República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal

GERSON CHAVERRA CASTRO
Magistrado Ponente

SP941-2026
Radicado n.° 68613
CUI 63001609902120180028901
Acta n.° 252

Bogotá D.C., doce (12) de agosto de dos mil veintiséis (2026)

I. OBJETO DE LA DECISIÓN

La Sala se pronuncia sobre el recurso extraordinario de casación interpuesto por el apoderado de ÁLVARO JAIME OSPINA RAMÍREZ, contra la sentencia del 11 de diciembre de 2024, por medio de la cual la Sala Penal del Tribunal Superior de Armenia confirmó el fallo de 7 de junio del mismo año, proferido por el Juzgado Segundo Penal del Circuito con función de Conocimiento de esa ciudad, que lo declaró penalmente responsable como autor del delito de pornografía con personas menores de 18 años.

II. HECHOS

El 2 de agosto de 2018 se llevó a cabo una diligencia de allanamiento y registro en el inmueble ubicado en la carrera 25 n.° 35-07 de Calarcá, Quindío. En desarrollo de la diligencia, fueron incautados un disco duro y una torre de cómputo integrada por dos discos más, contentivos de representaciones reales de actividad sexual que involucraba personas menores de 18 años.

En consecuencia, ÁLVARO JAIME OSPINA RAMÍREZ fue aprehendido durante el operativo.

III. ANTECEDENTES PROCESALES

1. El 3 de agosto de 2018, ante el Juzgado Primero Penal Municipal con función de Control de Garantías de Armenia, se legalizó la diligencia de registro y allanamiento, así como el procedimiento de captura de ÁLVARO JAIME OSPINA RAMÍREZ, a quien, seguidamente, la Fiscalía le formuló imputación como autor del delito de pornografía con personas menores de 18 años —verbo rector *almacenar*—, de conformidad con lo dispuesto en el artículo 218 del Código Penal. ÁLVARO JAIME no aceptó los cargos.

2. Presentado el escrito de acusación, el conocimiento del asunto correspondió al Juzgado Segundo Penal del Circuito con función de Conocimiento de Armenia, despacho ante el

cual se tramitaron las audiencias de formulación de acusación, preparatoria y juicio oral.

3. Concluido el debate probatorio, mediante sentencia de 7 de junio de 2024, el despacho de conocimiento declaró a ÁLVARO JAIME OSPINA RAMÍREZ penalmente responsable del delito objeto de imputación. En consecuencia, le impuso pena de 120 meses de prisión, multa de 150 *smlmv* e inhabilitación para el ejercicio de derechos y funciones públicas por el mismo término de la pena privativa de la libertad. Asimismo, le negó la concesión de los mecanismos sustitutivos de la pena.

La defensa interpuso el recurso de apelación.

4. Mediante fallo del 11 de diciembre de 2024, la Sala Penal del Tribunal Superior de Armenia confirmó integralmente la decisión de primera instancia.

La defensa interpuso y sustentó en término el recurso extraordinario de casación.

5. Admitida la demanda, la audiencia de sustentación se celebró el 11 de diciembre de 2025.

IV. SENTENCIA IMPUGNADA

El Tribunal negó una solicitud de nulidad y confirmó la sentencia de primera instancia. Así razonó:

1. **Sobre la nulidad**. De acuerdo con lo expuesto por el apelante, en la sesión de juicio de 27 de junio de 2023, el fiscal y el perito Harold Gamajoa estaban en la misma oficina organizando preguntas y respuestas. Contrario a lo pretendido por el recurrente, el testigo se dirigió a la oficina del fiscal por un instante breve durante un receso de la diligencia; además, no se trata de una situación irregular, cómo sí lo sería sugerir las respuestas. Empero, el recurrente no probó esa hipótesis.

2. **Sobre la valoración probatoria**. Los testimonios de Brandon Beltrán Larios —investigador que participó en el allanamiento e intervino en la incautación de discos duros—, Harold Gamajoa —perito investigador que participó igualmente en la recolección de la evidencia y realizó una previsualización de la evidencia digital recaudada—, Víctor Pimienta —perito en informática forense quien analizó con los protocolos de seguridad pertinentes la información recaudada— y Leonardo Castellanos ——perito en morfología forense quien estableció que las imágenes almacenadas en los discos duros correspondían a personas menores de 18 años—, son coherentes, precisos y, consecuentemente, creíbles.

