TELEFONOS CELLARES, NUEVO RETO PROBATORIO.

Andrés GUZMAN CABALLERO. [1]
andres@adalid.com

En Colombia, existen más teléfonos celulares que personas, somos alrededor de 50´000.000 millones de Colombianos, pero hay alrededor de 57´000.000. millones, de conformidad con el informe de Mintic, del segundo semestre de 2016, así las comunicaciones, recuerdos, mensajes, notas, navegaciones, búsquedas, recorridos, ubicaciones, entre otra importante información, queda registrada en estos equipos, lo que constituye sin duda un gran reto en materia técnica y legal, pues debemos adaptar nuestros procedimientos judiciales a la tecnología actual, sin desconocer que en materia probatoria Colombia tiene varios avances, como la ley 527 de 1999, los decretos que la reglamentan y algunas sentencias que la explica.

ASPECTOS LEY 527 DE 1999 – VALOR PROBATORIO A LOS MENSAJES DE DATOS DE TELEFONOS CELULARES (EVIDENCIA DIGITAL) [2]

Ley colombiana que da valor probatorio al mensaje de datos, esta norma exige que se cumplan varios requisitos para un archivo digital tenga validez jurídica, entre los principios tenemos: 1. Autenticidad, que el autor de la evidencia sea identificable 2. Integridad, que los datos recolectados no sufran alteraciones o modificaciones después de ser asegurados, 3. Confidencialidad, que los datos no estén desprotegidos 4. Preservación en el tiempo, que la evidencia recolectada y/o analizada puede consultarse nuevamente sin límite de tiempo. 5. Originalidad, que los datos estén en su formato original y este se proteja. Entre otras disposiciones.

De conformidad la Corte Constitucional Colombiana, estableció de forma clara, los requisitos de validez jurídica de los mensajes de datos, o evidencias digitales dejando claro, que se deberán tener en cuenta lo preceptuado en los Art. 6, 7 y 8 de la ley 527 de 199 así:

> *Conforme a lo anterior, el artículo 6 de Ley 527 de 1999 estableció que en todos aquellos casos en los cuales una norma jurídica requiera que la información conste por escrito, el requisito quedará satisfecho con un mensaje de datos, si la respectiva información es accesible para su posterior consulta. Por su parte, el artículo 7 previó que cuando se exija la firma del correspondiente documento, la*

[1] Abogado especializado en derecho y tecnología, perito informático certificado internacionalmente en cibercrimen, e-evidence, profesor de pruebas técnicas, evidencias digitales, delitos de alta tecnología, en varias Universidades en el mundo.

[2] *Congreso de la República de Colombia (1999). Ley 527, disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.htm*

exigencia se entenderá cumplida si se utiliza un método que permita identificar al iniciador del mensaje y determinar que el contenido cuenta con su aprobación, y si es confiable y apropiado para el propósito en virtud del cual el mensaje fue generado o comunicado.

Y, a la luz del artículo 8 ídem, en todos los supuestos en los cuales la ley imponga que la información sea presentada y conservada en su forma original, esta exigencia quedará llevada cabo con un mensaje de datos, siempre que obre alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma, y además, si de requerirse su presentación, puede ser efectivamente exhibida.[3]

Adicionalmente los criterios de validez Jurídica, la Corte Suprema de Justicia, estableció los criterios que se han de tener para validar su fuerza probatoria, de conformidad con el Art. 11 de la ley 527 de 1999, de forma general basado en su integralidad, inalterabilidad, rastreabilidad, recuperabilidad, y conservación así:

> 4.1.2 Para determinar la fuerza probatoria del mensaje de datos, el artículo 11 de la Ley 527, señala, como ya se pusiera de presente, que deben atenderse las reglas de la sana crítica, así como la confiabilidad que ofrezca la forma como se haya *generado, archivado o comunicado* el mensaje, la confiabilidad de la forma en que se hubiere conservado la *integridad* de la información, la forma como se identifique a su iniciador, y cualquier otro factor relevante.
>
> La **integralidad** de la información tiene que ver con que el texto del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como "sellamiento" del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el

