticidad establecida por el artículo 11 de la ley 446 de 1998 aplicaría para los documentos electrónicos y por lo tanto para la evidencia digital como una presunción de hecho. Sin embargo dicha presunción podría encontrarse limitada si tenemos en cuenta que elementos importantes para determinar la autenticidad de la prueba como las características de su creación, procesamiento, almacenamiento, recuperación y eliminación pueden adquirir una relevancia fundamental dentro de un proceso judicial a la hora de determinar la autenticidad de una prueba judicial, como requisito para que ésta sea aceptada.

Confiabilidad

Entendemos que la evidencia digital es confiable cuando «viene de fuentes que son creíbles y verificables" En un contexto digital el concepto de confiabilidad se podría equiparar al hecho de contar con una arquitectura de computación en correcto funcionamiento, pues solo cuando los sistemas funcionen de manera adecuada las pruebas productos de estas podrán ser consideradas como confiables. Es decir una prueba digital seria confiable siempre y cuando el sistema que la haya producido no haya sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba. Para lograr el adecuado funcionamiento de la arquitectura de computación del sistema que genera o almacena la evidencia digital, es necesario que esta cuente con una función que sincronice el registro de las acciones de los usurarios y que a su vez cuente con un registro centralizado e íntegro de los mismos.

Suficiencia

Este concepto esta íntimamente relacionado con el anterior en la medida en que se entenderá que una prueba es suficiente si esta es completa. Para asegurarnos que una prueba es completa es necesario contar con mecanismos de integridad, sincronización y centralización que permitan observar una imagen completa de la situación objeto de análisis. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos "definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos para establecer y conocer eventos ocurridos en una arquitectura o procesos"

Apego y respeto por las leyes y reglas del poder judicial.

Este último concepto nos lleva a concluir que toda evidencia digital debe cumplir con las características y requisitos enunciados en nuestros códigos de procedimiento y el resto de las disposiciones legales de nuestro ordenamiento. Así las cosas, es claro que cualquiera prueba digital que se pretenda valer en un proceso no solo deberá ser auténtica, confiable y suficiente sino que debe respetar toda la normatividad legal vigente en nuestro sistema jurídico. Una prueba que cumpla con los tres primeros requisitos mencionados sin la observancia de este último concepto llevaría a la inevitable conclusión que dicha prueba no puede ser admitida dentro de un proceso judicial por ser esta ilegal. Miremos entonces cuales son estas leyes y reglas del poder judicial mas de cerca, es decir cuales son los requisitos legales para que una evidencia pueda ser considerada como prueba dentro de un proceso.

Requisitos probatorios. ¿Qué requisitos deben cumplirse en la legislación actual para que exista una prueba?

El artículo 178 del Código de Procedimiento Civil y el artículo 235 del Código de Procedimiento Penal contienen los requisitos que verificará el funcionario para considerar una prueba como tal. A saber: conducente, pertinente, y útil.

"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"

Del primer enunciado del artículo entiende la doctrina que el legislador quiere decir que las pruebas han de ser conducentes. Lo anterior implica que se debe utilizar el medio de prueba adecuado, entendiendo por este aquel que sea legal y a su vez eficiente, es decir el medio idóneo para demostrar los hechos que pretenden hacerse valer. Ejemplo de lo anterior seria que antes que mostrar un video del parto de un menor para pretender demostrar que es hijo de alguna persona en particular es necesario presentar el registro civil de la persona, ya que en Colombia es este último documento el adecuado para demostrar el hecho pretendido.

Las pruebas, deberán así mismo, estar referidas al objeto del proceso y versar sobre los hechos que involucren el debate, puesto que de no tener relación con el *thema probandu*, serán impertinentes. Luego entonces se habla dentro del sistema que podrán existir pruebas conducentes que a su vez sean impertinentes. Lo anterior ocurriría cuando si bien una prueba no siendo ilegal ni requiriendo la ley un medio de prueba específico, nada aporte al objeto de la litis. Finalmente la utilidad por oposición a una prueba superflua, será aquella que aumente el nivel de certeza en el juez y le permita así aumentar su nivel de convencimiento.

Además de los requisitos antes mencionados la doctrina y la legislación han considerado que las pruebas también deben ser allegadas oportunamente (en todo proceso judicial existe una etapa propia para allegar, solicitar y practicar pruebas) y según el artículo 238 del Código de Procedimiento Penal estas deben ser apreciadas en conjunto con las demás pruebas allegadas al proceso y de acuerdo con las reglas de la sana crítica.

Es claro entonces que para que una prueba digital sea admitida dentro de un proceso esta deberá contar con los requisitos antes mencionados. No vemos problema alguno en que la evidencia digital cumpla con los requisitos antes mencionados, ya que ninguna de sus particularidades técnicas le impide cumplir con los requisitos antes mencionados. Cumplidos estos requisitos es necesario determinar, que si bien la evidencia digital puede ser una prueba, que tipo o medio de prueba sería. Este punto quedó resuelto con la llegada de la ley 906 de 2004 el cual permite concluir que la evidencia digital será considerada como prueba documentaria. Sin embargo es importante determinar si la evidencia digital será considerada como un documento privado o publico.