De otra parte, la declaración del perito Andrés Felipe Giraldo, convocado a juicio por la defensa, no es creíble. En primer lugar, porque no analizó directamente los discos duros, sino que se limitó a cuestionar los informes elaborados por los investigadores de policía judicial que recolectaron, extrajeron y analizaron la evidencia digital.

Bajo tal perspectiva, las conclusiones presentadas por el profesional constituyen especulaciones que incluso el mismo

testigo admitió al indicar «*ni yo ni el perito de Manizales*» estaban en posibilidad de establecer si existió una implantación de información o una alteración de los datos informáticos; además, sostuvo que el informe del perito forense Víctor Pimienta García sí satisfizo las exigencias técnicas que reclama el análisis de la evidencia.

Tampoco es de recibo el planteamiento de la defensa según el cual el investigador Harold Gamajoa Velásquez manipuló la evidencia, en el lugar de los hechos, sin ningún tipo de protección. En realidad, la labor del servidor se circunscribió a una *previsualización* de los datos. Tampoco hubo ruptura en la cadena de custodia con ocasión de la entrega de los CD —contentivos de las imágenes extraídas por el perito Víctor Pimienta— al morfólogo Leonardo Castellanos, pues como este lo explicó, tales elementos se le entregaron bajo los respectivos rótulos de cadena de custodia; además, la discrepancia en el número de archivos resulta intrascendente, habida cuenta que el tipo penal no exige un número determinado de representaciones.

La tesis de una implantación subrepticia de información durante el registro y allanamiento —derivada del hecho de que los equipos de cómputo del procesado estaban conectados a la red de internet—, sugerida en juicio por el procesado, carece de fundamento. En efecto, uno de los discos incautados resultaba inaccesible a la red wi-fi abierta, pues no se encontraba vinculado a algún dispositivo; tampoco es comprensible cómo se habrían copiado centenas de miles de archivos en tan solo algunos minutos.

Con fundamento en tales circunstancias, se encuentran acreditados los elementos estructurales del delito previsto en el artículo 218 del Código Penal, pues se demostró que ÁLVARO JAIME OSPINA RAMÍREZ almacenaba en los discos duros de su propiedad, representaciones reales de actividad sexual que involucraba personas menores de 18 años.

3. Con fundamento en tales planteamientos, confirmó el fallo de primera instancia.

V. DEMANDA DE CASACIÓN

Tras identificar los fallos de primera y segunda instancia y sintetizar los antecedentes procesales, el recurrente formuló dos cargos por violación indirecta de la ley sustancial.

1. **Cargo primero**. Falso juicio de existencia por omisión.

Las instancias omitieron valorar elementos de prueba que demostraban la falta de confiabilidad de la prueba digital en torno a la cual se cimentó la condena.

Concretamente, se verificaron irregularidades en el procedimiento de cadena de custodia, habida cuenta que, según lo explicó Harold Gamajoa Velásquez, servidor de la Policía Nacional convocado a juicio a instancia de la Fiscalía, el disco duro incautado no estaba conectado «*a ningún equipo de cómputo en el momento de la incautación, pero que posteriormente fue conectada a los computadores que llevaron los investigadores*». Esa evidencia regularmente, según lo

expresó el mismo testigo, *quedaría viciada* si se conecta a un equipo de cómputo sin los mecanismos de protección adecuados.

Esta antitécnica conexión «*compromete la autenticidad e integridad de la evidencia, dado que un almacenamiento digital puede ser modificado sin dejar rastro visible si no se utilizan herramientas forenses apropiadas*».

De igual forma, las imágenes en formato digital incorporadas no fueron autenticadas «*mediante sumas de comprobación criptográfica (hashes MD5 y SHA1), a pesar de que estas se encuentran registradas en el DVD número 8 dentro del archivo ofimático "Sumas de verificación información exportada.xlsx"*».

