INCORPORACIÓN DE LA PRUEBA CIBERNÉTICA E INFORMÁTICA: ELECTRÓNICA Y DIGITAL*

Judicial incorporation of the cybernetic and computer evidence: electronic and digital

Jaime Alberto Díaz Limón

Resumen

Los Tribunales y postulantes se enfrentan de forma cotidiana a la compleja labor de la incorporación de medios de convicción que provienen de las nuevas tecnologías de la información y la comunicación; lo anterior, deriva de la falta de legislación precisa y oportuna en materia de ofrecimiento, desahogo y valoración, así como el trabajo procesal de la conservación forense. Asimismo, impera el uso de sinónimos por lo que refiere a la prueba electrónica y digital, lo que esfuma la claridad para que el juez cuente con reglas claras para su revisión. El presente artículo tiene su base en un método deductivo y hermenéutico que pretende generar ruptura en la ideología dominante y rescatar el valor epistemológico del concepto "documento". Asimismo, propone un estudio etimológico sobre el concepto de pruebas cibernéticas, informáticas, electrónicas y digitales, los

* Artículo inédito.

Para citar el artículo: DÍAZ LIMÓN, Jaime Alberto. Incorporación de la prueba cibernética e informática: electrónica y digital. *Revista del Instituto Colombiano de Derecho Procesal*. No. 47 Enero – Junio. 2018, pp. 19-42.

Recibido: 14 de marzo de 2018 - Aprobado: 13 de agosto de 2018.

** Licenciado en Derecho por la Universidad Autónoma Metropolitana (México/Azcapotzalco). Maestro en Derecho Administrativo y Fiscal por la Facultad de Derecho de la Barra Nacional de Abogados. Fundador de la alianza iberoamericana "Código Abogado Digital". Coordinador de la columna de Propiedad Intelectual para la revista Foro Jurídico. Catedrático y conferencista internacional en materia de Derecho Informático y Propiedad Intelectual.

principios fundamentales para su incorporación y una vía adecuada, jurídico-técnica, para su debida valoración.

Palabras clave: Prueba digital, prueba cibernética, conservación forense, ley modelo, mensaje de datos.

Abstract

The Courts and the attorneys face on a daily the complex task of incorporating the proofs of conviction that come from the new information and communication technologies; the foregoing derives from the lack of precise and timely legislation in terms of offer, relief and assessment, as well as the work for forensic conservation before-procedural. Likewise, the use of synonyms reigns in terms of electronic and digital evidence, which fades the procedural clarity so that the judge has clear rules for review in sentencing. The present article has its base in a deductive and hermeneutic method that tries to generate rupture in the dominant ideology and rescue the epistemological value of the concept "document". This article proposes an etymological study on cybernetic, computer, electronic and digital proofs, as well as the fundamental principles for its procedural incorporation; in order to propose a suitable procedural path, legally- technicall, for its due assessment.

Keywords: Digital evidence, cybernetic evidence, forensic conservation, model law, data message.

Introducción

En el año 2014 *Apple* creó una herramienta de encriptación que permite que sus equipos sean matemáticamente infranqueables, esto brinda mayor seguridad a sus usuarios contra *hackeos* ilegales o probables intervenciones del gobierno. Sin embargo, esta garantía de invulnerabilidad (*no backdoor*) se convirtió en el dilema del gobierno americano, cuando el 2 de diciembre de 2015 dos practicantes radicales del Islam atacaron un edificio en el sur de California; a esto se le conoció como el caso "San Bernardino". Uno de los sospechosos, Syed Farook, trabajó para el condado y durante su gestión se le entregó un iPhone 5C. Esto facilitó la investigación del FBI, ya que los equipos anteriores a esa categoría aún cargaban automáticamente los datos, imágenes y archivos del equipo al servicio de nube conocido como *iCloud.* Empero, esto no demostró los hechos ni acreditó las causas probables del atentado terrorista, debido a que sólo se lograron rescatar datos hasta octubre de 2014, fecha en la que la *Apple* liberó su sistema de encriptamiento y transformó sus equipos móviles

en los "más seguros del mundo". Esta característica obligó al Buro Federal de Investigación a requerir al fabricante el desencriptar los equipos o desarrollar un *backdoor* para su propio sistema operativo, es decir, hackear su propio equipo de tal suerte que se permitiera la investigación; la respuesta de Tim Cook –CEO de la compañía- fue tajante, pues a pesar de manifestar que no simpatizan con los terroristas, también indicó que los extremistas fallecidos fueron usuarios *Apple* con garantía de protección activa, ello se tradujo en seguridad y encriptamiento absoluto de su información, incluida aquella relacionada en la comisión del delito. En respuesta a las declaraciones de Cook, Barack Obama –el entonces presidente de los Estados Unidos de América- se expresó públicamente en contra de la decisión de la compañía desarrolladora, arguyendo un inverosímil estado de Derecho que protege la privacidad de un par de usuarios, sobre la seguridad nacional, en tanto que el Buro de investigación a su cargo, amenazó con hackear estos equipos con la ayuda de *Apple* o sin ésta. Sin entrar a un debate de moral según lo plantea el dilema político-jurídico anterior, la amenaza del *FBI* advierte graves carencias en la comprensión de la obtención lícita de pruebas digitales, así como la cadena de custodia y la incorporación al proceso de cualquier mensaje de datos. Independientemente del precedente negativo que el caso de San Bernardino pudiere generar para la seguridad internacional, es indiscutible que cada día se colocan en el émbolo de relevancia jurídica los medios de convicción que se generan a través de medios cibernéticos, informáticos, electrónicos y digitales, sin embargo, ha sido poco el estudio jurídico que se brinda a los mismos y, en muchas ocasiones, se ocupan sinónimos que únicamente entorpecen el camino hacia su incorporación a procesos jurisdiccionales, por tanto, también complican el camino legislativo que pudiere ser la delgada línea de legalidad entre la prudente intervención de comunicaciones o la obtención de pruebas ilícitas en perjuicio de la privacidad de los usuarios. El objeto del presente artículo no sólo será el diseminar la ambigüedad con la que se trata a estos medios de convicción, sino delimitar los principios y estándares de incorporación de la prueba electrónica y digital. En ese tenor, el artículo brindará el panorama etimológico del concepto "documento" y pretende su flexibilización para su aplicación a medios tecnológicos de prueba; posteriormente, invoca el derecho comparado para reconocer los requisitos esenciales para la debida incorporación de las pruebas cibernéticas e informáticas, así como las reglas fundamentales para la conservación forense de éstas.