Documentos privados y públicos

Ahora bien, establecido lo anterior es necesario distinguir entre dos tipos de documentos, los privados y los públicos. Se entiende por documento público según el artículo ya mencionado "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 instrumento 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 público." Es de resaltar que el valor probatorio de un documento privado auténtico es del mismo valor que los públicos no sólo entre quienes lo suscribieron o crearon sino con respecto de terceros. Clasificación importante a tener en cuenta con anterioridad al artículo 83 de la Carta Política de 1991 ya que ésta disposición eleva el carácter de la valoración del funcionario hasta la presunción de buena fe de los documentos públicos a todo tipo de documentos.

Así las cosas, cuando estemos frente a un documento privado su validez dependerá principalmente de la autenticidad del documento. Dejamos abierto el tema del requisito de autenticidad que será tratado con mayor rigurosidad mas adelante.

La evidencia digital como prueba documentaria

Establecido entonces que la evidencia digital seria considerada como una prueba y que la modalidad o medio bajo el cual se presentaría, seria el documento en términos del artículo 175 del CPC, es necesario ahora determinar puntualmente cuales serían las condiciones o requisitos especiales que debería cumplir toda evidencia digital para ser considerada y aceptada como una prueba dentro de un proceso.

a) Condiciones de admisibilidad del documento electrónico

Según Mariliana Rico Carrillo en su escrito la función procesal probatoria del documento electrónico, en realidad existen varios requisitos para que un documento electrónico sea admitido como prueba sin embargo la mayoría están en caminados a demostrar la veracidad y la autenticidad de los mismos.

El primero sería el requisito de demostrar la calidad y el correcto funcionamiento de los sistemas utilizados para la elaboración y almacenamiento de los mismos. Otro iría encaminado a corroborar la veracidad de la información suministrada por el documento electrónico. En este sentido el contenido del mensaje enviado por el autor y aquel recibido por el destinatario deben ser idénticos y exactos. Este requisito esta obviamente relacionado con el primero en la medida en que solo si el sistema esta funcionando adecuadamente y no ha sido violado podrá cumplir con el requisito de integridad del mensaje exigida por el artículo 8 de la ley 527 de 1999.

Un tercer requisito para la admisibilidad del documento electrónico es la conservación y la posibilidad de recuperación del mismo. Este requisito nos obliga entonces a estudiar la integridad del documento electrónico, es decir que tan posible es que este haya sido deteriorado, manipulado o alterado en ultimas se estudia la vulnerabilidad del documento y del sistema que lo creo. Este requisito es el que nos permite según la ley de mensajes de datos y firmas electrónicas satisfacer el requisito legal que la información conste por escrito cuando la información que contiene un mensaje de datos es susceptible de ser consultada posteriormente. Así mismo, es necesario que el mensaje debe conservarse en su formato original o de no estarlo, en un formato que permita corroborar que aquello que este mensaje reproduce es exacto a la información generada, enviada o recibida.

Otro requisito para lograr la admisibilidad de los documentos en cuestión es la posibilidad de la individualización o identificación de los sujetos que participaron en la creación, envió, recepción y modificación del mismo. Así mismo es necesario establecer el rol que cada uno de ellos jugó en la creación y modificación del mismo. Es de resaltar que dicho documento debe ser también legible para el hombre lo que implica la utilización de sistemas o programas que "traduzcan" el lenguaje binario o el código del mensaje a un lenguaje alfanumérico para que este pueda ser leído, comprendido y analizado por las partes en el proceso.

Una vez que el documento electrónico haya cumplido con los requisitos antes mencionados y por supuesto con aquellos exigidos por la normatividad competente es necesario determinar como se va a allegar dicha prueba al proceso judicial.

b) ¿Cómo y bajo qué modalidad se allega la evidencia digital?

En países como España la modalidad bajo las cuales se deben presentar estas pruebas, ya no es un misterio sin embargo no contamos en nuestro país con una disposición parecida, lo cual hace necesario adelantar un estudio y análisis detallado. Para lograr esto es necesario recurrir no solo a la normatividad relativa a este punto sino que ésta debe ser leída y analizada teniendo en cuenta el concepto de equivalencia funcional. Así las cosas, según la ley 527 de 1999 y el análisis doctrinal y legal del código de procedimiento civil junto con el concepto de equivalencia funcional, es claro que este tipo de pruebas, deben presentarse bajo el concepto de prueba documental. Sin embargo, dado las características técnicas y especiales de este tipo de prueba es probable que dada su complejidad sea necesario así mismo apoyarse en peritajes o una inspección judicial según sea el caso.