Sin tales registros, no es posible predicar que las imágenes incorporadas como prueba en desarrollo del debate sean las mismas que se incautaron durante el procedimiento de allanamiento y registro. Tampoco puede asegurarse que no hayan sido alteradas.

De hecho, los registros de hora y fecha de ingreso a los discos duros, descritos por el perito Víctor Andrés Pimienta, son posteriores a la calenda en que se llevó a cabo el operativo en que fue aprehendido el procesado. De tal suerte, tales marcas temporales «*constituyen indicios claros de alteración de la evidencia, pero fueron ignoradas en la valoración probatoria del fallo impugnado*».

Además, los servidores de policía judicial que adelantaron el operativo pretermitieron los protocolos para la recolección de la evidencia digital previstos en la *Guía No. 13 de Evidencia Digital del Ministerio de las TIC* y por el *Manual del Sistema de Cadena de Custodia de la Fiscalía General de la Nación*.

1. **Cargo segundo**. Falso raciocinio.

Al conferirle valor probatorio al informe elaborado por el servidor Harold Gamajoa Velásquez, incorporado a instancia de la Fiscalía, el Tribunal incurrió en yerros de valoración.

Ciertamente, como lo detalló el ingeniero Andrés Felipe Giraldo, convocado al debate por la defensa, el informe aludido no satisface los estándares científicos y técnicos requeridos para la recolección, análisis y preservación de la evidencia digital.

Así entonces, el hecho de que para la manipulación de los discos duros no se hubiese realizado mediante herramientas especializadas —como bloqueadores de escritura, software certificado internacionalmente como EnCase o FTK; o equipos recomendados en la Guía N.° 13 de Evidencia Digital del MinTic—, condujo a una afectación de la integridad de los datos allí almacenados.

De esta manera, al asignarle mérito a lo declarado por el investigador Gamajoa, sin una confrontación con las observaciones realizadas por el perito Giraldo, el Tribunal incurrió en un falso raciocinio.

3. Con fundamento en tales reparos, solicitó casar la sentencia del Tribunal con el objeto de que se profiera sentencia absolutoria.

VI. INTERVENCIONES

1. En audiencia de sustentación, el defensor de ÁLVARO JAIME OSPINA RAMÍREZ ratificó los cargos de la demanda de casación.

Insistió en que, conforme lo admitió en juicio el investigador Gamajoa, el disco incautado fue conectado sin ningún tipo de bloqueador de escritura, lo que vició la evidencia digital recabada. De tal suerte, se trataba de elementos carentes de aptitud para soportar una condena.

Por otra parte, expresó que existe una diferencia ostensible entre dos de los paquetes de evidencia analizados; mientras uno contiene 167.586 archivos, el otro registró 396.161. De tal suerte, no resultaba razonable que el Tribunal valorara dichos archivos bajo la comprensión de que se trataba de los mismos elementos.

Además, el recaudo de tales evidencias tuvo lugar sin la observancia de los protocolos técnicos aplicables a ese tipo de procedimiento.

Con apoyo en tales argumentos, reiteró las pretensiones de la demanda.

2. El fiscal sexto delegado ante la Corte Suprema de Justicia, en condición de no recurrente, expresó que el falso juicio de existencia por omisión, vía de ataque seleccionada por el casacionista en el primer cargo, reclama la identificación de una prueba válidamente practicada en el debate que el fallador omite por completo. El demandante pretermitió indicar sobre cuál prueba se produjo la irregularidad denunciada.

En lugar de ello, estructuró el disenso únicamente a partir de las observaciones realizadas por el perito de la defensa, Andrés Giraldo. En todo caso, aun cuando el servidor de policía judicial Harold Gamajoa expresó en juicio que la evidencia n.° 1 no estaba conectada al momento de la incautación y luego se conectó a los equipos de los investigadores, en todo caso también fue enfático en punto a que tal procedimiento no comprometió la autenticidad de la información recabada. El testigo, asimismo, aseguró que se abstuvieron de utilizar bloqueadores porque no se iba a llevar a cabo una *copia espejo* sino una visualización en *forma de esclavo*, sin sacar copias ni alterar los datos.

