

Dr. José Luis Tamayo R.

SENTENCIA SP248-2025: ¿CORRECTA VALORACIÓN PROBATORIA?

Artículo jurídico de opinión

Marzo 2025

LA SENTENCIA SP248-2025: ¿CORRECTA VALORACIÓN DE LA EVIDENCIA DIGITAL?

Una revisión jurídica sobre la valoración de la evidencia digital
y el quebrantamiento de los principios que rigen su autenticidad

Dr. José Luis Tamayo Rodríguez¹
Marzo 22, 2025

RESUMEN

Este artículo examina críticamente la sentencia SP248-2025 dictada por la Sala Penal de la Corte Suprema de Justicia de Colombia, la cual reconoció la validez probatoria de una evidencia digital --seis fotografías-- obtenida mediante procedimientos que, según se desprende la propia sentencia, no cumplieron con los principios fundamentales de autenticidad digital: *confiabilidad*, *integralidad*, *accesibilidad*, *auditabilidad* y *repetibilidad*. A través de un análisis exhaustivo, se ponen de relieve graves fallas técnicas cometidas por el perito informático, como la omisión del cálculo de los códigos hash de la data original y de las imágenes incriminadoras, así como la indebida intervención de una funcionaria no acreditada en informática forense para extraer unos *pantallazos* que el perito no extrajo durante la realización de su experticia. Se cuestiona que, pese a estas deficiencias, la Sala haya atribuido valor probatorio pleno a las imágenes, sin aplicar con el debido rigor los criterios que ella misma enuncia. El estudio concluye que tales falencias debieron llevar a la desestimación de la prueba, en resguardo de la seguridad jurídica y del debido proceso penal.

1. LA EVIDENCIA DIGITAL Y LOS PRINCIPIOS QUE GARANTIZAN SU AUTENTICIDAD

La Sala Penal de la Corte Suprema de Justicia de Colombia, en su sentencia SP-248-2015 del 12 de febrero (Radicación N° 58275), señaló que la validez de la evidencia digital debe analizarse conforme a criterios esenciales, tales como la *confiabilidad*, *integralidad* e *inalterabilidad*, *accesibilidad*, *auditabilidad* y *repetibilidad*. Sin embargo, la misma sentencia contradice sus propias premisas al momento de evaluar la prueba en cuestión. Veamos.

¹ Abogado binacional, venezolano, nacido en Caracas (1958), egresado de la Universidad Central de Venezuela en 1981, con reválida en México. Doctor en Derecho y profesor de pregrado y postgrado de Derecho penal y procesal penal en la misma Universidad. Exjuez asociado en los Tribunales penales, de primera y segunda instancia, en Caracas (1992-1999). Abogado litigante con cuarenta y tres años de experiencia. Especializado en Derecho Digital y Pruebas electrónicas. Autor de nueve libros y el e-book "*Pruebas Electrónicas y Código hash*" (2024).

a) Confiabilidad: ¿Se utilizaron métodos confiables?

En torno a la *confiabilidad*, se lee textualmente en el fallo:

“i) Confiabilidad: En la forma como se ha generado, extraído, archivado o comunicado el documento, registro, información o mensaje de datos, a partir de procedimientos fiables y acreditados por el área de conocimiento específico. Preferiblemente, por personal capacitado e idóneo en el proceso de recolección y análisis de la evidencia digital.

En este punto, cobran relevancia conceptos como el de imagen forense digital², para lo cual se suele emplear un bloqueador de lecto/escritura o *White Blockers*³, así como programas o *software* para el copiado de la información y la generación de la imagen, que será almacenada en un disco de destino u otro dispositivo de almacenamiento, especialmente destinado a ello”.

¿Se respetó este principio? No.

Si bien el perito extrajo la imagen forense y calculó su hash, **no calculó el hash de la memoria SD** antes de realizar la extracción, lo que impide verificar que la imagen obtenida sea exactamente idéntica a la contenida originalmente en el dispositivo. Tampoco calculó el hash individual de las seis fotografías extraídas y ni siquiera acompañó los pantallazos de esta en su informe o dictamen pericial, pese a que le parecieron **“relevantes”**.

En tal sentido, se lee en el fallo:

“... para argumentar la exclusión, el *ad quem* también incurrió en falso juicio de identidad por tergiversación, pues al auscultar el testimonio del tecnólogo en ingeniería de sistemas, William Antonio Saldarriaga Zúñiga, rendido en sesión de juicio oral del 12 de agosto de 2016, en ningún momento advirió que las imágenes carecieran de valor hash.

En su declaración, dijo haber sido el encargado de extraer la información, como registro de llamadas entrantes, salientes, mensajes, mensajes de voz y, en general, todo lo que contenía, entre otros, el celular en mención.

Explicó su labor de recolección de información, de acuerdo al informe que rindió el 4 de marzo de 2015, desde el momento en que recibió los elementos

² Entendido como el proceso que se lleva a cabo para copiar de manera exacta, sector por sector -bit a bit- un dispositivo de almacenamiento donde se encuentra la información con relevancia probatoria. El cual, difiere del que se realiza cuando, por ejemplo, se copia y guarda un archivo de una carpeta a otra, o en distintos dispositivos. Tomado de:

https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_tecnicos.pdf

³ Dispositivo de hardware, empleado por un experto, para no contaminar la información introduciendo cambios, como modificaciones en la fecha de acceso al dispositivo por analizar. Tomado de: https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_tecnicos.pdf

embalados, su identificación, los procedimientos técnicos empleados, su grado de aceptación científica, el proceso de extracción y los resultados.

Aclaró que no fue posible la recolección de elementos del teléfono Vodafone, ya que tenía un bloqueo por patrón de seguridad y no le fue posible desbloquearlo. No obstante, como el dispositivo electrónico también contaba con una SIM card y una Micro SD de 4GB, en esta encontró **seis fotografías que le parecieron relevantes**, ya que coincidían con las características brindadas por los testigos presenciales del homicida..." (Mías las negrillas y subrayado).