1. Concepto de Documento *Lato Sensu* (sentido amplio)

El Diccionario de la Real Academia Española en su segunda y tercera acepción brinda aquellas de mayor importancia para la construcción de mi hipótesis: "Escrito en que constan datos fidedignos o susceptibles de ser empleados como

tales para probar algo…Cosa que sirve para testimoniar un hecho informar de él, especialmente del pasado."[1] A su vez, el Diccionario de Derecho Procesal Civil de Eduardo Pallares, sostiene que: "…documento es toda cosa que tiene algo escrito con sentido inteligible"; en el entendido que "escribir" se comprende como la actividad mediante la cual el hombre expresa ideas y sentimientos por medio de la palabra escrita, sin importar si dicha escritura se hace sobre papel o cualquier otro material, ni resultando indispensable que el lenguaje esté formado por "vocablos". En ese tenor, el procesalista Pallares, formula la incógnita y a su vez responde: "¿Los documentos taquigráficos son pruebas científicas o documentales? El Código las incluye entre las científicas, pero deben considerarse como documentales, porque contienen algo escrito con sentido inteligible…"[2]. En atención a su raíz etimológica, la voz documento deriva de *docere* (enseñar, hacer, conocer) y conforme lo dicta el Maestro Hernando Devis Echandía, es posible comprender un concepto de documento, desde el punto de vista estricto y amplio, a saber:

> "El documento, como el testimonio o la confesión, es el resultado de una actividad humana; pero, como observa *Carnelutti*, mientras los últimos son *actos*, el primero es una cosa creada mediante un acto y de allí se concluye que mientras que el acto testimonio o confesión es por sí mismo representativo del hecho testimoniado o confesado, el acto que crea el documento no es representativo del hecho narrado en este, sino que se limita a crear el vehículo de representación, que es ese documento. En **sentido estricto**, es documento <<toda cosa que sea producto de un acto humano, perceptible con los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera>>…Ha existido la tendencia de identificar los conceptos de documento e instrumento o escrito, como si todos los documentos consistieran en escritos… La representación, por lo tanto, no está en el documento, sino en el juicio de quien lo asume como medio de prueba e incluye en un concepto **amplio de documento** la huella de un evento natural o de un pie, por lo cual concluye afirmando que <<una definición correcta del documento prescinde del concepto de representación, que es propiamente la operación lógica de quien lo asume como medio de prueba, y debe operar únicamente en la relación documento-prueba>>, porque lo esencial no es la representación, sino un *posterius* respecto de su existencia"[3].

---

1 "Documento". Diccionario de la Real Academia Española. Definiciones. España, 2001. http://dle.rae.es/?id=E4EdgX1. Consultado en línea el 10 de julio de 2017.

2 PALLARES, Eduardo. *Diccionario de Derecho Procesal Civil*. Concepto de "documento". Vigésima Octava Edición. México. Editorial Porrúa, 2005, pp. 201-201.

3 DEVIS ECHANDÍA, Hernando. "De la Prueba Por Documentos". *Teoría General de la Prueba Judicial*. Sexta Edición. Tomo II. Bogotá. Pontificia Universidad Javeriana, Bogotá, Facultad de Ciencias Jurídicas. 2002.

Según la Doctrina de Chiovenda, documento *lato sensu* es toda representación material destinada e idónea para reproducir una determinada manifestación de pensamiento como una voz fijada duramente: *vox mortua*. Por otro lado, el propio procesalista indica que documento en *strictu sensu* será exclusivamente lo "escrito" (léase aquello escrito en papel)[4]. Interpretaciones y estudios procesales que permiten advertir la doble naturaleza del documento, asimismo, la separación que debe existir entre su capacidad de representación y el objeto material en sí mismo, sobre el cual se han plasmado hechos históricos que permiten acreditar que, en un momento específico, existieron hechos o actos de relevancia jurídica. Bajo la naturaleza del documento en sentido amplio, se permite la presencia de documentos tales como el cibernético e informático, en tanto que el documento electrónico y digital, cuentan con características que les permiten ser considerados dentro de la categoría de documento en sentido estricto. En ese tenor, el Doctor Carlos Barriuso sostiene que la prueba documental también es aquella que se trata de documentos electrónicos representados por cualquier sistema informático[5].

2. Documento cibernético e informático

La Cibernética, según la define el Diccionario de la Real Academia Española es la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas –definición muy similar a la que aporta el Diccionario Legal de Black según la voz *cybernetics*–; creado y regulado mediante computadora[6]. Tal como lo describe el Doctor Julio Téllez Valdés, la Cibernética es la ciencia que se encarga del estudio de la comunicación y control entre el hombre y la máquina. Rescata dicho concepto del matemático estadounidense Norbert Wiener (1948). Invita a reconocer a esta ciencia interdisciplinaria como aquella que estudia la forma en que el cerebro –humano– brinda instrucciones a las máquinas y, a su vez, reconoce la dependencia que la informática tiene con la misma.[7] A su vez, ésta se define en el Diccionario de la RAE como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras[8], en tanto

---

4 Supra. Cit., p. 109.

5 BARRIUSO, Carlos. *Interacción del Derecho y la Informática.* Madrid, España 1996. Editorial Dykinson, p. 100.

6 "Cibernético, ca". Diccionario de la Real Academia Española. Definiciones. España, 2001 http://dle.rae.es/?id=98YYoXW Se consultó en línea el 10 de julio de 2017.

7 TÉLLEZ Valdés, Julio. *Derecho Informático*. Cuarta Edición. México. Editorial McGrawhill. 2009, pp. 131-132.

8 "Informática, co". Diccionario de la Real Academia Española. Definicones. España. 2001 http://dle.rae.es/?id=LY8zQy3. Mismo que se consultó en línea el 10 de julio de 2017.

que el Doctor Téllez Valdés, la detalla como el conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miradas a aun adecuada toma de decisiones; neologismo conformado por los vocablos información y automatización, sugerido por Phillipe Dreyfus (1962). Así las cosas, es inconcuso que la cibernética como ciencia interdisciplinaria se conforma, entre otras disciplinas, por la informática, por lo que es asequible afirmar que existen distinciones claras entre un documento de origen cibernético y otro de carácter informático.

El documento cibernético podría definirse como la acreditación intangible de la instrucción de un usuario a una máquina integrada por circuitos, esto permitiría probar que, en un determinado momento, un sujeto encendió una computadora, la conecto a la corriente directa o bien, simplemente instaló, regeneró, copió o borró un disco duro. Conductas que podrían generar consecuencias jurídicas si se colocan estas hipótesis en situaciones similares a: i) No se cuenta con autorización para operar cierta computadora, ii) La computadora no se debía encender por instrucciones del ingeniero o iii) Se copió o borró información que pudiere tener calidad de confidencial o secreto industrial.

Ahora bien, los medios informáticos son las computadoras (máquinas integradas por circuitos) o herramientas dentro de las mismas (léase aplicaciones o programas de cómputo) creadas con el fin de automatizar la información. En consecuencia de lo anterior, el documento informático podría definirse como la acreditación cibernética, que advierte la existencia de la instrucción de un hombre hacia una computadora, para iniciar un proceso de automatización de información, sin que éste constituya la información automatizada *per se*. Es decir, el documento informático es la evidencia intangible a través de la cual, la computadora deja un rastro de la instrucción del inicio, progreso y fin de un proceso de automatización, sin que el resultado de ello sea considerado también informático, según se estudia en el parágrafo siguiente. Verbigracia, la hora de apertura de un procesador de texto (herramienta que permite automatizar un texto) como lo sería la hora de última conexión que señala el sistema de mensajería instantánea *Whatsapp.* A su vez, los medios informáticos pueden dividirse en dos categorías según la forma en que los documentos pueden almacenarse y distribuirse: i) Electrónico y ii) Digital.