Por otro lado, el recurrente pretermitió explicar si los archivos digitales fueron modificados, alterados, implantados o cambiados y, además, omitió referirse a otras pruebas practicadas, como los testimonios de los investigadores Beltrán y Pimienta, quienes sí emplearon bloqueadores y software forense para analizar la información contenida en los discos incautados, elementos en los que se hallaron cerca de 396.000 imágenes de niños de 9 a 13 años, de las que se descartó ser producto de inteligencia artificial.

Frente al segundo cargo, expuso que, en virtud del principio de libertad probatoria, no existe tarifa legal para establecer la autenticidad de la evidencia digital. Sumado a ello, el demandante no identificó cuál parámetro de la sana crítica resultó infringido en el caso; en su lugar, se limitó a reiterar las conclusiones del perito de la defensa, frente a las cuales los falladores se refirieron puntualmente en los fallos, a través de una valoración adversa a la pretensión del apoderado del procesado.

Con todo, recordó que, de acuerdo con lo probado en juicio, se demostró la materialidad y responsabilidad del procesado en la conducta endilgada, pues almacenaba imágenes reales de contenido sexual explícito de personas menores de 18 años.

3. El representante del Ministerio Público, en condición de no recurrente, preliminarmente indicó que el escenario expedito en el que la defensa podía rebatir la incorporación del informe elaborado por el perito Gamajoa Velásquez era la audiencia preparatoria, oportunidad en la que no formuló adecuadamente su oposición a la práctica de esa prueba.

En cuanto al primer cargo de la demanda, expresó que los jueces sí apreciaron la declaración de Gamajoa. Igualmente, los funcionarios judiciales coligieron que las imágenes almacenadas en los discos, así como estos elementos, fueron sometidos en debida forma al protocolo de cadena de custodia desde el momento en que se produjo el hallazgo.

Tal como lo precisó el Tribunal, la labor del nombrado profesional, al momento de la diligencia de registro y allanamiento, no se circunscribió a la obtención de una copia, sino a la previsualización de los archivos de imagen almacenados en los discos duros incautados. Aun así, como lo ha sostenido la Sala de Casación Penal, la autenticidad de la evidencia digital se acredita mediante el informe del experto y la originalidad del documento digital no radica en su formato, sino en el poder de convicción.

Con todo, no se verificó manipulación, alteración o implantación de información durante la diligencia de registro.

En lo que atañe al segundo cargo, enfatizó que las funciones desplegadas por el investigador Gamajoa Velásquez en el marco de la diligencia de registro correspondían a un filtro preliminar. De tal suerte, para ese momento no eran exigibles los protocolos técnicos para el aseguramiento de la evidencia digital, mismos que sí se aplicaron en el análisis de laboratorio de la información recaudada —bloqueador de escritura, software FTK, autenticación por hash MD5/SHA1—, tal como se constata en el informe elaborado por el investigador Pimienta.

Con base en tal discernimiento, solicitó no casar la sentencia de segunda instancia.

VII. CONSIDERACIONES

1. La Sala fallará de fondo en el presente asunto sin tener en cuenta las deficiencias de las que adolece la demanda

presentada por el defensor de ÁLVARO JAIME OSPINA RAMÍREZ, toda vez que su ajuste supuso el cumplimiento de las formalidades mínimas requeridas en sede de casación, bajo el entendido de la prevalencia de los fines del recurso vinculados a la efectividad del derecho material, las garantías debidas a los intervinientes en la actuación penal, la unificación de la jurisprudencia y la reparación de los agravios inferidos a las partes con la sentencia impugnada.

2. Problema jurídico y estructura de la decisión

2.1 La defensa denunció la inobservancia de los protocolos técnicos para la recolección y aseguramiento de las evidencias que sirvieron de base a las instancias para sustentar el sentido condenatorio de la sentencia.

2.2 Entonces, aun cuando la discusión propuesta en la demanda se circunscribe a la *legalidad* de la prueba recaudada y su adecuada *valoración* por parte de los funcionarios, la Sala se referirá en primer término a las particularidades dogmáticas del delito de pornografía con personas menores de 18 años.