Este inexplicable proceder del perito, de omitir el cálculo del hash de la evidencia original contenida en la memoria SD y de omitir también el cálculo del hash individual de las seis fotografías, pese a que él mismo las consideró "relevantes"; y de ni siquiera haber acompañado a su dictamen los pantallazos de las seis fotos incriminadoras, **anula de plano** cualquier garantía de autenticidad y fiabilidad de la evidencia.

Ello así porque esto implica observar los estándares internacionales contenidos en la Norma ISO/IEC 27037:2012 (citada expresamente en la sentencia de la Sala), que establece las directrices básicas para la obtención y preservación de la evidencia digital, enfatizando la importancia de garantizar la integridad de la evidencia durante todo el proceso, lo que implica que, a tal efecto, el perito ha de calcular el hash de la evidencia digital original o primigenia antes de realizar la imagen forense, y luego calcular el de esta, de forma tal que ambos sean idénticos. Todo este protocolo ha de quedar plasmado en el dictamen pericial.

Es más, en la "Cartilla de Evidencia Digital" de la Rama Judicial del Poder Público de Colombia, citada en tres oportunidades por el fallo en notas a pie de página N°s. 10, 11 y 13 (pp.31, 32 y 33, respectivamente), se subraya la relevancia de los valores hash en la verificación de la **integridad** de las copias de evidencia digital.

Específicamente, cuando hace referencia a las "*Característica técnicas de la evidencia digital y prueba electrónica*" (punto 9.11), indica que al comparar los **valores hash generados desde el original con los de la copia**, los analistas forenses pueden determinar si la copia está bien hecha.

Al efecto, se lee en el punto 9.11.13., página 47, lo siguiente:

“A través de procedimientos forenses el especialista puede generar **duplicados de la evidencia digital**, los cuales mediante un riguroso registro de cadena de custodia pueden garantizar la continuidad del debido cuidado de esta, su **integridad**, confidencialidad y disponibilidad. Los **duplicados de imagen forense**, por ejemplo, ayudan al especialista forense a dividir objetivos específicos con miras a determinar un hecho o acto particular jurídicamente relevante. Sin el duplicado la labor forense podría ser dispendiosa y afectar los tiempos de respuesta que requiere para su cabal cumplimiento de objetivos trazados. Otra perspectiva de la duplicidad de la evidencia digital la encontramos en la posibilidad de que la interacción de una o más personas a través de un medio informático se almacene de manera simultánea en diferentes repositorios susceptibles en todo caso de ser recolectados y aportados como evidencia digital, como ejemplo, existe la posibilidad de disponer de evidencia almacenada localmente en un dispositivo y paralelamente tener un duplicado en la nube disponible para consulta”. (Nuestras las negrillas).

En sintonía con lo anterior, el autor español José Luis Reyes González, en su monografía “*LA PRUEBA PERICIAL DIGITAL Y LA CADENA DE CUSTODIA*”, expresa:

“Desde el punto de vista jurídico, el **clonado** constituye una garantía del juicio de **fiabilidad** en el registro y análisis de los dispositivos y que permite acreditar la mismidad de lo aprehendido, esto es, que lo que se copia es imagen fiel de lo ocupado o intervenido. De este modo, se preserva la fuente original al tiempo que se facilita a los investigadores o peritos trabajar a partir de las copias, ya sin el riesgo de una alteración imprudente o malintencionada. Quedará así garantizada la **mismidad** del dispositivo intervenido y, ante cualquier duda que pueda plantearse en el proceso sobre alteración de la prueba, se podrán llevar a cabo las operaciones de contraste necesarias entre la copia y el original”.⁴ (Nuestras las negrillas).

Y agrega más adelante:

“El **clonado forense** de discos duros se realiza a fin de certificar y mantener la cadena de custodia de las evidencias digitales contenidas en el dispositivo. Ello es fundamental en cualquier proceso judicial ya que, de no hacerse correctamente, los elementos probatorios quedarían **invalidados**. Es deber del perito informático certificar la cadena de custodia, esto es, que las evidencias aprehendidas permanecen inalteradas desde el momento en que son intervenidas, pudiendo certificar su originalidad en cualquier momento posterior a la intervención.

La copia del dispositivo incautado se realizará en otro dispositivo de almacenamiento o fichero de imagen obteniendo la **firma hash** de los bits leídos durante el proceso. Con ello, se obtiene una copia exacta de todo el contenido del disco duro, además de certificar la correspondencia de su contenido con el original mediante la **coincidencia de las firmas con hash**”.⁵ (Nuestras las negrillas).

⁴ Universidad de La Laguna. Anales de la Facultad de Derecho. N° 38. Septiembre 2021, p. 58. San Cristóbal de La Laguna. Isla de Tenerife. Islas Canarias. España.

⁵ *Ibidem*, p. 59.

Ahora bien, en torno a los valores *hash*, agregó el perito informático según se lee en el fallo:

“Al inquirírsele sobre si obtuvo valores *hash* en el proceso de extracción, contestó afirmativamente. Al ser contrainterrogado al respecto, señaló que aun cuando no precisó en su informe el *hash* de las fotografías, esa información reposaba en el disco duro Buffalo, que podía ser consultado.

Incluso, acotó: *‘aquí en esta página 11 aparece al lado de donde dice resultados de la exportación, aparece un nombre que dice hash de hash, listado de archivos exportados, ¿por qué? Porque cuando generamos el hash nos pueden generar 2.000, 3.000 hash de todo, en este caso podríamos hablar de 2.162 hash, líneas, entonces se hace muy dispendioso imprimirlo, entonces a ese hash, a ese archivo se le saca un hash que es el que yo aporé aquí (...) entonces lo que hice fue a ese archivo hash, que podían ser unos dos mil y pico de archivos, le consigné solamente uno y en el que aparece aquí en la página 11 del informe que rendí’⁶.*”.

