LEGALIDAD Y CONSTITUCIONALIDAD DE LA EXTRACCIÓN Y FIJACIÓN DE LA EVIDENCIA DIGITAL*

Por Alexander Díaz García[1]

SUMARIO: Introducción. 1. Anuencia previa para accesar los ficheros. 2. Obtención de los ficheros con integridad, confiabilidad, disponibilidad y seguridad. 3. Autenticidad en la obtención de los ficheros con el análisis pericial. 4. Obtención de los ficheros con las solemnidades. Corolario.

RESUMEN: Este documento refiere los parámetros de legalidad aplicables en el procesamiento de la prueba digital, abonando con ello a la teoría general de la prueba luego que, cuando se trata de procesar evidencias digitales, los parámetros están determinados básicamente por aquellos lineamientos establecidos en 1966 por el artículo 9 de la Ley Modelo sobre el Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional –"UNCITRAL" por sus siglas en inglés-: "*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*". No obstante, además de describirlos, el autor estipula detalles que otorgan precisión a su procesamiento y valoración.

PALABRAS CLAVE: Prueba digital, Evidencia digital, Extracción de la prueba digital, Valor probatorio de la prueba digital. Valor probatorio del documento electrónico. Cadena de custodia. Elemento de pertenencia. Elemento de Integridad. Admisibilidad de la evidencia digital.

ABSTRACT: *This document refers to the parameters of law applicable in the processing of digital proof, thereby paying the general theory of proof then that when it comes to processing digital evidence, the parameters are determined primarily by those guidelines established in 1966 by Article 9 of the Model Law on Electronic Commerce of the United Nations Commission for International Trade Law - "UNCITRAL" for its acronym in English: "*Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor*". However, in addition to describing the author provides details that give precision processing and evaluation.*

* Artículo publicado previamente como "Notas sobre la prueba digital" el 11 de noviembre de 2012, en el sitio web español *http://es.scribd.com/doc/112827112/Notas-sobre-la-prueba-digital-Alexander-Diaz-Garcia-V-2* .

[1] Juez Segundo de Control de Garantías Constitucionales en Rovira Tolima, Colombia; Especialista en Nuevas Tecnologías y Protección de Datos; y Autor de la Ley 1273 de 2009 (Ley de Delitos Informáticos en Colombia) e-mail alediaga@yahoo.com

KEY WORDS: *Digital proof. Digital evidence. Removing the digital proof. Probative value of digital evidence. Probative value of electronic documents. Chain of custody. Element of belonging. Integrity Element. Admissibility of digital evidence.*

INTRODUCCIÓN

Se me pregunta con frecuencia sobre ¿qué es la extracción y fijación legal de la prueba digital? y les respondo siempre lo que expongo en mis clases y conferencias: es el ejercicio que el primer respondiente (policía judicial o no) tiene que realizar ante la posibilidad de vulneración de la información.

No cabe duda que los medios de comunicación nos han enseñado cómo erran algunos funcionarios en el procedimiento de extracción. Sabemos por mandato legal que son elementos materiales de prueba todos los objetos (sólidos, líquidos o gaseosos) que pueden servir para la determinación de la verdad durante la investigación, es un medio de prueba real y tangible (que se puede ver, tocar, oler, pesar o medir) para que tengan valor probatorio deben ser debidamente recolectados, protegidos, embalados, rotulados, transportados y entregados al funcionario competente, mejorando la cadena de custodia[2], con base a esta premisa tenemos que dividir el tema en varios subtemas y lo haremos de la siguiente manera:

1. ANUENCIA PREVIA PARA ACCESAR LOS FICHEROS

Con base en el contenido del artículo 250-3 de la Constitución Nacional, debemos contar siempre con la anuencia previa del Juez de Control de Garantías Constitucionales, para cuando: "***En caso de requerirse medidas adicionales que impliquen afectación de derechos fundamentales,…***" y ello implica entonces el accesar a los ficheros encontrados en los de almacenamientos masivos electrónicos incautados o hallados; primero porque no se sabe qué clase de contenidos vamos a encontrar y segundo que una vez vulnerado el derecho fundamental (Vg. datos sensibles) y humano el de la intimidad, no hay forma de resarcir (rehabilitarlo, teoría de la almohada de plumas)[3] el daño al revisarse una información que no le interesa a la investigación, como son los datos sensibles (generando por lo pronto la responsabilidad Estatal).

---

[2] El Dr. Santiago Acurio Del Pino, Profesor de la Pontificia Universidad Católica del Ecuador sugiere puntualizar "(*si* –NdelA) *la evidencia es la materia que usamos para persuadir al tribunal o al juez de la verdad o la falsedad de un hecho que está siendo controvertido en un juicio, son entonces las normas procesales y las reglas del debido proceso las que informarán al juez o al tribunal qué evidencias son relevantes y admisibles dentro de un proceso judicial y cuáles no lo son.". Asimismo señala a quien se interese por "establecer las bases para la admisibilidad de la evidencia digital", que recuerde que al introducir sus pruebas "se enfrenta a la clásica pregunta … «Cómo sabe usted y le consta que la evidencia no fue alterada»"*

[3] Como en el cuento "El almohadón de plumas", de Horacio Quiroga, donde el daño oculto conduce a la muerte.