La razón, es que los elementos estructurales de dicho modelo de conducta evidencian, por su naturaleza, una relación indisociable con la denominada *evidencia digital*. Por tanto, la Sala analizará en ese mismo acápite las particularidades del tratamiento de la evidencia digital.

Seguidamente, se referirá a los cargos propuestos en la demanda.

3. El delito de pornografía con menores de 18 años y el uso de la tecnología

3.1 El artículo 218 del Código Penal, modificado por el artículo 24 de la Ley 1336 de 2009, sanciona con pena de prisión y multa al que «*fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad».* La conducta se agrava cuando el agente *(i)* alimente con *pornografía infantil* bases de datos de Internet, con o sin fines de lucro o *(ii)* sea integrante de la familia de la víctima.

El comportamiento se ubica en el Capítulo IV del Título IV de la Parte Especial del estatuto represor, que se refiere a la *Explotación Sexual.*

Entonces, aun cuando la Sala, en una primigenia interpretación[1] del alcance de la conducta, la vinculó a contextos de *explotación* —comprendida desde un ámbito preponderantemente negocial—, posteriormente, en virtud de la inclusión de la expresión *«para uso personal»* en el tipo[2], se comprendió que el modelo de conducta previsto en el artículo 218 del Código Penal no se restringía a ese ámbito[3].

[1] CSJ SP4673-2019, rad. 47234.
[2] Art. 24, Ley 1336 de 2009.
[3] CSJ SP4235-2020, rad. 51626.

Bajo tal comprensión, no todas las conductas alternativas que describe el tipo reclaman la verificación de un propósito ligado al ámbito de la *explotación* propiamente dicha.

De igual forma, en cuanto al elemento normativo *representaciones reales de actividad sexual*, la Sala, tras un estudio comparado de las diferentes conceptualizaciones de *lo que es* el material pornográfico —a lo que se refiere de modo literal el tipo penal en su *nomen iuris* y sus elementos estructurales—, sostuvo que se trata de *«[…] la iconografía en la que participan seres humanos con edad inferior a la señalada, desarrollando conductas sexuales explícitas tendientes a producir excitación sexual»*[4].

Por consiguiente,

> […] en acatamiento de los principios de legalidad y estricta tipicidad, sin que haya lugar a extender la norma a aspectos no contemplados previamente por el legislador, **las siguientes modalidades de pornografía no son punibles en el ordenamiento nacional**: i) la **pornografía infantil técnica**, en la que intervienen personas que no tienen la condición de ser menores de edad, pero que aparentan serlo, bien porque físicamente parecen tales, o porque mediante recursos tecnológicos se les da esa apariencia; ii) la **pseudopornografía**, en la cual se insertan fotogramas o imágenes de menores reales en escenas pornográficas en las cuales no intervinieron realmente, lo cual significa que no fueron abusados; y iii) la **pornografía infantil artificial**, en la que intervienen *menores* creados a partir de un patrón irreal, ya sea por dibujos o animaciones de todo tipo, es decir, no representan a un ser humano con existencia real. (Negrillas fuera del texto).

[4] CSJ SP123-2018, rad. 45868.

Por otro lado, la jurisprudencia de la Sala ha decantado asimismo que, bajo específicas condiciones, el consentimiento de los mayores de 14 años y menores de 18 puede implicar la atipicidad de la conducta:

> Posteriormente, en la sentencia SP4235-2020, la Corte precisó que **la expresión para *«uso personal»*,** incluida en el tipo penal por la Ley 1336 de 2009, **amplió la posibilidad de tipificar el delito** a eventos diferentes al ámbito de la explotación sexual, **cuando la fotografía o la filmación se obtienen sin autorización de la persona mayor de 14 años, por constituir una forma de abuso contra el menor de edad**.
>
> **En consecuencia, si la persona mayor de 14 años otorga su consentimiento para fotografiar o grabar representaciones reales de contenido sexual para uso personal, la conducta resulta atípica** en razón a la libertad sexual que la ley colombiana reconoce en esa materia a quienes superan esa edad, pues si pueden sostener relaciones sexuales consensuadas, no hay razón para que no puedan permitir dichas actividades. (Negrillas fuera del texto original).