De lo anterior se sigue que el perito intentó justificar su **crasa omisión** de no haber “*hasheado*” las fotos, argumentando que generó un *hash global* del disco duro Buffalo, pero esto no reemplaza la obligación de calcular los hashes individuales de los archivos extraídos ni el de la memoria SD original antes de realizar la imagen forense como lo aconsejan las buenas prácticas forenses.

La función del *hash* no es sólo garantizar la integridad del conjunto, sino también la integridad de cada archivo **por separado**. ¿Cómo puede verificarse técnicamente si las “selfies” obtenidas de forma empírica y sin soporte técnico especializado, vía pantallazos, son las mismas que se extrajeron de la memoria SD si no hay un *hash* específico de cada una de ellas?

Es como si en una auditoría bancaria, en vez de mostrar los registros individuales de cada transacción, el auditor solo se limitara a presentar un Balance total sin acreditar cada movimiento en detalle. ¿Puede el solo Balance con esas características, tener el suficiente respaldo probatorio para considerarlo una prueba plena? La respuesta es obvia.

De otro lado, en cuanto a la afirmación que hace el perito respecto a que “... *se hace muy dispendioso imprimirlo*”, si bien en informática forense no es obligatorio imprimir los valores *hash*, sí lo es **documentarlos correctamente** en el informe pericial y garantizar su trazabilidad.

⁶ Audiencia de juicio oral del 12 de agosto de 2016. Récord: JHON FREYDER CAICEDO POPO-J3PCE-7652060000020150004400_761113107003_1.wma. Minutos: 00:53:26 a 00:24:20

Si el perito no quería imprimir los 2.162 hashes, al menos debió consignar en su informe el hash de cada foto extraída y, por supuesto, el hash de la evidencia original antes de su intervención. La falta de documentación implica que no hay forma de verificar si la imagen forense que analizó el perito corresponde efectivamente a la evidencia digital contenida en el dispositivo electrónico (memoria SD), ni tampoco si las fotos fueron alteradas, manipuladas o implantadas, que fue la tesis esgrimida por la defensa, aunque, por lo visto, de una manera pura y simple y sin mayores alegatos.

La omisión del perito no es un simple y pueril descuido técnico, sino un **error grave e inexcusable** en la preservación de la cadena de custodia de la evidencia digital, distinta de la cadena de custodia de la evidencia electrónica, como veremos líneas abajo).

Al no calcular ni documentar el hash de la evidencia digital contenida en la memoria SD, ni tampoco los *hashes* individuales de las fotos, el perito comprometió seriamente su *autenticidad, repetibilidad y confiabilidad*, afectando, por ende, su eventual eficacia probatoria.

No obstante lo anterior, la Sala restó importancia a ello, descuidando la trascendental importancia de la cadena de custodia de la evidencia digital, y a renglón seguido expresa:

“Lo reseñado rebate, entonces, dos asertos. Uno, que las fotografías carecieran de valor hash, pues incluso los códigos que se generaron por cada dato, archivo e información recolectada de la SIM Card y la Micro SD fueron, a su vez, autenticados por otro valor hash que los comprende.

Y dos, la afirmación del defensor, como no recurrente, consistente en que aquellas fueron implantadas, pues la acreditación de la debida cadena de custodia y, en especial, del código hash, llevan a deducir que la evidencia digital extraída de dichos dispositivos de almacenamiento no fue alterada durante el procedimiento digital forense ni cuando fueron almacenados en el disco duro de destino -Buffalo S/N 8559922441294 modelo HDPNTU3 color vino tinto- descubierto a la defensa, ya que, de lo contrario, no tendrían el valor hash que respalda la mismidad de la información.

Por tanto, las seis fotografías corresponden íntegramente a las que reposan en la Micro SD, del celular marca Vodafone blanco, hallado en el día y lugar en el que fue ultimado el periodista Édgar Quintero, de manera que **su valor probatorio**, contrario a lo aducido por el Tribunal, **es pleno**”. (Mías las negrillas).

A la luz de lo expresado por la Sala en los párrafos antes transcritos, es preciso destacar lo siguiente:

1. El hecho de que exista un hash general sobre un listado no permite verificar la integridad ni la **inalterabilidad individual** de cada imagen, y mucho menos su autenticidad de manera autónoma.

Si se hubiese implantado una fotografía (como lo afirmó la defensa, aunque de manera empírica y sin fundamento técnico) dentro del conjunto de archivos antes de crear ese listado, su hash también sería incluido, y el hash del archivo global no evidenciaría esa implantación.

Por tanto, no es cierto que esa operación subsane la omisión de calcular los hashes individuales de las fotos extraídas de la Micro SD.

2. La Sala incurre en un **razonamiento circular peligroso**: presume que todo lo contenido en el disco duro Buffalo es auténtico porque el listado general de archivos fue "hasheado".

Pero eso es como decir que un archivo comprimido en .zip con documentos falsificados goza de autenticidad solo porque el .zip tiene un hash. El contenido puede seguir siendo espurio, y el hash general no tiene ningún poder probatorio individual.

3. La propia sentencia exige que se garantice la integridad e inalterabilidad de la evidencia digital. Sin un hash calculado directamente sobre el archivo original de cada fotografía, no es posible probar que esa imagen no fue modificada ni implantada antes de ser impresa o capturada en un "pantallazo".

4. Al pretender que un único hash de un archivo intermedio (el listado) abarca todos los requisitos de autenticidad, la Sala genera una **falsa sensación de seguridad probatoria**, omitiendo estándares internacionales como los de las normas ISO/IEC 27037:2012 y 27042:2015,⁷ que marcan pautas para la creación de imágenes forenses y el cálculo del hash de la evidencia digital original.

⁷ Esta Norma ISO/IEC, no citada expresamente en la sentencia, establece las directrices para analizar la evidencia digital, estableciendo estándares destinados a garantizar su fiabilidad, integridad, transparencia, repetibilidad y reproducibilidad. Todo perito informático debe conocerla y aplicarla en su labor pericial para que sus conclusiones tengan valor probatorio robusto.