3. Documento electrónico y digital

El Diccionario Legal de Black, define a los medios electrónicos como cualquier dispositivo que almacena y permite la distribución o el uso de información electrónica (televisión, radio, internet, fax, CD-ROM, DVD y cualquier

otro medio electrónico)[9]. Por su lado, el Doctor Julio Téllez define al documento electrónico como el conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que, sometidos a un adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o impresora, asimismo, resalta que para evitar las ambigüedades en el uso de electrónico o digital, prefiere denominarles documentos informáticos –no obstante lo sostenido en el parágrafo anterior–; en el entendido que éstos se crean con la intervención no ya de una computadora, sino de todo un sistema informático[10]. Definición que resulta consonante con lo que hasta ahora hemos expuesto, pero que no permite brindar las características esenciales de cada tipo de documento, en términos del objeto del presente parágrafo. En atención de ello, es el propio Doctor Téllez Valdés, quien afirma que el documento electrónico puede ser concebido en un sentido amplio y en un sentido estricto: i) *Lato Sensu:* Es el que se forma por una computadora (dispositivo electrónico) a través de sus propios órganos de salida, y que es perceptible por el hombre sin la necesidad de máquinas traductoras; y ii) *Strictu Sensu:* El que aparece instrumentado sobre la base de impulsos electrónicos y no sobre un papel; es el conservado en forma digital en la memoria central de la computadora o en las memorias de masa, y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales.[11] Sin embargo, al leal entender de quien esto escribe, parece ser que la definición de documento electrónico en sentido estricto nos remite a una probable acepción de documento digital, en el entendido que este es contenido que se comprimió digitalmente[12] para ser manipulado, distribuido, representado y transmitido a través de redes informáticas. Concepto que se logra fortalecer gracias a la definición que brinda el Diccionario Legal de Black: "…Lo digital son datos enviados en código de encendido y apagado, representado por 1 y 0 (código binario)"[13] . Ello permite aproximarnos a una clasificación concreta respecto de la naturaleza particular de los documentos digitales frente a los documentos electrónicos, en tanto que los

---

9 "Medios Electrónicos". Diccionario Black de Leyes. Definiciones. Estados Unidos de América, 2007. http://espanol.thelawdictionary.org/medios-electronicos/ mismo que se revisó el pasado 10 de julio de 2017.

10 Ob. cit., p. 113.

11 Ibídem.

12 TECHNET, Microsoft. "¿Qué son los medios digitales?" *Microsoft Product Lifecycle*. Contents. Estados Unidos de América, 3 de diciembre de 2012. https://technet.microsoft.com/es-es/library/what-is-digital-media-2(v=ws.11).aspx mismo que se analizó en línea el 10 de julio de 2017.

13 "What is Digital?" Diccionario Legal de Black. Definiciones. Estados Unidos de América, 2007. http://thelawdictionary.org/digital/ Se consultó en línea el 10 de julio de 2017.

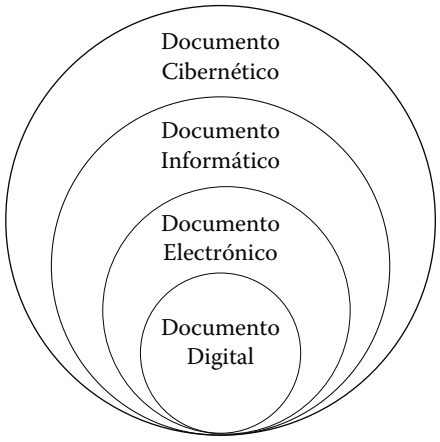
primeros dependen de la funcionalidad de los medios informáticos que permitan que la información sea representada mediante código binario –o cualquier otro código– para ser manipulada, distribuida, representada y transmitida a través de canales digitales; mientras que aquellos de origen electrónico pueden estar presentes en distintos tipos de almacenamiento, lo que permite su consulta, reproducción y transmisión, sin necesidad de que estos se encuentren codificados en un estado de unos y ceros. Si bien es cierto, ambos tipos de documentos pertenecen a la categoría de los documentos informáticos, la diferencia radical entre ambos yace en la calidad para formar parte de la red de redes, en atención a la naturaleza conforme la cual han sido concebidos –informatizados–. Siendo precisos con los medios electrónicos de comunicación que pudieren considerarse digitales, encontramos la televisión digital e internet, por lo que es inconcuso que los documentos que se generan a través de estas plataformas pueden considerarse documentos electrónicos y particularizando, documentos digitales. Así las cosas, un documento electrónico puede considerarse un archivo de texto generado por un procesador que automatice caracteres (una carta escrita en *Office Word*), mientras que un correo "electrónico" no debería considerarse documento electrónico, por el simple hecho de que éste, para su almacenamiento, depende de la codificación digital. Bajo esta hipótesis, la carta de referencia mutaría la naturaleza bajo la cual fue concebida, en el momento que esta se carga al servidor (*Upload)* y ahora pertenece a la red de redes, requiriendo, para su consulta, reproducción y comunicación, acceder a la *World Wide Web*. El documento electrónico muta en documento digital al momento de que éste ingresa a la compleja telaraña de la autopista de la información. Sin embargo, la calidad de documento digital no se pierde por realizar el proceso inverso de almacenamiento virtual, es decir *Download*, toda vez que esta acción no consiste en retirar el documento de internet, sino únicamente un proceso de reproducción en dispositivos que no necesariamente se encuentren diseñados para estar conectados a la red de redes en todo momento; así las cosas, este proceso de **descarga** permitirá almacenar una versión del documento bajo la modalidad de electrónico. Es imperativo resaltar que las diversas mutaciones, así como reproducciones que pudiere sufrir el documento, atentan contra el valor probatorio del mismo, toda vez que cada versión de éste pudiere afectar los estándares de integridad y autenticidad (según se definen más adelante).

Hasta ahora hemos logrado identificar la diferencia que existente entre un documento en sentido amplio y en sentido estricto, entre escritura y documento, así como las categorías que se desprenden de la cibernética para analizar la naturaleza de cada tipo de soporte. Es importante invocar las letras del Maestro Hernando Devis Echandía, quien señala:

> "Se ha confundido en ocasiones el documento con la materia de que está formado, especialmente con el papel utilizado para los escritos o instrumentos

> privados y públicos, pero no sólo existen otras materiales utilizables para esta clase de documentos, como telas, maderas, cueros…sino que el documento es algo más que esa materia y principalmente está constituido por su contenido gráfico, escrito o figurativo o de otra clase (como en los discos y cintas magnetofónicas) …Además, se identifica erróneamente el contenido con el continente, siendo así que, incluso cuando se trata de escritos o instrumentos, la forma es la exterioridad del hecho o acto jurídico documentado..."[14].