Bajo tal comprensión, el consentimiento, en los términos precisados, opera únicamente cuando: *(i)* la representación de actividad sexual corresponda a un mayor de 14 y menor de 18 años; *(ii)* exista manifestación expresa y libre de consentimiento conferida por la persona que interviene en la actividad sexual, lo que excluye eventos en que medie engaño, violencia, coacción o cualquier mecanismo que interfiera en ese ámbito decisional; y *(iii)* la representación de actividad sexual se obtenga con la finalidad del *uso personal* de quien la posee; de manera que, aun mediando consentimiento expreso y libre, otorgado por una persona mayor de 14 años y menor de 18, tal manifestación no resultará válida si el agente obtiene dicha

representación con propósitos diferentes al del uso personal —como la comercialización, explotación, divulgación, etc.—

3.2 La Sala, igualmente, recordó que la pornografía infantil constituye un problema de «*amplificada dimensión en el contexto universal, por la irrupción de incesantes y novedosas tecnologías que han transformado las pautas de producción de este tipo de material*».

Ciertamente, la *digitalización* de las dinámicas comunicativas, consustancial a la globalización tecnológica, ha instituido un modelo de representación de la información —texto, imágenes, video, audio, etc.— sustentado en un lenguaje lógico binario. La información digitalizada o *dato informático*, debe entenderse entonces, en los términos del Convenio Sobre Ciberdelincuencia de Budapest de 2001, aprobado en Colombia mediante la Ley 1928 de 2018, como la «*[u]nidad básica de información, ello es, toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático*»[5].

La capacidad representativa del dato informático, por tanto, le confiere vocación probatoria en el proceso penal.

No cabe duda, por consiguiente, que las *representaciones* de actividad sexual a las que alude el artículo 218 del Código Penal pueden estar asociadas a medios físicos, pero también presentarse como un *dato pasible de tratamiento informático*.

[5] CSJ SP065-2026, rad. 69530.

En tales circunstancias, podrá emplearse como *evidencia digital* —en el ámbito de la investigación, como medio para estructurar diferentes juicios inferenciales propios de esa etapa— o *prueba digital* —durante la etapa de juicio—, a condición de que en su recolección, aseguramiento, práctica y apreciación se respeten el principio de legalidad, así como los parámetros del debido proceso probatorio. Sobre el particular la Sala retomará más adelante.

3.3 Ahora bien, tanto la evidencia tangible como la información representada en datos informáticos están sujetas a distintas vulnerabilidades. En el caso de la evidencia digital, su estructura basada en un lenguaje lógico binario la torna particularmente susceptible a *(i)* la *volatilidad* —el dato informático puede perderse como consecuencia del apagado del dispositivo o hardware de almacenamiento, como ocurre, por ejemplo, con la información que se almacena en la memoria de acceso temporal (RAM)—; *(ii)* la *eliminabilidad* —un dato informático no necesariamente se *elimina* con el comando empleado para ese efecto por el usuario; en su lugar, el dato se pierde cuando se reescribe—; o *(iii)* la *modificabilidad* —cambio o modificación; total o parcial de la forma o el contenido del dato informático, sin que necesariamente se afecte su *disponibilidad*—[6].

En el contexto descrito, la escisión de la información de los medios tangibles tradicionales ha facilitado

[6] Así, entre otros, Oliva León, R., & Valero Barceló, S. (Coords.). (2016). *La prueba electrónica: validez y eficacia procesal*. Juristas con Futuro; Posada Maya, R. (2017). *Los cibercrímenes: un nuevo paradigma criminal*. Universidad de los Andes.

significativamente no solo la circulación, sino la *manipulación* de los datos[7].