Será necesario un peritaje para complementar o apoyar la prueba documental para determinar la autenticidad de la prueba, cuando se tache su autenticidad o para determinar elementos claves del mismo como su fecha de emisión o recepción si el mensaje fue abierto, para descifrar el documento, comprobar firmas electrónicas etc. Así mismo, podría ser necesaria una inspección judicial para determinar la calidad de los sistemas informáticos que hicieron parte en la creación del documento. Por medio de esta herramienta el juez puede ponerse en contacto directo con las condiciones y garantías en que se encuentra un documento o la fiabilidad de su contenido con la ayuda de un perito experto en el tema.

c) ¿En qué momento se debe presentar la evidencia digital?

Analizado el tipo de medio de prueba bajo el cual se debe presentar la evidencia digital es necesario ahora establecer en que momento o etapa procesal esta debe ser presentada. Así las cosas, si la prueba que se pretende hacer valer es el fundamento de la pretensión principal dentro de un proceso es claro que entonces este debe incorporada al momento de la presentación de la demanda o de la contestación de la misma según sea el caso. La anterior regla general encuentra ciertas excepciones legales establecidas por el código de procedimiento o de las demás normas procesales quienes en ciertas circunstancias permiten la incorporación posterior (por fuera del tiempo o etapa probatoria) sobre la base de causas determinadas. Las oportunidades probatorias están claramente definidas por nuestro código de procedimiento civil en su artículo 183 y demás legislación relevante en otras jurisdicciones, estas normas deberán ser respetadas a la hora de presentar evidencias digitales dentro de un proceso. Es claro así mismo, que aun si la parte no promueve la evidencia si el juez del proceso conoce de la existencia de la misma este pude de solicitar de oficio que esta sea decretada, siempre y cuando "las considere útiles para la verificación de los hechos relacionados con las alegaciones de las partes"

d) ¿En qué medio o soporte debe presentarse la evidencia digital?

En cuanto al medio o el soporte en el que se debe presentar la evidencia digital si bien es cierto en ocasiones puede ser más fácil presentarlo en su medio electrónico (disquete, CD ROM, disco duro etc.), no consideramos como lo hace la profesora Rico Carrillo que este debe modalidad debe ser exclusiva. El anterior distanciamiento encuentra su sustento en que, si bien es cierto, la forma impresa de una evidencia digital representa ciertos desafíos a la hora de demostrar su autenticidad, su integridad y completitud esta también puede ser una modalidad de soporte válido. Con esta posición nos alejamos del criterio cronológico de la teoría de diferenciación entre original y copia y nos acercamos más al concepto de inalterabilidad para catalogar un documento como original. Según el primer criterio, el cronológico, el documento original es el que primero en el tiempo se ha generado y los demás serán copias de este, para lograr establecer el factor cronológico se utilizan funciones de sellado temporal que permiten identificar el momento, lugar, hora y fecha de creación, emisión y/o envió de un documento. Sin embargo la teoría de la inalterabilidad parte del supuesto que puede existir más de un "original" de un documento. Siendo lo anterior cierto, para esta teoría lo que determinará si un documento es original o no será si este es una fiel copia del documento maestro es decir que no ha sido alterado, en cuyo caso será este considerado también como original. La teoría antes mencionada encuentra mayor peso si se tiene en cuenta que la ley 527 de 1999 en su artículo 8 establece que el requisito de "original" de un documento quedara satisfecho cuando se garantice que este ha conservado la integridad de la información a partir del momento en que se generó por primera vez. Similar solución se ha encontrado en México, Estados Unidos, Venezuela y España, en este último según el profesor Illescas Ortiz serían 3 los requisitos para considerar como original un documento: "1. La conservación integra y sin alteración desde el momento inicial del documento, de modo permanente y constante. 2. La aptitud del mensaje para ser presentado o exhibido ante terceros (exhibición que podrá ser efectuada por medios electrónicos o mediante la impresión del documento en soporte de papel). 3. La recuperación del mensaje, que implica que sea accesible para su ulterior consulta". Es claro entonces que en esta teoría de la inalterabilidad la distinción entre original y copia se eliminaría para así hablar de una versión fidedigna e inalterada del documento.

e) La cadena de custodia

Así mismo, consideramos necesario mencionar, como elemento complementario para aumentar la protección de la evidencia el concepto de la cadena de custodia. Si bien es un procedimiento consignado en el Código de Procedimiento Penal en los artículos 244, 257, 288 y 289, es una buena práctica organizacional en el momento de contar con evidencia digital de un hecho catalogado como fraudulento o criminal. Es necesario mencionar que este concepto cobra especial relevancia cuando una inspección judicial se hace necesaria. Cuando una inspección sea realizada los elementos probatorios recaudados se recogerán y conservaran conforme a los procedimientos de la 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. Las personas antes mencionadas deben dejar una constancia escrita que cumpla con los requisitos establecidos por el artículo 289 del Código de Procedimiento Penal. Así mismo es importante mencionar que está en cabeza del Fiscal General de la Nación reglamentar lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, conforme con los avances científicos y técnicos como lo es el objeto de estudio de esta investigación.