Afirmación que permite aclarar que en tanto los documentos cibernéticos a que hemos hecho referencia contengan un elemento declarativo o representativo de valor jurisdiccional, estos deben ser analizados bajo la categoría que les corresponda; en atención a lo que se pretende acreditar con el contenido de los mismos y no bajo el estricto examen del continente de dicho hecho o acto jurídico. Asimismo, se debe considerar la naturaleza de los cibernéticos e informáticos desde la postura de los documentos en sentido amplio, mientras que los documentos en sentido estricto, permiten el ingreso de medios de convicción electrónicos y digitales por la "escritura" que se puede desprender de ellos, vestigio que resulta de trascendencia jurídica aunque ello no se desprenda de un medio tradicional de probanza –tal como lo es un papel–, según las aportaciones de Eduardo Pallares y Chiovenda que se han invocado con anterioridad. Hasta este punto, me permito proponer al lector el siguiente diagrama de Venn:



Según la teoría de conjuntos propuesta, es inconcuso afirmar que todo documento digital es un documento electrónico, a su vez informático y cibernético. Además, todo documento electrónico es informático y cibernético, sin embargo, no necesariamente será digital. Por su lado, se advierte que todo

[14] Ob. cit., p. 110.

documento informático es cibernético y éste, podría almacenarse y distribuirse a través de medios electrónicos y digitales, lo cual tendría por origen un documento electrónico o digital, según sea el caso.

Es importante resaltar que el presente conjunto de Venn, únicamente resulta una propuesta para comprender las categorías de documento desde la perspectiva del análisis técnico jurídico que se brinda, sin que resulte limitante a las posturas legislativas que se presentan en cada país.

4. Características de los documentos electrónicos y digitales

En diversas legislaciones se ha adoptado el sistema de la sana crítica o el principio de libertad de prueba ["que consiste en otorgar libertad a los juzgadores para determinar los medios de prueba, su eficacia probatoria y la manera de producirlos"] por lo que refiere a la valoración probatoria de soportes informáticos. Según lo expone el Doctor Julio Téllez, algunos soportes se enfrentan al desconocimiento jurídico para ser considerados como prueba dentro de procedimientos jurisdiccionales, con independencia de que estos pudieren resultar benéficos en atención a la durabilidad y fidelidad al original que presentan, respecto de aquéllos de naturaleza tradicional.[15] Afortunadamente para el panorama procesal de las pruebas que actualmente estudiamos, el 30 de enero de 1997 se aprobó por la Comisión de las Naciones Unidades para el Derecho Mercantil Internacional en la Asamblea General de ONU, la Ley Modelo sobre Comercio Electrónico, con la finalidad de armonizar y unificar a los países involucrados, en atención de permitir el progreso amplio del comercio internacional. Posteriormente, ésta traería a la vida el proyecto conocido como "Ley Modelo de la CNUDMI sobre Firmas Electrónicas". El mérito de la Ley Modelo en materia de comercio radica en la invitación internacional para dotar de valor probatorio a mensajes de datos que estuvieren contenidos en medios electrónicos, ópticos o similares –léase, digitales–, así como prescribir las reglas para su incorporación a un procedimiento, siempre que cumplieran con los principios contenidos en la propia normativa estandarizada. Inicialmente, conviene invocar el contenido del artículo 2 de dicha Ley, ya que la misma aporta definiciones fundamentales para el entendimiento del presente apartado:

> "Artículo 2.- Definiciones Para los fines de la presente Ley: a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o

[15] TÉLLEZ VALDÉS, Julio. "Capítulo XVI. Valor probatorio de los soportes informáticos". *Derecho Informático*. Segunda edición. México. Editorial Mc Graw Hill. 1998. 115-121 pp. https://biblio.juridicas.unam.mx/bjv/detalle-libro/1941-derecho-informatico visto el 29 de noviembre de 2017.

> comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax; b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto…"

Desde el punto de vista semántico, el artículo que reproduzco permite aclarar la unidad de medida mínima a estudiar en el presente parágrafo, mismo que se denomina "mensaje de datos", a la cual se puede considerar el *contenido*. A su vez, fija el parámetro jurídico para calificar al soporte que se presentará como prueba dentro de un proceso, ya sea de naturaleza óptica, electrónica o digital; a éste se le considerará el *continente*. Por otro lado, dicta las reglas del juego electrónico, al colocar como sujetos de protección al "iniciador-intermediario-destinatario" que ocupan un sistema de información para generar, enviar, recibir, archivar o procesar un mensaje de datos. A modo de reflexión, la regla general en el proceso dicta que el mensaje informático es aquél que se deberá ofrecer, desahogar y valorar dentro de un procedimiento, en tanto que el soporte (continente) debería fungir como el mecanismo, por excelencia, para que éste se fije en el procedimiento y se respeten cada uno de los principios que señala la Ley en cita. Como excepción, algunos Tribunales han optado por aceptar el mensaje de datos, pero no permiten su desahogo a través del soporte *ex profeso;* es decir, se inclinan por posturas de perfeccionamiento de la prueba (pruebas corroborantes) a través de certificaciones notariales, inspecciones oculares o cotejos, como si se tratare de pruebas tradicionales.

Si bien es cierto que la Ley Modelo UNCITRAL no resulta aplicable por razón de materia a otras ramas del Derecho, ésta ha servido como base doctrinaria para que los países partes adapten sus legislaciones más allá del universo mercantil. Así las cosas, ha obtenido popularidad legislativa la postura de tomar los principios de la Ley Modelo y flexibilizarlos a otras ramas de nuestra ciencia, siempre que los documentos electrónicos o digitales, respeten la debida integración de los mismos, según los principios y estándares que a continuación se detallan.

4.1 Equivalencia funcional, no discriminación y neutralidad

La *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio electrónico* es un documento anexo a la Ley Modelo, cuyo fin primordial es orientar a los usuarios de los medios electrónicos de comunicación en los aspectos jurídicos de su empleo. Dicha guía reconoce la necesidad de vencer impedimentos al empleo de comercio electrónico y la

admisibilidad de mensajes de datos a procesos, frente a conceptos ortodoxos como "escrito", "firma" y "original"; mismos que hemos ido destruyendo –o flexibilizando– en el recorrido del presente artículo. En ese tenor, invita a los Estados incorporados a no abandonar conceptos y planteamientos jurídicos que requieran de un escrito, pero siempre con miras de adaptar su funcionamiento a los nuevos avances técnicos de las comunicaciones. Así las cosas, la Comisión de las Naciones Unidas logró acuñar con éxito el criterio de "equivalencia funcional", el cual no sólo aplicó a la presente Ley Modelo, sino a la relacionado con Arbitraje Comercial Internacional y el contenido del artículo 13 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Bajo ese tenor, el criterio de equivalencia funcional se puede definir como el análisis de los objetivos y funciones de un requisito tradicional de presentación de un escrito consignado sobre papel contra aquél que pudiere presentarse en un soporte electrónico o digital, en atención a los siguientes estándares:

1. Proporcionar un documento legible para todos;
2. Asegurar la inalterabilidad de un documento a lo largo del tiempo;
3. Permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar;
4. Permitir la autenticación de los datos consignados suscribiéndolos con una firma; y
5. Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades.[16]