En conclusión, la Sala incurre en una **grave falacia técnica y jurídica**. El hash de un archivo contenedor (*“hash de hash”*) no suple la ausencia de los hashes individuales de los archivos clave, y mucho menos constituye prueba plena de su autenticidad. Esta interpretación es incompatible con los estándares internacionales de manejo de evidencia digital y vulnera los principios que la propia Sala enunció como esenciales.

Si la defensa hubiese impugnado técnicamente esta argumentación —por ejemplo, con un contraperitaje especializado—, habría quedado al descubierto la precariedad del razonamiento probatorio en este punto.

Resulta entonces **jurídicamente inadmisibile**, a nuestro modo de ver, que la Sala haya considerado a la prueba de pantallazos como **plena**, pues, reiteramos, la falta de cálculo del hash original y de los hashes individuales de las fotos no permite garantizar ni la autenticidad ni la integridad; menos aún la *“mismidad de la información”* que proclama la Sala en su fallo.

No puede haber *confiabilidad* ni *integridad* en unas imágenes sin hash, ni *auditabilidad* en un procedimiento que no fue documentado, ni *repetibilidad* en una experticia que no puede ser verificada con los mismos resultados.

La Sala terminó avalando como prueba electrónica con eficacia probatoria plena algo que no cumplió con ninguno de los estándares que ella misma citó y reconoció como indispensables.

En consecuencia, las *“selfies”* como evidencia debían haber sido valoradas con el mismo rigor con el que se examina el testimonio de un testigo poco confiable o cualquier otra prueba de dudosa certidumbre o legalidad: con sumo escepticismo jurídico y no con complacencia probatoria.

En resumen, la Sentencia SP-248-2025 que venimos analizando, merece una **crítica firme**, ya que da pábulo a validar pruebas electrónicas que no cumplen con los estándares mínimos de autenticidad e integridad, y por ende, de *fiabilidad*.

Y lo anterior, en el contexto actual de las evidencias digitales, es **extremadamente riesgoso** y reñido con el debido proceso probatorio.

b) Integralidad e inalterabilidad: ¿Se preservó la evidencia en su estado original?

Dice el fallo:

“ii) Integralidad e inalterabilidad: Referida a que la información sea presentada en su forma original, en las mismas condiciones en que fue obtenida, extraída, en forma completa e inalterada. Lo que también implica que sea conservada o preservada en esa misma condición, evitando su deterioro o destrucción.

En este aparte, se tratan conceptos como el de certificados digitales, de que trata el artículo 30 de la Ley 527 de 1999⁸, así como el numeral 3° del artículo 426 de la Ley 906 de 2004, como método de autenticidad e identificación del documento.

Asimismo, los códigos o valores *hash*, han sido entendidos como una identificación única o huella digital de cada archivo. Para ello, en términos generales, mediante un *software* que emplea algoritmos, se toma un archivo, una carpeta o dispositivo de almacenamiento como entrada, para generar un hash o salida, que corresponde a un resumen único de la información ingresada o código alfanumérico.

Este método permite: *«estar seguros de que algunas comunicaciones o archivos no fueron alterados de alguna forma, se pueden examinar los valores hash creados antes y después de la transmisión de los datos. Si los dos valores hash son idénticos, significa que no ha habido ninguna alteración»*⁹.

En síntesis, la sentencia reconoce que la integralidad o inalterabilidad de la evidencia digital debe garantizarse mediante el cálculo de **valores hash**, lo que permite verificar que no ha sido modificada desde su obtención.

¿Se respetó este principio? No.

Al no calcularse el hash de la memoria SD original, no hay forma de probar que la imagen forense generada contenga los mismos archivos del dispositivo (memoria SD) al momento de su intervención.

Además, la investigadora del caso, Leidy Judith Orejuela Gutiérrez accedió al (al parecer¹⁰) al disco duro Buffalo y obtuvo los “pantallazos” de las “selfies” sin usar herramientas forenses, lo que pudo haber alterado la metadata de los archivos

⁸ Referido a las actividades que realizan las entidades de certificación de la firma digital o electrónica de personas naturales; la verificación en la alteración entre el envío y recepción de mensajes de datos y documentos electrónicos transferibles; el registro o estampado cronológico en la generación, transmisión y recepción de mensajes de datos, entre otros.

⁹https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_tecnicos.pdf. Págs. 30 y 31.

¹⁰ Ver infra el análisis de su testimonio, que denota cierta confusión respecto a si los pantallazos los obtuvo del Disco Duro Buffalo, en el cual el perito almacenó la imagen forense de la Memoria SD, o si los obtuvo directamente del propio celular color blanco colectado en el sitio del suceso, al lado del cadáver del periodista asesinado.

contenidos en la imagen forense almacenada en el disco duro Buffalo sin que nadie se percatara.

En tal sentido, rindió declaración, reseñada por el fallo así:

“... en sesión de juicio oral del 5 de agosto de 2016, la investigadora del C.T.I., Leydi Judith Orejuela Gutiérrez, declaró que por orden de policía judicial le fue asignado realizar un análisis de la información recolectada de unos elementos materiales probatorios, encontrados en el lugar de los hechos, cuatro celulares y dos grabadoras de mano o de “periodista”, que fue extraída por el experto y almacenada en un disco duro “Buffalo”. Labor que consignó en el informe de investigar del 14 de abril de 2015, que da cuenta del análisis de la información contenida en el disco duro externo Buffalo S/N 8559922441294 modelo HDPNTU3 color vino tinto.

De ello, dijo, *‘se extrajo información relevante de un celular que recuerdo era de color blanco, que era el celular que llamó la atención desde el inicio de la investigación porque no correspondía ni a las personas que estaban dentro de la panadería ni correspondía a los celulares del hoy occiso. A ese celular el perito extrae una información, esa información la incluye en el disco duro, yo lo único que hago es mirar la información de ese celular e imprimo unas fotografías’*¹¹.