Valoración de la evidencia digital

Incorporada ya la evidencia digital en un proceso judicial es necesario establecer cuales serán los criterios para valorar y analizar dicha prueba. Es claro según nuestro código de procedimiento civil que "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." Así mismo el artículo 11 de la ley 527 de 1999 establece que: "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."

Siendo esto así sería claro que el juez debe valorar y analizar las pruebas según las reglas de la sana crítica, sin embargo debido a la complejidad técnica hay ciertos aspectos que el juez también debe valorar. Algunos de estos aspectos son "la fiabilidad del sistema utilizado para generarlo, la fiabilidad de la forma de conservación, la integridad del mensaje, la identificación de su iniciador..." entre otros. Para la valoración de la evidencia digital existen factores importantes que debe considerar el juez al momento de fallar, entre estos elementos están el momento de creación del documento, la autenticidad del mismo entre otros.

Momento de creación de los documentos

En cuanto al momento de creación o la fecha de los documentos, en el documento público la fecha será la que figure en él y quien no este de acuerdo con la misma deberá tacharlo de falso y demostrar su falsedad. La fecha en el documento privado auténtico será, al igual que en el público, la que figure en él entre las partes, pero si el documento se quiere hacer valer frente a un tercero será la fecha de la autenticación. Es de resaltar que si las fechas del documento y de la autenticación no son las mismas el tercero queda facultado para escoger a cual de las dos fechas atenerse.

El anterior tema merece una reflexión en cuanto a los documentos electrónicos como evidencia digital que se pretenda ser admitida dentro de un proceso judicial. Según el estándar australiano, las fechas de las creaciones y de las certificaciones de dichos documentos estarían dadas por el sistema de computadores y por sellos de tiempo y fecha que el mismo sistema adjuntaría a los registros electrónicos. El anterior procedimiento podría seguir el formato tanto del RFC 3339-*Date And Time On The Internet: Timestamps* como el propuesto en el ISO/IEC 18014-*Time-stamping Services*. Así mismo para asegurar que los sellos antes mencionados sean precisos y fieles los organismos estatales, los entes certificadores y en general todas las compañías deberían cerciorarse que todos los relojes de sus sistemas de computadores estén sincronizados con una referencia central que puede ser el Universal Time Coordinated Clock o la hora Zulu como también se le conoce.

Autenticidad

Los documentos y por lo tanto la evidencia digital que se pretendan hacer valer como pruebas dentro de un proceso deben ser auténticos. Nos define el código de procedimiento civil en su Art. 252.- Modificado por la ley 794 de 2003 (art. 26). que "es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado". Sin embargo los documentos y por lo tanto la evidencia digital cuentan, gracias al noble propósito de descongestionar los despachos judiciales que inspiró a la ley 446 de 1998 en su artículo 11 y el mismo artículo 252 ya mencionado, con una presunción de autenticidad de los documentos cuando estos provienen de las partes. También será autentico según el mismo artículo 252 "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", lo anterior "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". Del anterior artículo, sin embargo, nace la siguiente interrogante: ¿al establecer como auténticos los documentos elaborados, manuscritos o firmados implica esto que sólo serán presumidos como auténticos aquellos documentos que contengan la firma de su autor? En otros términos ¿la presunción establecida en el artículo ya mencionado es para todos los documentos digitales o solo para aquellos que hayan sido firmados digitalmente? Es la opinión de la Corte Suprema de Justicia en sentencia proferida por la Sala de Casación Civil del 4 de septiembre de 2000 con ponencia del Dr. Carlos Ignacio Jaramillo que "es indispensable que el documento se encuentre firmado" Así las cosas la autenticidad de los documentos electrónicos dependería principalmente de si cuenta con una firma electrónica que cumpla con las condiciones exigidas para equiparar la firma electrónica con la firma manuscrita. Es de resaltar que dicha sentencia se profirió no con ocasión de un documento electrónico y su firma digital, sino de un documento ordinario y su firma de puño y letra. Sin embargo, por ser el tema objeto de nuestra investigación uno sin incidencias jurisprudenciales relevantes, y basados en los criterios de equivalencias funcionales y por el espíritu impregnado en la ley 527 de 1999 consideramos que dicha sentencia se podría aplicar como respuesta a la pregunta antes planteada.