Conforme a lo anterior, la documentación consignada en medios electrónicos no sólo brinda un grado de seguridad equivalente al de papel, sino superior, en la mayoría de los casos; así mismo, resulta preferente si lo sometemos a un examen de fiabilidad, originalidad e integridad. Por otro lado, invita a no descartar medios de convicción por tratarse de un mecanismo no tradicional de probanza y en su caso, permitir la evaluación en igualdad de circunstancias de un documento digital frente a uno tradicional (***no discriminación y neutralidad***). Lo anterior resulta claro frente a incómodos escenarios procesales en los que alguna de las partes estime que el contenido de un documento tradicional fue alterado o no se suscribió por quién se manifestó; para el caso de los documentos electrónicos y digitales, resulta

[16] ONU. CNUDMI. *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUNDMI sobre Comercio Electrónico*. Estados Unidos de América, Nueva York, 1999, p. 15. https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf Visto el 27 de noviembre de 2017.

un trabajo pericial complejo realizar cualquier modificación sobre el origen del documento, la cantidad y calidad del contenido (número de caracteres, espacios, fuente, tamaño e imágenes contenidas), así como la firma que pudiere contener, ya que la firma consiste en un conjunto de caracteres alfa numéricos que se forjan como la huella digital de dicho soporte, cuya inalterabilidad se considera humanamente invensible; hipótesis que no se podrían defender respecto del documento tradicional. Empero, el principio de equivalencia funcional no debe ser interpretado como la búsqueda en la substitución jerárquica de los documentos tradicionales con aquéllos de naturaleza avanzada, sino como la invitación para fijar requisitos mínimos que favorecen la incorporación de un mensaje de datos electrónico, cuando así resultare aplicable según el examen propuesto. Verbigracia, sería insostenible presentar a examen de equivalencia una probanza digital, cuando el argumento medular sobre un juicio sea la autenticidad de una firma autógrafa; escenario en el que resultaría indispensable la presencia del soporte físico *sub judice*.

Por lo que refiere al panorama internacional y en afán de brindar una apreciación global de las características del documento electrónico, resultan aplicables los artículos 8° y 9° de la Ley Modelo UNCITRAL. El numeral octavo de referencia, prescribe:

> "Artículo 8. Ley Modelo UNCITRAL.- Original 1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos: a) Si existe alguna garantía fidedigna 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 a la que se deba presentar... 3) Para los fines del inciso a) del párrafo 1): a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y 7 b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso [...]."

Conforme a los criterios que se reprodujeron, en consonancia con los preceptos invocados, parece claro que un documento electrónico y digital podría aspirar al valor probatorio pleno dentro de un proceso, siempre que cumpla con los **principios de equivalencia funcional, no discriminación y neutralidad** y no exista duda razonable sobre su **fiabilidad, integridad y autenticidad** (en continente o contenido), sin importar si la duda surge en la psique del juzgador o en las intenciones del contrario.

5. Incorporación procesal de pruebas electrónicas y digitales

En términos de los argumentos anteriormente expuestos, resulta inverosímil aceptar cualquier tipo de ofrecimiento y desahogo (incorporación) de una prueba electrónica y digital fuera de los parámetros sostenidos, sin embargo, la realidad procesal provoca que en muchas de las ocasiones los Tribunales no se encuentren debidamente capacitados para comprender la naturaleza *sui géneris* de nuevos medios de convicción y que los abogados postulantes no cuentan con la capacitación técnica para precisar el alcance de la prueba *tecnológica* y porqué ésta debería incorporarse al proceso sin atentar contra su naturaleza digital. Es decir, no resulta admisible que el Tribunal de la causa exija a las partes desahogar una prueba electrónica o digital, a través de mecanismos tradicionales que pudieren afectar los principios de **no discriminación, neutralidad y equivalencia funcional;** verbigracia, un Juez que solicita a la parte oferente de un documento electrónico, que imprima las constancias de un mensaje de datos emitido a través del servicio de mensaje corto (SMS) y, en su caso, perfeccionar dicho medio de convicción a través de certificación notarial, atenta contra la naturaleza tecnológica de dicha probanza, por lo que debería ser permisible exhibir el propio mensaje dentro del equipo telefónico destino, o bien, solicitar el apoyo de la compañía telefónica para obtener un registro confiable de la emisión y recepción de esos datos; de tal suerte que el mensaje que se pretende incorporar a un proceso no pierda su naturaleza, ni sea valorado conforme a principios tradicionales que mermen el valor probatorio. En tales términos, no se deben admitir requerimientos caprichosos en perjuicio de la naturaleza tecnológica de las pruebas, tal como lo sostienen las Naciones Unidas en su Ley Modelo UNCITRAL, cuyo artículo 9° dicta:

> "(…) **Artículo 9**.- **Admisibilidad y fuerza probatoria de los mensajes de datos**
>
> 1) En todo trámite legal, **no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos**:
>
> a) Por la sola razón de que se trate de un mensaje de datos; o
>
> b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.
>
> 2) **Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria**. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente **la fiabilidad** de la forma en la que se haya generado, archivado o comunicado el mensaje, **la fiabilidad** de la forma en

> la que se haya conservado **la integridad de** la información**, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente**."[17] (**El énfasis es añadido).**

El precepto de referencia permite afirmar que las Naciones Unidas ya se preparaban para la aceptación de las pruebas tecnológicamente avanzadas y, en su caso, invitan a los Tribunales a admitir las mismas y brindarles un valor probatorio adecuado a sus circunstancias. Tan sólo del artículo recientemente transcrito, se advierte que el juzgador deberá atender a: i) **Equivalencia funcional.-** Por lo que refiere a no obstaculizar su ofrecimiento y, en todo caso, por ser el mensaje de datos "la mejor" prueba sobre una de carácter tradicional; ii) **Originalidad/ Fiabilidad.-** Por lo que refiere a la capacidad para determinar que el mensaje de datos que se aporta al procedimiento no sufrió ningún cambio desde su emisión, durante su archivo y hasta el momento de su incorporación a un procedimiento; iii) **Integridad.-** Por lo que refiere a la fidelidad del contenido del mensaje de datos; conforme al principio anterior, ni continente o contenido deberán sufrir alteraciones para ser incorporados a un procedimiento; y iv) **Autenticidad.-** Por lo que refiere a la posibilidad de acreditar la identidad de su iniciador/emisor –algunas legislaciones pudieren exigir la presencia de una firma electrónica o digital, empero, no debe considerarse al certificado autenticador un requisito *sine qua non* para considerar por satisfecho el presente requisito; características que deberán interpretarse armónicamente con el artículo 8° del propio ordenamiento.