Aclaró que las fotos le parecieron relevantes, pues desde el inicio de la investigación, se tomó la declaración de dos testigos presenciales que describieron al responsable como una persona de sexo masculino, raza negra, de contextura delgada, labios gruesos, cabello corto, siendo estas las mismas características o similares de quien estaba retratado en aquellas”.

Lo realizado por la funcionaria, siguiendo, a su decir, *“orden de policía judicial”*, no constituye un procedimiento forense válido, máxime aún cuando la investigadora no acreditó ser experta en informática.

Extraer pantallazos de manera empírica, hurgando en el disco duro marca Buffalo contentivo de la imagen forense de los archivos extraídos por el perito de la memoria SD del celular sin preservar la metadata y sin garantizar la inalterabilidad de los archivos, destruye la validez probatoria de las imágenes obtenidas por falta de *fiabilidad*.

El citado autor español González Reyes, al referirse al *juicio de fiabilidad*, expresa:

“El **juicio de fiabilidad**, por su parte, se refiere a la posibilidad de poderse comprobar la **autenticidad** e **integridad** de los documentos digitales obtenidos y su no manipulación. Esta fiabilidad se asegura con la denominada cadena de custodia, que se describe en el apartado siguiente, pero también con el

¹¹ Ibidem. Minutos: 00:17:10 a 00:17:20

adecuado análisis racional, y más extenso, al objeto de que la convicción judicial no adolezca del vicio de **inveracidad**²⁵.¹²

Y en esa nota N° 25, al pie de la misma página 51, expresa:

“Por desgracia, no estamos en un ámbito exento de la posibilidad de que se fabriquen pruebas informáticas manipuladas, montajes ficticios, falsedades o distorsiones fraudulentas del material informático de las supuestas víctimas u obtención con técnicas espurias, incluso por los propios investigadores policiales, como recurrentemente pone de relieve la Doctrina técnica especializada en este campo. Cfr. esta idea en Rubio Alamillo, J., «La Informática en la reforma de la Ley de Enjuiciamiento Criminal», diario La Ley, núm. 8663, 2015, p. 8, donde se expresa explícitamente que los datos informáticos pueden ser manipulados sin que, en ocasiones, ni siquiera pueda detectarse esa manipulación por peritos informáticos”.

El mismo autor, agrega más adelante:

“Es el **juicio de fiabilidad** lo que nos va a permitir aceptar la viabilidad procesal de la supuesta evidencia digital como auténtica (no manipulable), **íntegra** (conservación del contenido) y **confiable** (obtenida sin técnicas espurias). Ello implica sujetarse a los estándares y requisitos técnicos por parte del juzgador para comprobar si, efectivamente, se ha analizado correctamente y de modo «confiable» el proceso de obtención de las evidencias digitales y su copia clonada, así como la fiabilidad del procedimiento de preservación, análisis del material y correspondencia de lo incautado con el presentado al órgano judicial llamado a decidir”.¹³

c) **Accesibilidad**

Al respecto, se lee en el fallo:

“iii) Accesibilidad: En cuanto se debe garantizar el acceso para posteriores consultas de los documentos, registros, informaciones o mensajes de datos extraídas, así como su origen y destino, fecha y hora de creación, en que fue enviado o recibido el mensaje o producido el documento, entre otros, o metadatos. Por ello, de requerirse su reproducción esta debe corresponder, con exactitud, al momento en que fue generado el documento, enviado o recibido el mensaje de datos.

En ese sentido, conforme a la evolución constante de la tecnología, es claro que otros criterios han sido reconocidos en parámetros internacionales, como los previstos en la norma ISO/IEC 27037 del 2012¹⁴, expedida por la Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC), para el manejo de la evidencia digital y que resultan atendibles, a manera de orientación, para establecer el valor probatorio de los datos contenidos en recursos electrónicos o digitales, idóneos para acreditar un hecho jurídicamente relevante. Estos, interpretados de la norma en cita, son:...” (*Auditabilidad y Repetibilidad*).” (Nuestro el paréntesis).

¹² GONZALEZ R., José M., ob. cit., pp. 50-51.

¹³ *Ibidem*, p. 52

¹⁴ <https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en>

¿Se respetó este principio? No.

En vez de presentar las fotos en su formato digital original con metadatos verificables, se utilizaron pantallazos impresos tomados por la investigadora, lo que elimina cualquier posibilidad de analizar la fecha de creación, ubicación GPS o detalles técnicos de los archivos digitales de imagen, dado que, obviamente, estos metadatos se pierden al imprimirse el “pantallazo”.

El criterio de *accesibilidad*, tal como lo establece la propia Sala Penal en la sentencia *in comento*, exige que la evidencia digital pueda ser consultada posteriormente en condiciones que permitan verificar su origen, contenido, metadatos, momento de creación, envío o recepción, así como todos aquellos elementos (metadatos) que rodean su existencia digital.

No basta, por tanto, presentar un simple contenido visual o textual, como una fotografía impresa o una simple captura de pantalla. Se debe garantizar que esa información pueda ser abierta, examinada y analizada en su estado original, bajo condiciones técnicas replicables.

De manera que el criterio de *accesibilidad* se ve **gravemente vulnerado** cuando lo que se presenta al juez --como ocurrió en el caso-- son espurios pantallazos impresos, de muy escaso o nulo valor probatorio por sí solos dada la facilidad con la cual se pueden falsificar o alterar o modificar fotografías, no solo con el conocido y manido *photoshop*, sino con avanzadas herramientas de inteligencia artificial que permiten elaborar imágenes, fotos y videos de impresionante realismo y prácticamente perfecto.

Y para *agrarar aún más* la situación, resulta, como hemos venido diciendo, que no fue el experto informático el que extrajo los pantallazos, sino que fue la investigadora del caso, quien, sin ser perito acreditada en informática forense y a riesgo de contaminar una evidencia que ya había sido peritada, extrajo e imprimió las seis fotos incriminatorias a partir de una visualización directa y subsiguiente manipulación del disco duro Buffalo.