Nos apartamos nosotros de la decisión y la interpretación hecha por la Corte Suprema en la decisión ya comentada por una serie de razones. Es nuestra opinión que la redacción del artículo es clara en el sentido que ofrece 3 acciones que no deben darse en conjunto sino subsidiariamente. Lo anterior encuentra sustento en que el legislador utilizó el calificativo o determinante "o" lo cual implica que para que opere la presunción basta con que cualquiera de las 3 circunstancias se constaten. Si por el contrario la intención del legislador hubiese sido que la firma fuese un requisito indispensable este hubiese utilizado la palabra "y" para hacerle entender a los jueces y los particulares que dicho elemento era indispensable. Así mismo lo expresa el profesor Hernán Fabio López Blanco "si la ley no distingue, el intérprete no le esta dado hacer diferenciaciones, es una antigua regla de hermenéutica que en este caso tiene cabal aplicación, debido a que si el artículo 11 de la ley 446 de 1998 no diferencia entre documentos originales o en copia, firmados o sin firmar, manuscritos o realizados por medios mecánicos, no es adecuado interpretar que debemos entender que opere únicamente para originales o los que están manuscritos o firmados y menos basados en normas que precisamente la nueva ley vino a derogar". Encontramos también sustento en la interpretación que hacemos del artículo en que en nuestro sistema jurídico las presunciones de autenticidad cuentan con un apoyo constitucional. Presumir la autenticidad de un documento por el hecho que una de las partes demuestre que dicho documento fue elaborado, manuscrito o firmado (sin ser este último un requisito indispensable) encuentra su sustento en la presunción de la buena fe de todas las personas. Existe en nuestro sistema, una arraigada presunción de buena fe que no sólo se constata a nivel de códigos y leyes sino de la constitución misma, no olvidemos que el artículo 83 de la Constitución Política reza que: "Las actuaciones de los particulares y de autoridades publicas deberán ceñirse a los postulados de la buena fe, la cual se presumirá en todas las gestiones que aquellos adelanten antes estas". Así mismo el código de Procedimiento Civil en su artículo 71 establece que uno de los deberes de las partes dentro de un proceso es "proceder con lealtad y buena fe en todos sus actos"

Es necesario resaltar que nuestra posición no implica que dicha presunción de autenticidad deba operar automática e irreversiblemente por la simple afirmación de una de las partes procesales. Lo anterior sería ir en contra de los preceptos de la igualdad de las cargas procesales y violaría el derecho de defensa. Es por esto que reconocemos la necesidad imperiosa que todo documento sea este electrónico o no cuente con signos o señales que permitan su individualización.

Lo anterior implica que un demandante no puede pretender valer como prueba o sustento de su demanda un documento electrónico elaborado por procesador e imputarle la autoría del mismo a otro sujeto sin que en dicho documento electrónico se constate una firma digital o un signo o señal electrónica que permita atribuir la autoría del documento al demandado (individualizarlo). Permitir lo anterior sería desconocer que dicho documento carecería de las características básicas para la presunción de autenticidad, ya que ni estaría firmado ni sería viable afirmar con certeza (requisito establecido por el artículo 252 del CPC) que fue manuscrito o elaborado por el demandado, a este último no le quedaría otro camino que el de tachar de falso dicho documento. Así las cosas aún cuando el documento electrónico no haya sido reconocido, el juez puede considerarlo como auténtico si ha mediado resistencia a su reconocimiento o en los supuestos de silencio o respuestas evasivas

Referente a este tema afirma el manual estadounidense que si bien la evidencia digital se trata en principio como aquella evidencia material, es menester que aquel interesado en proponer la prueba, demuestre su autenticidad. Carga adicional que le es impuesta y que para nuestro sistema se considera como una necesidad únicamente si es controvertida la prueba, es decir si es puesta en duda.

Otro tema relacionado con la autenticidad de los documentos es la figura de las entidades certificadoras que trae la ley 527. Ha sido materia de pronunciamiento judicial y criticado ya el tema de las entidades certificadoras. En sentencia C-662 de 2000 la demandante dice cuestionar el texto íntegro de la Ley 527 de 1999 y, en especial, sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999, por estimar que violan el artículo 131 de la Carta Política, así como los artículos 152 y 153.

La trasgresión del artículo 131 Constitucional en su criterio, se produce, en cuanto las normas acusadas crean unas entidades de certificación las que, de conformidad con la misma Ley 527 de 1999, están facultadas para emitir certificados en relación con las firmas digitales de las personas y para ofrecer los servicios de registro y estampado cronológico, la de certificación de la transmisión y recepción de mensajes de datos, así como cualquier otra de autenticación de firmas relativas a las comunicaciones basadas en firmas digitales, a emitir certificados en relación con la veracidad de firmas digitales de personas naturales o jurídicas es decir acaparamiento de las funciones exclusivas de los Notarios, únicos depositarios de la fe pública.

Cita la sentencia a la demandante: «lo que no permite la Constitución Política es que la autenticidad del documento privado sea función que pueda ejercer cualquier persona, por cuanto esta es una función propia del servicio público notarial y solo le puede corresponder al Notario, el cual siempre tiene que ser una persona natural, que llegue a serlo en propiedad o por concurso.»

«... si la ley le asigna la función fedante a personas diferentes de los Notarios, infringiría en forma directa lo establecido en el artículo 131 de la Carta y esto es, precisamente lo que ha hecho la ley acusada, en especial en los artículos antes citados 2, 10, 11, 12, 13, 14, 15, 26, 27, 28, 29, 30 32, 34, 35, 36, 37, 38, 39, 40 41, 42, 43 y 45 de la Ley 527 en comento.»