[3] Sentencia C-604-16

> mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo. Incluso, la tecnología actual permite al emisor establecer si el receptor abrió el buzón de correo electrónico y presumiblemente leyó el mensaje.
>
> Esa característica guarda una estrecha relación con la "**inalterabilidad"**, requisito que demanda que el documento generado por primera vez en su forma definitiva no sea modificado, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, tales como la criptografía y las firmas digitales.
>
> Otros aspectos importantes son el de la **"rastreabilidad**" del mensaje de datos que consiste en la posibilidad de acudir a la fuente original de creación o almacenamiento del mismo con miras a verificar su originalidad y su autenticidad. La **"recuperabilidad**", o sea la condición física por cuya virtud debe permanecer accesible para ulteriores consultas; y la **"conservación**", pues de ella depende la perduración del instrumento en el tiempo, siendo necesario prevenir su pérdida, ya sea por el deterioro de los soportes informáticos en que fue almacenado, o por la destrucción ocasionada por "virus informáticos" o cualquier otro dispositivo o programa ideado para destruir los bancos de datos informáticos. Una óptima conservación de la información puede lograrse mediante la aplicación de protocolos de extracción y copia, como también con un adecuado manejo de las reglas de cadena y custodia.

(sentencia del 16 de diciembre de 2010, con ponencia del Magistrado Pedro Octavio Munar en el radicado 11001311000520041007401)

En materia penal los documentos electrónicos, están regulados por la citada ley 527 de 1999, en la ley 600 de 2000, por virtud del Art. 23, que remite directamente al ordenamiento procesal civil, que fue integrado por el Art. 10 de la ley 527 de 1999, de la misma forma por el Art. 244 del código general del Proceso remite por definición "mensaje de datos" a la ley 527; así mismo la ley 906 de 2004 establece

en el Art. 275 literal G) la aplicación de los criterios establecidos en la citada ley 527 de 1999, en los elementos materiales probatorios.

NORMAS TECNICAS A TENER EN CUENTA, PARA ANALISIS FORENSE DE TELEFONOS CELULARES.

ISO/IEC 27037 DE 2012 - INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDANCE FOR IDENTIFICATION, COLLECTION, ACQUISITION, AND PRESERVATION OF DIGITAL EVIDENCE [4]

Esta norma internacional proporciona pautas para actividades específicas en el manejo de la evidencia digital, las cuales se refieren a procesos relacionados con la identificación, recolección, consolidación y preservación de evidencia digital. Estas metodologías están diseñadas para mantener la integridad de la evidencia digital a través de la aplicación de procedimientos aceptados por la comunidad técnico-científica, que permita la admisibilidad de la prueba en escenarios legales en cualquier estadio del derecho. Esta norma Internacional pretende orientar a las personas responsables de la identificación, recolección, aseguramiento y preservación de la evidencia digital, dando recomendaciones para los primeros respondientes en la recolección de la evidencia, especialistas en la recolección de la evidencia digital, especialistas de respuesta a incidentes, grupos de investigación criminal, administradores de laboratorios forenses y demás profesionales a fines.

ISO/IEC 27042 DE 2015 - INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDELINES FOR THE ANALYSIS AND INTERPRETATION OF DIGITAL EVIDENCE [5]

Esta norma internacional proporciona principios y orientación para el análisis e interpretación de evidencia digital, para garantizar: continuidad, validez, reproducibilidad y repetibilidad. Provee una lista de mejores prácticas para la selección, el diseño y la implementación de procesos de análisis y registro de la información suficiente para permitir que estos procesos sean sometidos a un control independiente cuando sea necesario. También proporciona orientación sobre los mecanismos apropiados para demostrar la aptitud y la competencia de los expertos que intervienen en el análisis. Esta norma internacional proporciona un marco común, para los elementos de análisis y de interpretación de manejo de incidentes de seguridad de sistemas de

---

[4] *ISO/IEC 27037:2012, Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence, disponible en http://www.iso.org/iso/catalogue_detail?csnumber=44381*

[5] *ISO/IEC 27042:2015 Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence, disponible en http://www.iso.org/iso/catalogue_detail.htm?csnumber=44406*

información, que pueden ser utilizados para ayudar en la aplicación de nuevos métodos y proporcionar un estándar común mínimo para las pruebas digitales recolectadas dentro del marca de una investigación.