En ese tenor ha reaccionado el gobierno peruano, a través del Decreto Legislativo número 681 *Uso de tecnologías avanzadas en materia de Archivo*[18], cuyo fin es regular el uso de las "TIC's" en materia de archivos de documentos e información que se produce a través de mecanismos informáticos; en lo particular, faculta la participación de un fedatario informático que auxiliaría en la creación de *microformas* de documentos análogos (*strictu sensu)* y reconoce la validez de los *microarchivos* para acreditar el contenido de los documentos, aún ante la destrucción del soporte "original". Normatividad que, procesalmente, reconoce la fuerza probatoria de los documentos electrónicos y prevé mecanismos particulares de su perfeccionamiento antes de su incorporación al

---

17 Nueva York, Estados Unidos de América, *Ley Modelo de la CNUNDMI sobre Comercio Electrónico,* 1999.

18 ARCHIVO GENERAL DE LA NACIÓN. *Uso de tecnologías avanzadas en materia de archivo. Decreto Legislativo 681.* 11 de octubre de 1991, Perú. Visto a través del vínculo http://webapp.regionsanmartin.gob.pe/sisarch/LEGISLACION/6.%20TECNOLO GIA%20AVANZADA%20EN%20ARCHIVOS/DL_No_681.pdf Este Decreto fue reformado por Decreto Supremo el 6 de octubre de 2016, sin embargo, sostiene el vigor de las figuras jurídicas invocadas.

juicio, en afán de omitir requerimientos ociosos o desnaturalizantes durante el desahogo de aquellos.

El rumbo colombiano resulta un ejemplo de progreso legislativo y judicial, en términos de su Ley 527 de 1999, también conocida como Ley de Comercio Electrónico. En lo particular, sus artículos 10 y 11 brindan la posibilidad de otorgar valor probatorio a un mensaje de datos que se incorpore a un procedimiento, siempre que cumpla con las reglas de la sana crítica y los siguientes aspectos:

> "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**."[19] (El énfasis es añadido)

A su vez, los diversos 8° y 9° del propio ordenamiento fijan las reglas para el ofrecimiento y desahogo de un "mensaje de datos"; en lo esencial, obliga al juzgador a aceptar este medio de probanza siempre que i) Exista garantía confiable de que se ha conservado la integridad de la información; y ii) Que el mensaje de datos y la información pueda mostrarse a la persona que se deba presentar (juez). Es inconcuso que esta Ley reproduce la conducta normativa que exige la Ley Modelo UNCITRAL.

De forma similar, parece ser que el Cuerpo de Administradores Gubernamentales de Buenos Aires, Argentina, ha encontrado la guía jurídica para entender la prueba digital. La Ley número 25.506 de Firma Digital la que

---

[19] REPÚBLICA DE COLOMBIA. CONGRESO DE COLOMBIA. *Ley 527 de 1999.* Publicada el 18 de agosto de 1999. Puede consultar el texto íntegro a través del vínculo http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/ley_527_1999.pdf

establece la validez legal del documento electrónico, de la firma electrónica y de la firma digital, cuyos preceptos 6, 11 y 12 dictan:

> **"Firma Digital. Ley 25.506**
>
> **(…) ARTÍCULO 6º-** Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.
>
> **ARTÍCULO 11.-** Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.
>
> **ARTÍCULO 12.-** Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción. (…)"[20].

Sin embargo, también existen legislaciones que además de los estándares de incorporación procesal, exigen la presencia de peritos especializados para permitir la comprensión del contenido de la prueba digital en el proceso. Verbigracia, en el caso de la normatividad española, la Ley de Enjuiciamiento Civil[21] rescata los estándares de integridad y autenticidad, además del principio de licitud en la obtención de la prueba; empero, añaden la calificación pericial de un técnico informático para **aclarar** –obligatoriamente– el contenido de la prueba digital a favor de las partes y el juzgador; en términos del artículo 346 de la Ley de Enjuiciamiento Civil. No obstante lo anterior, el diverso 326, inciso 3 de la propia Ley, recuerda que la eficacia de un documento electrónico dependerá de la integridad con la que se presenten, al tenor del artículo tercero de la Ley de Firma Electrónica (documentos privados firmados electrónica-

---

[20] ARGENTINA. CÁMARA DE DIPUTADOS DE LA NACIÓN DE ARGENTINA. *Firma Digital. Ley 25.506.* Promulgada el 11 de diciembre de 2001. Argentina. Visible el 04 de diciembre de 2017 a través del vínculo http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[21] JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 1/2000*. 7 de enero, de Enjuiciamiento Civil. BOE número 7, de 8 de enero de 2000. Visto a través del Boletín Oficial del Estado en https://boe.es/buscar/act.php?id=BOE-A-2000-323

mente)[22]. Consideraciones que podrían permitir aducir a la fortaleza de los documentos electrónicos en el proceso, aún sin la presencia de un experto informático, en tanto se acredite la autenticación de los mismos.

Sobre el particular y la autenticación de documentos que incluyen firma electrónica, el artículo 342 apartado 6° del Código de Procedimientos de Chile, prescribe que se considerará como instrumento público en juicio a los documentos electrónicos suscritos mediante firma electrónica avanzada; precepto que se debe leer armónicamente con los artículos 4° y 5° de la Ley 19,799 *Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.* En ese tenor, la jurisdicción chilena permite la impugnación y ofrecimiento de prueba complementaria de autenticidad, como una carga procesal adicional al impugnante, no como un estándar de admisibilidad de la prueba, tal como ocurre en el caso español; lo que a mi humilde parecer es la ruta procesal adecuada para desvirtuar el alcance o valor probatorio de una prueba electrónica o digital, que se emitió con los requisitos que exige la ley[23].

El caso mexicano es paradigmáticamente ortodoxo en materia de incorporación de pruebas electrónicas y digitales. Verbigracia, en el caso del contenido de las páginas web (o electrónicas), nuestro Poder Judicial de la Federación estima que éstas se deben incorporar al proceso como "hecho notorio" y no como **prueba digital**, que sería la calificación jurídica adecuada. A saber, el precedente jurisdiccional dicta:

> **"PÁGINAS WEB O ELECTRÓNICAS. SU CONTENIDO ES UN HECHO NOTORIO Y SUSCEPTIBLE DE SER VALORADO EN UNA DECISIÓN JUDICIAL.**
>
> Los datos publicados en documentos o páginas situados en redes informáticas constituyen un hecho notorio por formar parte del conocimiento público... Por tanto, el contenido de una página de Internet que refleja hechos propios de una de las partes en cualquier juicio, puede ser tomado como prueba plena..."[24]

---

[22] JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 59/ 2003*. 19 de diciembre, de firma electronica. BOE número 304, de 20 de diciembre de 2003, páginas 45329 a 45343. Visto a través del Boletín Oficial del Estado en https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

[23] MINISTERIO DE ECONOMÍA. *Norma Ley 20217. Modifica el código de Procedimiento Civil y la Ley número 197999 sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas.* 12 de noviembre de 2007, Chile. Visto a través de la Biblioteca del Congreso Nacional de Chile en https://www.leychile.cl/Navegar?idNorma=266348

[24] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN (México). *Páginas Web o electrónicas. Su contenido es un hecho notorio y susceptible de ser valorado en una decisión judicial.*

Algunos lectores podrían afirmar que el criterio que invocó no resulta perjudicial para el entendimiento y comprensión del valor probatorio de un documento digital, sin embargo, la notoriedad, accesibilidad, aceptación e imparcialidad del conocimiento contenido en la página *sub judice* pudiere desaparecer antes de la incorporación al proceso; es decir, existe peligro real de que la página desaparezca, así como su contenido y aquélla prueba que resultaba idónea para acreditar las pretensiones del oferente. Hipótesis jurídica que permite acreditar el temor procesal de la desnaturalización de la prueba electrónica o digital, no sólo por restarle merito probatorio, sino por el riesgo que implica para llevarle "íntegramente" hasta su valoración, dentro de la sentencia.