Lógica y acertadamente se separa la Corte de tan inapropiada aseveración e instruye afirmando que son entidades de certificación, aquellas que expidan actos denominados Certificados, los cuales se deberán entender como manifestaciones hechas, resultado de la verificación que efectúan sobre la autenticidad, veracidad y legitimidad de las claves criptográficas y la integridad de un mensaje de datos.

La naturaleza de la función de las entidades de certificación se considera como la prestación de un servicio público, que trata el artículo 365 de la Constitución Política, los cuales pueden ser prestados tanto por las entidades públicas como las privadas o conjuntamente. Esta norma permite que este servicio lo presten los particulares, si reúnen los requisitos exigidos por la ley y cuentan con la aprobación de la Superintendencia.

Podrán ser entidades de certificación según el artículo 31, las Cámaras de Comercio, los notarios y cónsules, las personas jurídicas nacionales y extranjeras, tanto públicas como privadas, autorizadas por la Superintendencia respectiva, que cumplan con los requerimientos y condiciones establecidos por el Gobierno Nacional.

Una vez las entidades de certificación sean autorizadas, podrán realizar actividades tales como, emitir certificados en relación con las firmas digitales; ofrecer o facilitar los servicios de creación de firmas digitales certificadas; servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos; servicios de archivo y conservación de mensajes de datos, entre otras.

Afirma la citada providencia que en consecuencia, serán las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, lo que las hace importantes y merecedoras de un control ejercido por un ente público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico.

Se consideró que la Superintendencia de Industria y Comercio debe ser la entidad encargada del control y vigilancia de las entidades de certificación, por cuanto su competencia es afín con estas labores.

En razón a que la naturaleza de las funciones de las entidades de certificación se consideran como la prestación de un servicio público, la inspección y vigilancia de los servicios públicos que tienen que ver con la certificación, actividades que ejercerán las entidades de certificación, debe radicarse en cabeza de una Superintendencia como la de Industria y Comercio.

Conclusiones

La incorporación de nuevas tecnologías en nuestras vidas y los retos y dificultades que estas nos presentan en muchas facetas, como la jurídica, se ha intensificado día tras día. Prueba de esto son los problemas y las dificultades a la hora de determinar claramente conceptos como nacionalidad, jurisdicción, competencia, ley aplicable etc., todos estos conceptos utilizados en la creación de políticas públicas y normas jurídicas. Los anteriores conceptos cuando son analizados en contextos tecnológicos modernos como el Internet entre otros parecen perder y desdibujarse sus límites y su esencia. En Colombia aún cuando nos hemos concientizado de lo anterior y de los problemas y retos que traen consigo, nuestros esfuerzos se han quedado cortos. En cuanto a nuestro tema de investigación estas limitaciones y peligros se evidencian en varios puntos ya mencionados a lo largo de este escrito, sin embargo a manera de ejemplo, reiteramos la carencia a nivel legislativo de definiciones del concepto de evidencia digital y los peligros que esto implica al permitir una aplicación del parágrafo segundo del artículo 175 del Código de Procedimiento Civil en cuanto al trato que se le debe dar a la evidencia considerada como documento para su admisibilidad y manejo dentro del proceso.

De otra parte, si bien la investigación ofrece resultados como los anteriores, es necesario concluir que la legislación actual con ciertas modificaciones permitiría el reconocimiento de la evidencia digital como una prueba. La evidencia digital se presentaría entonces bajo la modalidad de la prueba documentaria, siempre y cuando cumpla con ciertos requisitos de autenticidad, confiabilidad y suficiencia. Cumplidos estos requisitos es claro entonces que el valor de la evidencia digital como prueba, sería el de cualquier otra prueba dentro del proceso ya que se debería apreciar en conjunto con el resto del acervo probatorio conforme a las reglas de la sana critica. Sin embargo, después de analizar los códigos, jurisprudencia y demás normativa, se evidencia un vacío por cuanto no habría reglas jurídicas claras en cuanto a los requisitos que deba cumplir la evidencia digital, ni reglas claras para su manejo y conservación. Es claro que no existe una conciencia generalizada entre los ciudadanos que muchos de los documentos que posee son pruebas en la forma de evidencia digital. El no ser conscientes de lo anterior, no les permite reconocer la necesidad imperiosa de que estas pruebas sean conservadas y administradas adecuadamente y que la solución está en la incorporación de una política clara sobre la administración y manejo de la evidencia digital que permita satisfacer las necesidades de autenticidad, confiabilidad y suficiencia necesarias para que adquieran un valor jurídico relevante.