Esa acción, completamente alejada de un protocolo forense mínimamente aceptable, impide el acceso a los metadatos inherentes a cada archivo, tales como la fecha y hora exacta de captura, la ubicación GPS (si existía), el modelo del

dispositivo con que fueron tomadas, la secuencia de creación o modificaciones del archivo, e incluso información oculta clave, como los hashes individuales.

Todos esos elementos —de valor incalculable en un proceso penal— se pierden irremediabilmente cuando se convierte la imagen digital en una impresión plana en papel, que no permite constatar nada más allá de lo que el ojo humano percibe en una impresión. La evidencia queda amputada de su riqueza técnica, se convierte en una *sombra sin cuerpo*, y su idoneidad demostrativa es prácticamente nula.

En consecuencia, el criterio de *accesibilidad*, entendido como la posibilidad real, técnica y forense de examinar la prueba digital con su información integral y verificable, fue **claramente injuriado** en este caso. No se garantizó acceso a los archivos originales ni se reprodujeron con fidelidad técnica.

La Sala, al aceptar como evidencia probatoria *plena* los pantallazos impresos por una funcionaria sin estar capacitada en la práctica de pericias informáticas, renunció, de hecho, al **rigor técnico** que exigen las evidencias digitales dada la facilidad con la cual pueden ser falsificadas, adulteradas o suprimidas por su naturaleza volátil y modificable.

d) Auditabilidad.

Añade el fallo:

“iv) Auditabilidad: En cuanto el proceso de recolección de la evidencia digital, así como su posterior análisis debe estar documentado y justificado, con el fin de que pueda ser revisado, no solo por las partes sino por la autoridad judicial.

¿Se respetó este principio? No.

En efecto, nada de lo que afirma la Sala ocurrió con los pantallazos presentados por la funcionaria Leidy Judith Orejuela. El fallo reseña que ella accedió al disco duro Buffalo en el cual el perito almacenó la imagen forense, de cuyo disco habría seleccionado las seis “selfies”, les tomó capturas de pantalla y las imprimió.

Sin embargo, el análisis de su declaración rendida en la sesión del juicio del 5 de agosto de 2016, resulta poco convincente. Según se lee en el fallo, Orejuela manifestó:

“... se **extrajo información relevante de un celular** que recuerdo era de color blanco, que era el celular que llamó la atención desde el inicio de la investigación porque no correspondía ni a las personas que estaban dentro de la panadería ni correspondía a los celulares del hoy occiso. A ese celular el perito extrae una información, esa información la incluye en el disco duro, **yo lo único que hago es mirar la información de ese celular** e imprimo unas fotografías”¹⁵. (Nuestras las negrillas).

Pues bien, este testimonio lejos de aportar claridad sobre el origen técnico y documental de los pantallazos y cuando se hizo, genera serias dudas que comprometen directamente el principio de **auditabilidad**.

Ella afirmó al principio de su deposición que: “... *se extrajo información relevante de un celular que recuerdo era de color blanco...*”; y al final que: “... *yo lo único que hago es mirar la información de ese celular e imprimo unas fotografías*”, expresiones que parecen indicar que accedió directamente al **dispositivo celular** y no al disco duro Buffalo.

Esta ambigüedad es alarmante, pues no dejó constancia de cuándo accedió, con qué medio técnico, qué carpetas exploró, cómo identificó las fotos, qué equipo utilizó para las capturas ni cómo las imprimió, lo que representa una falta absoluta de trazabilidad técnica y una clara vulneración del principio de *auditabilidad* reconocido en la propia sentencia.

Peor aún, si efectivamente accedió al celular para obtener directamente las imágenes, ello implicaría que logró desbloquear el dispositivo, lo que el propio perito forense había declarado imposible en su informe y en juicio. De ser así, nos encontraríamos no sólo ante una actuación sin acreditación ni respaldo técnico-forense, sino además, ante una gravísima contradicción fáctica que debilita aún más la fiabilidad de la prueba electrónica que dio lugar a la condena.

En todo caso, sea como haya sido, la funcionaria obtuvo los pantallazos sin dejar constancia alguna del procedimiento que utilizó para ello ni cómo identificó esas imágenes como relevantes ni de cuál dispositivo (celular o Disco Duro Buffalo) las extrajo realmente. Es decir, la funcionaria investigadora actuó sin observar ningún tipo de protocolo técnico y fuera de cualquier marco de documentación forense verificable.

¹⁵ Ibidem. Minutos: 00:17:10 a 00:17:20

Lo anterior se traduce en una **falta de trazabilidad** absoluta: no se puede reconstruir el camino seguido por la funcionaria ni verificar que actuó con fidelidad técnica. Sin trazabilidad no hay transparencia, y sin transparencia, la prueba no puede ser auditada, ni por el juez, ni por la defensa, ni por otro perito.

Este incumplimiento invalida el principio de *auditabilidad* en su esencia. La auditabilidad no es un mero formalismo; es el mecanismo que permite revisar si todos y cada uno de los pasos dados por los actores forenses fueron los correctos, si se cometieron errores, manipulaciones o accesos indebidos, y si la evidencia conservó su integridad a lo largo del recorrido.

Al no existir registros confiables y verificables del procedimiento seguido por Orejuela para obtener los pantallazos, la prueba queda fuera del control y del escrutinio técnico, y su validez se basa únicamente en la confianza subjetiva de su palabra, lo cual es inaceptable en el manejo de evidencia digital.

En consecuencia, la prueba pierde uno de los pilares que sostienen su legitimidad técnica y jurídica. La Sala, que en su propia argumentación reconoce la *auditabilidad* como condición para el valor probatorio de la prueba digital, incurre en evidente contradicción cuando acepta como válidas evidencias digitales *inauditable*s, dado que su irregular proceso de extracción no puede ser verificado ni constatado.

e) Repetibilidad.