2. OBTENCIÓN DE LOS FICHEROS CON INTEGRIDAD, CONFIABILIDAD, DISPONIBILIDAD Y SEGURIDAD

También he observado lamentablemente que algunos especialistas en algunos Distritos Judiciales de Colombia, no se si por ignorancia o falta de diligencia, han ordenado la aducción de la evidencia con la simple informalidad de la impresión en soporte de papel, olvidando que el documento electrónico –y en especial los correos electrónicos–, tienen unos atributos que no podemos pasar por alto.[4] Tales rasgos son:

La integridad: Recordemos que es la garantía de que el documento está incólume en su contenido, esto es, que no ha sido alterado, modificado. Recordemos que modificado no sólo quiere decir aumento de contenidos en textos o imágenes, sino de bits originales, que son los espacios en blanco no usados (el simple correr del cursor en un espacio en blanco, se modifica el documento electrónico), porque dicho espacio recorrido aumenta el peso original estampado en los metadatos.

Confiabilidad: Se determinará de acuerdo con los fines para los cuales la información fue generada y todas las circunstancias relevantes del caso, como la forma en la que se haya generado, archivado, comunicado y conservado la integridad de la información.

Disponibilidad: Se entiende que sea accesible para una posterior consulta.

Seguridad: Que el documento sea conservado en el formato que se haya generado, enviado o recibido, o en algún formato que permita demostrar que se reproduce la misma información, generada, enviada o recibida.

3. AUTENTICIDAD EN LA OBTENCIÓN DE LOS FICHEROS CON EL ANÁLISIS PERICIAL

Ahora bien, pensamos que si un juez autoriza simplemente una impresión en soporte papel del contenido de un correo o documento electrónico sin que se haya previamente establecido el origen del mismo, su autenticidad, esto es, que el autor realmente es quien afirma ser, su integridad y que el formato usado por el receptor es el mismo que uso el emisor; subsiste una incertidumbre completa sobre la autenticidad del documento.

[4] Que en el caso de la realidad jurídica mexicana, son especificados en el artículo 210-A del Código Federal de Procedimientos Civiles de esa nación, que es dónde se establece, primero, que "Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas"; y segundo que: "Cuando la ley (o «Cuando el mandato judicial…» –en una interpretación extensiva del autor-) requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta".

El origen se determina mediante el direccionamiento de encabezados IP;[5] La autenticidad se determina confirmando que la dirección IP desde donde se emitió, fue asignada por el ISP[6] a una persona determinada.[7] Que el autor del correo sea quien afirma ser es algo de lo que puede dar fe la empresa operadora del correo. La integridad con la que se comprueba que el documento no ha sido modificado, así como que el formato usado tanto por el emisor como por el receptor es el mismo, todos estos son atributos que sólo pueden ser suministrados cuando se le ha hecho un estudio forense al documento.

Respecto del examen forense requerido, cabe anotar como elementos para construir la admisibilidad de la evidencia digital, los referidos por el Dr. Santiago Acurio Del Pino:

> "1. Elemento de Pertenencia de la evidencia digital. El Estado debe establecer que en el equipo informático donde se encontró la evidencia digital (mensaje de datos), es el equipo informático del sospechoso o imputado, más allá de toda duda razonable.
>
> "2. Elemento de integridad de la evidencia digital. El Estado debe establecer que el mensaje de datos descubierto dentro del equipo informático del sospechoso o el imputado fue guardado o almacenado originalmente en dicho equipo, más allá de cualquier duda razonable de que alguna otra persona lo plantó ahí o que la prueba fue creada por el equipo utilizado por el perito-investigador en el curso de su trabajo.
>
> "3. Elemento de autenticación de la evidencia digital. La autenticación en base a estos dos enunciados requiere del empleo de una función Hash, que tiene la misma funcionalidad que una firma electrónica pues se presenta como un valor numérico de tamaño fijo, que se convierten en una verdadera huella digital del mensaje de datos, pues para autenticar la evidencia obtenida, se deben comparar los valores Hash obtenidos de los mensajes de datos encontrados en el equipo informático examinado por el perito, con los obtenidos dentro de la etapa del juicio, luego que si los valores Hash son idénticos, entonces será admisible