6. Licitud en la obtención y conservación forense de la prueba electrónica y digital

Dentro de las complicaciones en materia de ofrecimiento de pruebas electrónicas y digitales, es la obtención lícita y conversación forense de las mismas hasta el momento de su valoración. En primer término, es imperante distinguir el principio de licitud en la obtención de la prueba, como una categoría del derecho procesal probatorio análogo, en el entendido que cualquier medio de convicción cuya fuente atente contra un derecho fundamental, como lo son la vida privada, la intimidad y las comunicaciones que se originan en las esferas más sensibles del ser humano, deben seguir las reglas del debido proceso. Así lo sostiene el Doctor Hernando Devis Echandía, al precisar el alcance del principio de licitud de la prueba y del respeto a la persona humana, como el límite u oposición a procedimientos ilícitos para la obtención de la prueba, bajo pena de considerarle sin valor jurídico[25]. Sin embargo, las cargas garantistas del debido proceso no sólo dependen del correcto protocolo procesal o adjetivo que se siga en la incorporación de las pruebas *tecnológicas*, además deben vigilar la legal conservación forense que se aplique sobre ellas. Desafortunadamente, existen pocos protocolos normativos que dicten reglas sobre la segunda hipótesis. Procesalmente, es importante comprender que la indebida intervención de equipos que contengan comunicaciones privadas y mensajes de datos de relevancia para el proceso, genera la ilicitud en las pruebas obtenidas –además del "envenamiento" del proceso–, sin embargo, las consecuencias de derecho no

---

Tribunales Colegiados de Circuito. Tesis I.3°.C.35K. Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 26, Noviembre de 2013, Tomo II, p. 1373. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de diciembre de 2017.

25 DEVIS ECHANDÍA, Hernando D. *Teoría General de la Prueba Judicial.* Tomo I. Sexta edición. Colombia, 2012. Pontificia Universidad Javeriana, Bogotá, Facultad de Ciencias Jurídicas. Editorial Temis, p. 127.

sólo se limitan a su debida incorporación, sino a la debida cadena de custodia en la obtención éstas. Verbigracia, en el caso *Uzun vs Alemania*, el Tribunal Europeo de Derechos Humanos consideró que la vigilancia del demandante a través de *GPS*, así como el tratamiento y la utilización de los datos obtenidos por ese medio, contravenían el artículo 8° de la Convención Europea de Derechos Humanos[26].

El Departamento de Seguridad Nacional de los Estados Unidos de América fue consciente de esta complicación y no sólo se detuvo a crear dependencias que se encargaran de regular el ciberespacio, sino que permitió el perfeccionamiento de buenas prácticas para la cadena de custodia informática que respetaran derechos fundamentales y garantías constitucionales, para brindar uno de los sistemas de conservación forense más eficientes del orbe. En el año 2007, la División de Investigaciones Criminales del Servicio Secreto de los Estados Unidos de América, publicó el documento intitulado *Best Practices for Seizing Electronic Evidence v.3. A Pocket Guide por First Responders*[27], derivado de la política de ciberseguridad sostenida por el Departamento *Homeland Security*. Éste surgió como una guía legal para reforzar al personal con mejores prácticas para la conservación de evidencia electrónica derivado de crímenes tecnológicos. La guía actualmente cuenta con una versión "4.2" y fija las reglas puntuales para asegurar una cadena de custodia transparente y brindar una adecuada conservación forense. Con la finalidad de evitar reproducir todo el documento, únicamente traduciré y fijaré las "Reglas de Oro" del documento, así como algunas sugerencias del mismo, respecto a principios que deben seguir los "Primo-respondientes" cuando enfrentan un delito en que intervinieron computadoras o tecnología electrónica, a saber:

Reglas de Oro

1. Siempre que sea posible, es mejor contar con un Perito entrenado Informático o Analista, para recabar la evidencia electrónica;
2. Contar con los fundamentos legales para conservar la computadora (hardware);

---

[26] HUBER, Florian. *Tecnologías de Información y Comunicación, Protección de Datos y Derechos Humanos en la Jurisprudencia del Tribunal Europeo de Derechos Humanos. Derecho y TIC, Vertinentes Actuales.* México, 2016. Evelyn Téllez Carvajal, Coordinadora. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas y Centro de Investigaciones e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Primera edición, p. 79.

[27] U.S.SECRETE SERVICE *Best Practices for Seizing Electronic Evidence v.3. A Pocket Guide For First Responders.* US Dept of Homeland Security. 2007. http://www.listcrime.com/BestPracticesforSeizingElectronicEvidence.pdf

3. Si existen dudas razonables para creer que una computadora se involucra en una investigación criminal, esta debe preservarse como evidencia;
4. Si la computadora se encuentra apagada, debe permanecer apagada. No tratar de encenderla;
5. Si la computadora se encuentra encendida y no existe un perito disponible en la escena, debe asegurar adecuada la computadora y preservar la evidencia;
6. Si tiene creencias razonables de que la computadora destruye evidencia, debe apagar la misma inmediatamente desde su centro de poder;
7. En todos los escenarios, se debe documentar la localización y estado de la computadora, incluido los medios electrónicos que incluya;
8. En todos los escenarios, se debe fotografiar la computadora, su ubicación y cualquier mecanismo adjunto. Se debe fotografiar la pantalla; y
9. Considerar la protección legal de documentos contenidos en el equipo (datos personales, información confidencial).

Por lo que refiere a la conversación de dispositivos que se encuentran conectados a una red, el Manual indica que se deberá recolectar no sólo el equipo, sino los datos relativos a la conexión, tales como: i) Dirección IP, ii) Puertos abiertos, iii) Conexiones a la red activas, y iv) Cualquier dato que estime el perito. La identificación de los puertos, así como las conexiones abiertas permitirían la ubicación de personas involucradas en el crimen que se investiga. En términos generales, la "guía de bolsillo" dicta las pautas de una debida cadena de custodia para los primeros respondientes ante un hecho que involucre soportes electrónicos o digitales y hasta ahora, ha permitido que la políticas detrás del *FinCEN* se traduzca en la capacitación activa de todas sus unidades para actuar conforme lo dictan las buenas prácticas en informática forense. Sin embargo, ello no resuelve enteramente lo que podría ocurrir en la web y portales que se pudieran encontrar "colgados" con información ilegal o ilícita, en su totalidad o parcialmente.