Y agrega la sentencia:

“v) Repetibilidad: En el sentido de garantizar que, si un investigador o perito utiliza los mismos métodos y condiciones para la obtención y análisis de una evidencia digital, empleado por otro, obtendrá el mismo resultado”.

¿Se respetó este principio? No.

Como ya dijimos, el perito no calculó el hash de la data original contenida en la memoria SD, limitándose exclusivamente a extraer su imagen forense y obtener su hash.

Esto significa que no existe un punto de comparación que permita verificar que esa imagen --y que presuntamente contenía las seis fotos incriminadoras-- es una copia fiel y exacta del contenido original.

Sin ese hash inicial, que ha de obtenerse antes de realizar la imagen forense, el estándar de comparación de *hashes* (el de la data original de la Memoria SD y el de la imagen forense extraída) que da sustento técnico a la repetibilidad de la prueba, es inexistente. No puede reproducirse la pericia, ni evaluarse si los resultados coincidirían o no con los obtenidos por otro perito bajo iguales condiciones, lo cual atenta contra uno de los pilares fundamentales de la informática forense: la posibilidad de contrastar y validar los hallazgos de un experto con otro.

A lo anterior se suma el hecho de que tampoco se calcularon los hashes individuales de las seis fotos, y que el procedimiento mediante el cual fueron extraídas vía pantallazos --realizado por una investigadora que no es perito informático-- no se documentó ni fue supervisado técnicamente.

En conclusión: ni se puede repetir la pericia original, ni tampoco auditar el acto de extracción de los pantallazos que Orejuela implementó. Todo el proceso queda sumido en la opacidad técnica y en la imposibilidad de ser repetido, comparable a un testigo que dice haber visto algo relevante para un caso, pero que jamás puede ser confrontado ni verificado por otro testigo ni de ningún otro modo.

Por ello, afirmar --como lo hizo la Sala-- que el valor probatorio de los pantallazos “es *pleno*”, resulta **jurídicamente insostenible** y **técnicamente indefendible**.

2. LA DOBLE CADENA DE CUSTODIA: EL ERROR DE LA SALA AL IGNORARLA

La Sala Penal constató la correcta preservación de la cadena de custodia de la evidencia electrónica (celular, tarjeta SIM y memoria SD), pero no fue rigurosa en la cadena de custodia de la evidencia digital (la información extraída de estos dispositivos).

Las pruebas electrónicas tienen **dos niveles** de cadena de custodia:

- **Cadena de custodia de la evidencia electrónica:** Se refiere a la conservación del dispositivo físico desde su incautación hasta su análisis.
- **Cadena de custodia de la evidencia digital:** Comienza cuando el perito recibe el dispositivo y extrae la información de él.

¿Se protegieron ambas cadenas por igual? No.

Si bien el celular y la memoria SD (evidencias electrónicas) fueron debidamente recolectados y envasados, la información extraída (evidencia digital) no tuvo controles adecuados, pues, simple y llanamente, el perito informático inobservó abiertamente los protocolos establecidos por las Normas ISO/IEC 27037:2012 y la ISO/IEC 27042:2015, antes referidas, que son estándares mundialmente reconocidos.

Respecto a la primera Norma, reiteramos lo que dice la sentencia:

“.. es claro que otros criterios han sido reconocidos en parámetros internacionales, como los previstos en la norma ISO/IEC 27037 del 2012¹⁶, expedida por la Organización Internacional de Estandarización (ISO) y la Comisión Internacional Electrotécnica (IEC), para el manejo de la evidencia digital y que resultan atendibles, a manera de orientación, para establecer el valor probatorio de los datos contenidos en recursos electrónicos o digitales, idóneos para acreditar un hecho jurídicamente relevante”.

Y es más que indiscutible, por todo lo antes expuesto, que el perito informático no aplicó esta normativa. De haberlo hecho, habría calculado el hash de la evidencia original previo a la extracción de la imagen forense y luego comprarlos para verificar su coincidencia absoluta, y después habría calculado el hash de cada una de las fotografías que le parecieron relevantes para el caso, pues con esto aseguraba la integridad e inalterabilidad de la evidencia.

Además, habría explicado con precisión las razones por las cuales señaló que “... *no fue posible la recolección de elementos del teléfono Vodafone, ya que tenía un bloqueo por patrón de seguridad y no le fue posible desbloquearlo*”, según se lee en la sentencia, toda vez que, hoy por hoy, esto es técnicamente factible sin mayores obstáculos utilizando las herramientas de análisis forenses adecuadas.

¹⁶ <https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en>

Era su obligación brindar las debidas explicaciones y razones por las cuales no pudo desbloquear el celular, qué procedimientos utilizó para ello sin poder lograrlo y explicar cuáles herramientas utilizó para el análisis que no le permitieron realizar el desbloqueo. Esta falencia, aunada a las antes anotadas, torna aún más dudosa la capacidad técnica y eficiencia del perito informático y, por supuesto, la experticia por él realizada y el correspondiente dictamen pericial.

Ello así porque existen numerosas herramientas de análisis forense que sortean con relativa facilidad los bloqueos de una inmensa mayoría de dispositivos electrónicos (v.gr., UFED Cellebrite).

Tal omisión, a no dudar, genera una presunción de **negligencia técnica**. Existen herramientas de uso común en la informática forense capaces de acceder incluso a celulares con cifrado o patrones de seguridad complejos, y si el perito no demuestra que las usó o que las empleadas en su pericia eran inviables para el caso específico del celular Vodafone, su dictamen debió explicar detalladamente lo concerniente a la imposibilidad del desbloqueo y a las herramientas empleadas sin éxito. No hacerlo, implica que el dictamen carece de rigor científico.

Además, hay que tener presente que las Normas ISO/IEC 27037:2012 y 27042:2015, exigen que cada paso del análisis sea justificable, documentado y reproducible. No cumplir estos estándares reduce la credibilidad del dictamen y disminuye significativamente su valor suasorio, el cual puede ser nulo en definitiva.