Es decir, parte esencial de las modificaciones necesarias para que la evidencia digital se considere sin mayores dudas como una prueba y para que esta cuente con un correcto funcionamiento y cumpla con todos los requisitos y se exploten todas sus bondades y se minimicen sus riesgos es contar con un estándar de admisión, manejo y valoración de la evidencia digital. Los retos y problemas planteados por este escrito ya analizados, se podrían resolver en un contexto práctico si se adopta un estándar de evidencia digital que permita establecer parámetros claros y precisos que aseguren que la integridad, sincronización y centralización de la evidencia digital se cumpla y con esto se logre un adecuado estudio y valoración de la misma. Esta solución ha sido la adoptada por varios países como Australia, Estados Unidos, Inglaterra y Canadá y nuestro país debe ser conciente que dicha tendencia debe ser incorporada dentro de nuestro sistema para sanear los problemas ya analizados a través de este escrito. Existen entonces dos grandes retos el primero modificar la normatividad vigente para permitir que la evidencia digital sea aceptada sin mayores contratiempos y segundo crear o adoptar un estándar que permita establecer parámetros claros y precisos que aseguren que la integridad, sincronización y centralización, autenticidad y confiabilidad de la evidencia digital.

Bibliografía

DOCTRINA

CANO, JEIMY JOSE. (2000) Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas, Derecho de Internet & Telecomunicaciones de la facultad de derecho de la Universidad de los Andes. Legis 2003 Basado en una definición del autor Casey E. en Digital Evidence and Computer Crime, Academic Press.

CANO, JEIMY JOSE (2000) "Credenciales para investigadores forenses en informática. en la revista Electrónica de derecho Informático No 38 Septiembre http://v2.vlex.com/global/redi/detalledoctrinaredi.asp?articulo =114090

CARDOSO ISAZA, JORGE. (1985) Pruebas judiciales. Librería Jurídicas Wilches. Bogota

CARNELUTTI, FRANCISO. (1944) Sistema de Derecho Procesal Civil. T. II. Trad. de Niceto Alcalá -Zamora y Castillo y Santiago Sentís Melendo. Buenos Aires. Uteha..

DICCIONARIO DE LA REAL ACADEMIA ESPAÑOLA (2003)

DICCIONARIO JURÍDICO GUILLERMO CABANELAS DE LAS CUEVAS Y ELEANOR C. HOUAGUE, TOMO I ED. HELIASTA (1998)

GATES, WILLIAM H. (1995) Camino al futuro. McGraw/Interamericana de España SA.

GUERRERO M., MARIA FERNANDA (2003) La ciberdelincuencia: la ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso colombiano". Derecho de Internet & Telecomunicaciones. Facultad de derecho de la Universidad de los Andes. Legis

GUTIERREZ GOMEZ, MARIA CLARA (2003) "Hacia el gobierno electrónico: elementos para el desarrollo de una política estatal" Derecho de Internet & Telecomunicaciones. Facultad de derecho de la Universidad de los Andes. Legis.

KATSH, ETHAN. (1985) The Electronic Media and the Transformation of Law. Oxford University Press.

LEIVA, JIJENA JAVIER, RENATO. (2001) Naturaleza jurídica y valor probatorio del documento electrónico, Informática y Derecho No 23/26 V. 2

LESSIG, LAWRENCE. (1999) Code and Others Laws of Cyberspace. Grupo Santillana Editorial S.A.

LESSIG, LAWRENCE (2001). THE FUTURE OF IDEAS, The fate of The Commons in a Conencted World,. Random House, Inc. United States, New York and Random House of Canada Limited, Toronto 2001.

LOPEZ BLANCO, HERNAN FABIO (2001) "Procedimiento Civil, Pruebas" Editorial Dupre.

LYNCH, HORACIO M (1996) Revista jurídica LA LEY. Buenos Aires Argentina.Vol. l15 de mayo de 1996

MCLUHAN, MARSHALL (1989) The Gutemberg Galaxy. Toronto. University of Toronto Press, 1962, cit. por M. Ethan KATSH, en The Electronic Media and the Transformation of Law. Oxford University Press.

ORTIZ R., ILLESCAS (2001). Derecho de la contratación electrónica, Civitas, Madrid.

RAMÍREZ GÓMEZ, JOSÉ FERNANDO (2000) La Prueba Documental Teoría General. Señal Editora, Medellín. Séptima edición.

RICO CARRILLO, MARILIANA (2003) La función procesal probatoria del documento electrónico. Derecho de Internet & Telecomunicaciones. Facultad de derecho de la Universidad de los Andes. Legis

RODRÍGUEZ AZUERO, SERGIO. (2003) Contratos Bancarios sus significación en América Latina. Editorial Legis

VIRUSPROT artículo "Informática forense, liderando las investigaciones en el portal de seguridad Virusprot. http://www.virusprot.com/Col8.html. Entrevista a Jeimy J. Cano.