En el caso colombiano, los tratadistas Deisy Yanet Acevedo Surmary (Universidad del Externado de Bogotá) y Élber Enrique Gómez Ustaris (Universidad Santo Tomás, Bogotá), realizan un brillante estudio sobre el comportamiento judicial en su país y la interacción que tienen con la Asociación Colombiana de Ingenieros en Sistemas (entidad que fija y establece las normas de procedimiento de investigación frente a documentos electrónicos). Sostienen que el juez no es perito en todas las materias, por lo que para emitir una sentencia justa podrían requerir del consejo de un asesor informático que cuente con habilidades suficientes para conservar la prueba, ayudar a las partes a su incorporación procesal y por último, brindar las reglas básicas para su valoración. Al respecto, el perito emitiría un dictamen que no sólo reconozca la calidad tecnológica de la prueba, sino que éste "certificará" que la misma se obtuvo de

una debida cadena de custodia, e inmediatamente procederá a rendir su opinión crítica en un lenguaje que sea comprensivo para el juzgador, en el cual debe informar cual fue el diseño utilizado en la prueba, la metodología de extracción, la técnica de análisis, el estado del arte en ingeniería forense y las conclusiones del perito. El juez Colombiano que pretenda hacer uso de esta herramienta procesal –el dictamen- podrá acudir a ACIS. El dictamen contendrá datos de relevancia y pertinencia jurídica tales como la fecha de creación, de modificación, tipo de formato, y tamaño del documento electrónico o digital, e igualmente, identificará quién fue su creador y receptor y si fue o no encriptado, lo que permite comprobar la seguridad del mismo[28].

Sobre la conservación forense de un correo electrónico, el Director Nacional de Tecnología de la Información, Santiago Acurio del Pino, brinda un adecuado análisis de la naturaleza del correo digital y recuerda al primer respondiente, que el mensaje/carta se almacena en un servidor del intermediario o prestador del servicio, siendo pocas las ocasiones que el usuario almacena éste en su propio equipo:

> "Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (ISP). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo TCP/IP. Los paquetes pasan por una computadora especial llamada servidor (server) que los fija con una identificación única (Message-ID) posteriormente los sellan con la fecha y hora de recepción (Sello de tiempo)…. Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar. Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada[29]".

---

[28] ACEVEDO, Deysi y GÓMEZ, Élber. *Los documentos electrónicos y su valor probatorio: En procesos de carácter judicial.* IUSTITIA Número 9. Diciembre de 2011. ISSN: 1692-9403.

[29] ACURIO DEL PINO, Santiago. *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0.* Dirección Nacional de Tecnología de la Información. Washington, D.C Organization of American States*, 2011.* https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf. Visto el 04 de abril de 2018.

Empero, la conservación forense de las pruebas *tecnológicas* no puede detener su camino en el aseguramiento de mensajes, equipos o, en su caso, requerir el apoyo de expertos que cuenten con el conocimiento adecuado para preservar la prueba informática; ya que más allá del proceso, las personas involucradas (usuarios) cuentan con herramientas suficientes para lograr la desaparición del indicio digital; así las cosas, el juez de la causa deberá tomar las medidas necesarias para obtener contraseñas y nombres de usuario (en carácter de confidencial) necesarios para evitar que estos pudieren ser utilizados en perjuicio del proceso, única y exclusivamente para los fines que ocupe al juicio.

Conclusiones

1. El concepto de documento en sentido estricto, merece flexibilización en atención de contenido que se fija a través de tecnologías de la información y la comunicación; lo anterior, invita al análisis del concepto de documento en sentido amplio.
2. El documento en sentido amplio es toda representación material destinada e idónea a reproducir una determinada manifestación de pensamiento. Adicional a la categoría de documento análogo, esta visión jurídica permite calificar al documento cibernético dentro de la ciencia jurídica.
3. Los documentos cibernéticos e informáticos, en sentido amplio, permiten la creación, almacenamiento y reproducción de otras categorías de documentos, en sentido estricto: i) Documento Electrónico y ii) Documento Digital.
4. Para la incorporación de un documento cibernético, informático, electrónico o digital en un proceso, se debe acreditar que este cumple con los principios de neutralidad, equivalencia funcional y no discriminación; además, de forma mínima deberá cubrir los estándares/requisitos de autenticación, fiabilidad e integridad.
5. La incorporación procesal de pruebas electrónicas o digitales debe atender a su naturaleza *sui genéris*, por lo que no es permisible exigir mayores requisitos para su desahogo, sobre todo aquellos que pudieren atentar contra la naturaleza de dichas probanzas y que afectaren la eficacia probatoria de las mismas.
6. En materia de conservación forense de pruebas electrónicas o digitales, resulta de vital importancia la capacitación de las fuerzas forenses, sin los cuales, la prueba podría viciarse y resultar inútil para un juicio. La licitud en la obtención de la prueba electrónica o digital atiende a criterios procesales y, en lo particular, a la correcta cadena de custodia que se pudiere aplicar sobre aquella.

Bibliografía

ACEVEDO, Deysi y GÓMEZ, Élber. *Los documentos electrónicos y su valor probatorio: En procesos de carácter judicial.* IUSTITIA Número 9. Diciembre de 2011. ISSN: 1692-9403.

ACURIO DEL PINO, Santiago. *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0.* Dirección Nacional de Tecnología de la Información. *Organization of American States.* Washington, D.C.

BALLINA, Hidalgo. *Derecho Informático.* México, 2013. Flores Editor y Distribuidores. Instituto Internacional del Derecho y el Estado.

BARRIUSO, Carlos. Interacción del Derecho y la Informática. Madrid, España 1996. Editorial Dykinson.

DEVÍS ECHANDÍA, Hernando. *Teoría General de la Prueba Judicial*. Sexta Edición. Tomo I y II. Bogotá. Pontificia Universidad Javeriana, Bogotá, Facultad de Ciencias Jurídicas. 2002.

DICCIONARIO, Black de Leyes.

DICCIONARIO de la Real Academia Española.

HUBER, Florian. *Tecnologías de Información y Comunicación, Protección de Datos y Derechos Humanos en la Jurisprudencia del Tribunal Europeo de Derechos Humanos. Derecho y TIC, Vertinentes Actuales.* México, 2016. Evelyn Téllez Carvajal, Coordinadora. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas y Centro de Investigaciones e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Primera edición.

ONU. CNUDMI. *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUNDMI sobre Comercio Electrónico*. Estados Unidos de América, Nueva York, 1999.

PALLARES, Eduardo. *Diccionario de Derecho Procesal Civil.* Concepto de "documento". Vigésima Octava Edición. México. Editorial Porrúa, 2005.

RIVOLTA, Mercedes. *Construyendo el Estado Nación para el crecimiento y la Equidad. Panel: Gobierno Electrónico: Experiencias en el poder legislativo y judicial*. Cuarto congreso argentino de administración pública. Buenos Aires, Argentina.

Suprema Corte de Justicia de la Nación. Semanario Judicial de la Federación y su Gaceta.

TECHNET, Microsoft. "¿Qué son los medios digitales?" *Microsoft Product Lifecycle*. Contents. Estados Unidos de América, 3 de diciembre de 2012.

TÉLLEZ VALDÉS, Julio. *Derecho Informático*. Cuarta Edición. México. Editorial McGrawhill. 2009.