En síntesis, el perito incurrió en graves faltas:

- No calculó el hash de la memoria SD original antes de extraer la información.
- No calculó el hash de las fotos individualmente.
- Propició (dado que él no lo hizo) que una investigadora sin formación en informática forense accediera al disco duro contentivo de la imagen forense y extrajera empíricamente evidencia de forma manual.
- No aplicó los estándares internacionales de las Normas ISO/IEC 27037:2012 y 27042:2015, que establecen las directrices básicas para la obtención, preservación y análisis de la evidencia digital, las cuales, por lo visto, las ignoraba o desconocía el perito, o, simplemente, no las aplicó

deliberadamente, tejiendo un manto de dudas sobre su *expertise* como perito informático calificado y competente.

Pese a todo lo anterior, la Sala Penal confió en la “palabra sagrada” del perito y proclamó que era “**pleno**” el valor probatorio de los pantallazos. Sin embargo, lo cierto del caso es que tan crasos e inexcusables errores en la estricta observancia de la **cadena de custodia de la evidencia digital**, si bien no conllevaban a su exclusión automática del proceso, en atención a que, según se lee en el fallo:

“...ha sido línea pacífica de la Sala que los aspectos relacionados con la cadena de custodia no condicionan la admisión de la prueba, sino que, en caso de presentarse irregularidades concernientes a ella, la consecuencia que se deriva no es otra que la disminución de eficacia, credibilidad y asignación de mérito suasorio al elemento, como así se desprende del artículo 273 del Código de Procedimiento Penal...”

sí debieron operar como causa suficiente para atribuirle **nulo valor suasorio**, dadas las graves falencias advertidas. Ello, además, resulta plenamente coherente con lo que también sostiene la propia Sala en el mismo fallo, al señalar que:

“De ahí que, la recolección, preservación y aseguramiento de la evidencia digital, así como su aducción al juicio como prueba digital o electrónica y la valoración que de esta realice el funcionario judicial, debe atender a ciertos principios, a partir de los cuales, podrá ser considerada con pleno, disminuido o **nulo valor suasorio**”. (Nuestras las negrillas),

En consecuencia, lo jurídicamente correcto habría sido **desechar** de plano los pantallazos como prueba válida de cargo, tal como lo hizo el Juzgado Superior.

3. CONCLUSIONES: UN FALLO QUE CONTRADICE SU PROPIO RAZONAMIENTO

1. La sentencia SP248-2025 del 12 de febrero, incurre en una **notoria contradicción** al proclamar principios rigurosos para valorar la evidencia digital, pero omitir su aplicación en el caso concreto que sentenció.

2. El perito informático incumplió estándares técnicos esenciales e indispensables como el cálculo del hash de la data original y de cada fotografía, y no documentó adecuadamente su actuación, amén de no haber explicado en su dictamen las razones por las cuales no pudo desbloquear el celular Vodafone y acceder a su data.

3. La participación de una funcionaria no perito en la extracción y presentación de los pantallazos, careció de garantías técnicas, afectando la autenticidad y auditabilidad de la prueba.

4. La cadena de custodia de la evidencia electrónica se respetó, pero no así la de la evidencia digital, cuyo tratamiento fue deficiente.

5. La evidencia digital constituida por los seis pantallazos no cumple con los principios de *confiabilidad, integralidad, accesibilidad, auditabilidad y repetibilidad* por lo que su valor suasorio debió ser calificado por la Sala como **nulo** y jamás como **pleno**.

6. Este caso pone en evidencia la **urgente necesidad** de que los operadores jurídicos --jueces, fiscales y litigantes-- comprendan los estándares forenses esenciales aplicables a las pruebas electrónicas. Solo con ese conocimiento técnico crucial podrán gestionarlas adecuadamente y valorarlas conforme a una verdadera **sana crítica digital**.

7. Una defensa técnica y especializada en materia de pruebas electrónicas y evidencias digitales podría haber cambiado el rumbo del proceso de haber sostenido oportunamente, con argumentos técnicos y jurídicos sólidos y fundados, la tesis de la posible suplantación de las seis fotografías.

4. COLOFÓN

Finalmente, opinamos que a las pruebas electrónicas hay que valorarlas conforme a dos principios cardinales básicos: el primero, la **sana crítica digital**, consistente en aplicar el principio general de la sana crítica con criterios técnicos y científicos propios de la informática forense; y, el segundo, las **máximas de experiencia digital**, que aluden al conocimiento especializado y actualizado sobre el funcionamiento de los sistemas, dispositivos, software y métodos de análisis digital que permitan al juez valorar con objetividad si una evidencia electrónica fue obtenida, preservada y analizada conforme a las buenas prácticas forenses.

Estos dos principios los analizaremos en detalle en próximo artículo.

digital@joseluisamayorodriguez.com
jolutaro1958@gmail.com

Instagram: @joseluisamayorodriguez.com
Celular: +52 3630656

REFERENCIAS BIBLIOGRÁFICAS

- Corte Suprema de Justicia de Colombia, Sala de Casación Penal, Sentencia SP248-2025, Rad. 58275, 12 de febrero de 2025.
[https://archivodigitalapi.cortesuprema.gov.co/share/2025/3/Boletines/SP248-2025\(58275\).pdf](https://archivodigitalapi.cortesuprema.gov.co/share/2025/3/Boletines/SP248-2025(58275).pdf)
- ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. <https://www.iso.org/standard/44381.html>
- ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence. <https://www.iso.org/standard/44406.html>
- Consejo Superior de la Judicatura (Colombia), Escuela Judicial. Cartilla de Evidencia Digital: Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica, 2020.
https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_tecnicos.pdf
- José Luis Reyes González: “*LA PRUEBA PERICIAL DIGITAL Y LA CADENA DE CUSTODIA*”. Universidad de La Laguna. Anales de la Facultad de Derecho. N° 38. Septiembre 2021. San Cristóbal de La Laguna. Isla de Tenerife. Islas Canarias. España. <https://dialnet.unirioja.es/ejemplar/597726>