JURISPRUDENCIA

Corte suprema de justicia sala de casación civil del 4 de septiembre de 2000 con ponencia del Dr. Carlos Ignacio Jaramillo

People v. Holowko, 486 n.e.2d 877, 878-79 (ill. 1985) (Estados Unidos)

Sentencia c-562 de 2000 del Magistrado Vladimiro Naranjo Mesa

Sentenica c-662 de 2000 del Magistrado Fabio Morón Díaz

Tribunal Supremo Español en sentencia del 30 de noviembre de 1981

United States v. Bonallo, 858 f.2d 1427, 1436 (9th cir. 1988)

United States v. Catabran, 836 f.2d 453, 458 (9th cir. 1988).

United States v. Degeorgia, 420 f.2d 889, 893 n.11 (9th cir. 1969)

United States v. Dioguardi, 428 f.2d 1033, 1038 (c.a.n.y. 1970).

United States v. Glasser, 773 f.2d 1553, 1559 (11th cir. 1985)

United States v. Glasser, 773 f.2d 1553, 1559 (11th cir. 1985) United States v. Glasser, 773 f.2d 1553, 1559 (11th cir. 1985)

United States v. Miller, 771 f.2d 1219, 1237 (9th cir. 1985)

United States v. Moore, 923 f.2d 910, 915 (1st cir. 1991)

United States v. Oshatz, 912 f.2d 534, 543 (2d cir. 1990)

United States v. Salgado, 250 f.3d 438, 452-53 (6th cir. 2001)

United States v. Vela, 673 f.2d 86, 90 (5th cir. 1982)

United States v. Whitaker, 127 f.3d 595, 601 (7th cir. 1997)

NORMAS

Nacionales

Circular del 14 de mayo de 1997 de la Presidencia de la República

Codigo de Procedimiento Civil

Codigo de Procedimiento Penal

Codigo Penal

Constitucion Politica

Decreto 1094 de1996

Estatuto Tributario 661-1

Ley 223 de 1995,

Ley 446 de 1998

Ley 527 de 1999

Ley 98 del 20 de diciembre de 1993

Internacionales

Artículo 7 de la ley sobre mensajes de datos y firmas electronicas (lmdfe) (Venezuela)

Código Federal de Procedimientos Civiles. Artículo 210-a (México)

Código Penal Español

Federal. Rules of Evidence 901(b)(9) (Estados Unidos)

Ley 16 de 1985 del patrimonio histórico de 25 de junio (España)

Ley sobre servicios de la sociedad de la informática y el comercio electrónico (ley 34 de 11 de julio de 2002) Artículo 24.2 (España)

Normas generales de derecho probatorio de los Estados Unidos

Real Decreto 828/1995 de 19 de mayo de 1995 (España)

ESTANDARES Y URL´S

(http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm

- Evidence Act (Northern Territory)
- Evidence Act 1906 (Western Australia)
- Evidence Act 1929 (South Australia)
- Evidence Act 1958 (Victoria)
- Evidence Act 1971 (Australian Capital Territory)
- Evidence Act 1977 (Queensland)
- Evidence Act 1995 (New South Wales)
- Evidence Amendment Act 1999 (Tasmania)

5fact/ea199580/?query=title+%28+%22 evidence%22+%29

Commonwealth Evidence Act 1995 (Federal jurisdiction)

consol%5fact/ea80/?query=title+%28+%22evidence%22+%29

de http://www.bsi-global.com/News/FAQ/Standard.xalter

ea197780/?query=title+%28+%22evidence%22+%29

http://scaleplus.law.gov.au/html/pasteact/2/1182/top.htm

http://scaleplus.law.gov.au/html/pasteact/2/1182/top.htm

http://scaleplus.law.gov.au/html/sasact/0/165/top.htm

http://www.austlii.edu.au/au/legis/act/consol_act/ea197180/

http://www.austlii.edu.au/au/legis/tas/consol_act/eaa1999160/

http://www.austlii.edu.au/au/legis/wa/consol_act/ea190680/

http://www.austlii.edu.au/cgi-bin/ disp.pl/au/legis/nsw/consol%

http://www.austlii.edu.au/cgi-bin/disp.pl/au/legis/nt/

http://www.austlii.edu.au/cgi-bin/disp.pl/au/legis/qld/consol%5fact/

http://www.bsi-global.com/index.xalter

http://www.ctose.org/info/index.html

http://www.cybercrime.gov/s&smanual2002.htm#_VA_ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Department of Justice)

http://www.dca.gov.uk/foi/codemanrec.htm

http://www.dms.dpc.vic.gov.au/l2d/E/ACT01286/13_7.html

http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#Proposed

http://www.group5.pwp.blueyonder.co.uk/company.htm

http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html

http://www.pro.gov.uk/about/preservation/digital/archive/default.htm

http://www.pro.gov.uk/recordsmanagement/

http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/2002referencefinal.pdf

http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/default.htm

http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS342335504743

http://www.tso.co.uk/bookshop/bookstore.asp?FO=1149607&DI=513225

http://www.law.ualberta.ca/alri/ulc/current/felev.htm

www.icontec.org.co