NJ 199408 - FORENSIC EXAMINATION OF DIGITAL EVIDENCE, A GUIDE FOR LAW ENFORCEMENT, U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAM, NATIONAL INSTITUTE OF JUSTICE[6]

Esta guía está desarrollada con el propósito de estandarizar buenas prácticas frente a la administración de evidencia digital; brinda un marco de situaciones más comunes encontradas durante el examen de evidencia digital. Pueda ser utilizada como ayuda para el desarrollo de políticas y procedimientos, siguiendo los siguientes principios forenses:

- Las medidas adoptadas para asegurar y reunir pruebas digitales no deben afectar a la integridad de esa evidencia.
- Las personas que realicen el examen de la evidencia digital deben ser capacitadas y tener competencias en la materia.
- Actividades relacionadas con la incautación, el examen, el almacenamiento o la transferencia de la evidencia digital, deben ser documentadas, preservadas, y estar disponibles para su revisión.
- A través de todo esto, el examinador debe ser consciente de la necesidad de realizar un examen preciso e imparcial sobre la evidencia digital.

DOCUMENTACIÓN FISCALÍA GENERAL DE LA NACIÓN - GUÍA INTERNA DE INFORMÁTICA FORENSE FGN-41300-G-10

La Fiscalía General de la Nación ha desarrollado documentos dentro de sus sistema de gestión de calidad, en donde explican y desarrollan los procedimientos y actividades que debe aplicar la Policía Judicial, frente al hallazgo, recaudo y aseguramiento de las evidencias en el lugar de la escena, por ende, y teniendo en cuenta que a través de esta entidad se regula todos los temas relacionados con cadena de custodia para Colombia, de toma como referente todos aquellos procedimientos que hablen sobre el recaudo de evidencia digital, y para ello se hace referencia al documento denominado, ***Guía de Delitos Informáticos FGN-41300-G-10***, en donde se documentan todas aquellas actividades que deben desarrollar los funcionarios de las Unidad y/o Grupos de Informática Forense frente al hallazgo, identificación, obtención, preservación, análisis y presentación de

[6] *NJ 199408, Forensic examination of digital evidence: A Guide for Law Enforcemen, U.S. Department of Justice, Office of Justice Program, National Institute of Justice, John Ashcroft. U.S. Dep. of Justice, Apr. 2004*

la información y/o datos existente en medios de almacenamiento u otros medios tecnológicos, como apoyo a las investigaciones Judiciales, de tal manera que se realice un adecuado recaudo y análisis de la mismas y así estas no pierdan su valor probatorio.

Particularmente las actividades realizadas enunciadas, se enmarcan dentro de la ciencia de la INFORMÁTICA FORENSE, que tiene como propósito la adecuada recolección, embalaje, custodia, transporte, análisis y presentación de evidencia digital, velando siempre por la protección de las características de integridad, confidencialidad, disponibilidad, no repudio, mismidad, autenticidad y trazabilidad sobre la información recaudada (conforme a los preceptos de la Ley 527/99 Art. 6 al Art. 11), así como también de los contenedores en donde se obtienen las correspondientes imágenes forenses, así se tiene la plena certeza de que la imagen forense es otro original, esto en razón a que los datos contenidos en ella son adquisiciones exactas a nivel de bits, esto es comprobable mediante la extracción de las correspondientes huellas digitales HASH **(cadena de 32 caracteres hexadecimales para MD5 y 40 caracteres hexadecimales para SHA1)** que son considerados como identificadores únicos e inequívocos de un archivo y/o imagen forense, esto se logra mediante procedimientos algoritmo-matemáticos de reducción criptográfica.