[5] IP.- Protocolo de Internet. Gmail no envía el IP publico en sus cabeceras, Hotmail, Yahoo si lo hacen y en este caso pareciera existir esta limitante, no obstante, para lograr el direccionamiento de encabezados IP de Gmail, es simplemente abrir el correo y en la pestaña superior derecha, junto al ícono que señala respuesta del mensaje, se puede pinchar y lograr un menú que dice entre otras cosas: "MOSTRAR ORIGINAL", al elegirlo te reporta la dirección IP de tu emisor. En Colombia he logrado que los Fiscales Delegados (mediante acción de inconstitucionalidad ante la Corte Constitucional de algunos artículos del Código de Procedimiento Penal), soliciten al Juez de Control de Garantías Constitucionales, anuencia previa para la apertura de los ficheros de los ISP para establecer a quien le corresponda esa IP y más si ésta es dinámica. Por otra parte,

[6] ISP.- Proveedor de Servicios de Internet.

[7] En el caso del Juicio en Línea mexicano son las partes, en principio quienes tienen que requerir que los análisis periciales constaten, además de lo previsto en el artículo 210-A del Código Federal de Procedimientos Civiles de esa nación, "que la dirección IP desde donde se emitió, fue asignada por el ISP a una persona determinada", entre otros.

como prueba ese o esos mensajes de datos, luego que estos códigos de integridad son como una huella digital informática, la cual es de difícil alteración o modificación.

"En este caso la aplicación de la cadena de custodia, implica una vinculación de tipo físico, y otra de tipo electrónico derivada del elemento de integridad generado por la llamada función Hash y un sellado de tiempo al mensaje de datos que sirve como evidencia.

"En conclusión, y a fin de evitar que la evidencia digital sea inadmisible en un proceso judicial, el perito forense debe adoptar los procedimientos necesarios para que todos los mensajes de datos que sean relevantes para la investigación, y la información contenida en los dispositivos de almacenamiento encontrados en la escena del delito, deben tener su código de integridad lo más rápido posible."

4. OBTENCIÓN DE LOS FICHEROS CON LAS SOLEMNIDADES

Un documento que no ha acreditado su autenticidad y menos los otros atributos arriba citados, deben ser excluidos tal como lo señala el artículo 29 inciso final de la Constitución Nacional, pues es un documento que se ha arrimado sin las solemnidades que para esta clase de evidencia se exige para acreditar sus valores de apta,[8] constituyéndose muy posiblemente en un documento espurio. Finalmente no podemos descartar un origen ilegítimo del documento, como puede ser un acceso ilegal a una cuenta de correo, una interceptación ilegal de correspondencia o de redes, conductas que constituyen delitos informáticos en Colombia.

COROLARIO

Finalmente quiero recordarles que por su esencia, la evidencia digital como correos electrónicos, log's de sistemas,[9] mensajes de texto, etc. son documentos muy vulnerables si no son conservados técnicamente. Al ser admitidos por algunos Jueces o Magistrados de la República sin mayores elucubraciones (formalidades), permitiendo simplemente

[8] Las formalidades requeridas para la aportación de pruebas en formato electrónico en el caso del Juicio en Línea del Tribunal Federal de Justicia Fiscal y Administrativa mexicano se establecen primordialmente en los artículos 58-K y 58-L de la Ley Federal de Procedimiento Contencioso Administrativo, independientemente de lo dispuesto en otros artículos del mismo ordenamiento (arts. 14, 15, 20, 40 al 46 y 58-D) y de la aplicación supletoria en su caso del artículo 210-A del Código Federal de Procedimientos Civiles de esa nación.

[9] Un log es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados. Tal vez su uso más inmediato sería el log de accesos al servidor web, que analizado da información del tráfico de nuestro sitio. Cualquier servidor web dispone de un log con los accesos, pero además, suelen disponer de otros log, por ejemplo, de errores. Los sistemas operativos también suelen trabajar con logs, por ejemplo para guardar incidencias, errores, accesos de usuarios, etc.

que se junten impresiones en soporte papel al expediente, pensamos que en un incidente procesal como una tacha de falsedad, no se podrá verificar técnicamente aspectos tan relevantes como: cuándo se envió, quién lo emitió, cuándo se creó, cómo se obtuvo, qué formato se usó y si no se realizó ningún trabajo de edición. Con el simple soporte papel no habrá forma que establezcamos dichos atributos propios del documento, pues sólo tendremos en nuestras manos un simple mensaje de datos el que pudo haber sido editado previamente a la impresión. Si ello continúa y lo permitimos, podrá presentarse que cualquier sujeto procesal pueda dolosamente entregar un correo falso como prueba, y su contraparte no podrá desestimarlo, porque se le dejará sin armas técnicas, para controvertirla, lo que implicaría pasar por alto el contenido de la Ley 527 de 1999[10] y en consecuencia se le violaría el debido proceso a la parte afectada.

[10] El 18 de agosto de 1999 fue expedida en Colombia la Ley 527 de 1999 (Ley de Comercio Electrónico), por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.