Consciente de tal realidad, la Sala, en decisión CSJ SP248-2025, rad. 58275, con sujeción a las disposiciones contenidas en la Ley 527 de 1999[8], así como en la norma ISO/IEC 27037 del 2012, expedida por la Organización Internacional de Estandarización —ISO— y la Comisión Internacional Electrotécnica —IEC—, definió algunos criterios para conferirle *efectos jurídicos* a la evidencia digital:

> 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 digital[9], para lo cual se suele emplear un bloqueador de lecto/escritura o White Blokers[10], 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.
>
> ii) Integralidad e inalterabilidad: Referida a que **la información sea presentada en su forma original**, en las mismas condiciones en

[7] Burri, Mira (2023), *The impact of digitalization on Trade Law*. German Law Journal, 551-573. https://doi.org/10.1017/glj.2023.29
[8] 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, y se establecen las entidades de certificación y se dictan otras disposiciones
[9] 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_teicnicos.pdf
[10] 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_teicnicos.pdf

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 1999[11], así como el numeral 3º 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»[12].

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.
[…]
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.

v) Repetibilidad: En el sentido de garantizar que, si un investigador o perito utiliza los mismos métodos y condiciones para la obtención

[11] 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.
[12]https://escuelajudicial.ramajudicial.gov.co/sites/default/files/22_cartilla_evidencia_digital_-_procedimientos_teicnicos.pdf. Págs. 30 y 31.

> y análisis de una evidencia digital, empleado por otro, obtendrá el mismo resultado. (Negrillas fuera del texto original).

3.4 Considerando, entonces, la vocación demostrativa de los datos informáticos, la Sala ha sostenido igualmente que la información sometida a tratamiento informático es equiparable a los elementos materiales probatorios, así como a la prueba documental, en los términos previstos en los artículos 275 y 424 de la Ley 906 de 2004. Precisamente, en virtud del «*criterio de equivalencia funcional, la Ley 527 de 1999 asigna un efecto jurídico, validez y fuerza obligatoria a la información expuesta bajo la forma de mensaje de datos*»[13].

3.5 Debido a su naturaleza —como equivalente funcional del documento—, sus vulnerabilidades y los criterios que deben tenerse en consideración para *conferirle efectos* a la evidencia digital, la jurisprudencia[14] ha delimitado las exigencias a las que debe plegarse la parte que pretenda utilizar ese medio de conocimiento como sustento de la acusación o la hipótesis alterna.

Tales reglas pueden sintetizarse de la siguiente manera:

3.5.1 **Fase de recolección y extracción**. Deben asegurarse las condiciones técnicas para la recolección del elemento, lo que supone una descripción completa de las caracterísiticas que lo identifican, emplear procedimientos que garanticen la inalterabilidad de la información y la participación de profesionales capacitados en el área de la informática.

[13] CSJ SP1284-2025, rad. 36784.
[14] Puntualmente lo desarrollado en las decisiones CSJ SP1284-2025, rad. 36784 y CSJ SP248-2025, rad. 58275, antes citadas.

La razón de tales exigencias radica en la necesidad de preservar la *integridad*, *identidad* y *mismidad* del dato informático recabado, para lo cual, sin perjuicio del principio de libertad probatoria, podrán verificarse el *certificado digital*, de acuerdo con lo previsto en los artículos 30 de la Ley 527 de 1999 y 426.3 de la Ley 906 de 2004, o bien, los valores *hash*, esto es, una secuencia algorítmica —como el MD5 o SHA 1— que permiten establecer la identidad del dato informático —la *huella digital* de la evidencia, en los términos de la Sala— y, de contera, si este ha sido objeto de modificaciones.

En todo caso, el procedimiento de recolección y extracción debe estar en debida forma documentado.

3.5.2 **Fase de análisis forense: la cadena de custodia**. Por tratarse de un equivalente funcional del elemento material probatorio y la prueba documental, la evidencia digital debe someterse a los protocolos de cadena de custodia, de conformidad con lo previsto en el artíuculo 254 del Código de Procedimiento Penal.

Tal procedimiento tiene por objeto demostrar la *autenticidad* del elemento, y supone la verificación de algunos indicadores como la recolección, identidad, integridad, preservación, embalaje, envío y registro.

Así las cosas, aun cuando el artículo 273 del mismo compendio adjetivo fija el cumplimiento de la cadena de custodia como uno de los parámetros de *valoración* de la evidencia, lo cierto es que, como lo ha sostenido la Sala, la inobservancia total

o parcial de tal procedimiento no conduce a la inadmisión del elemento, sino a la atemperación de su mérito probatorio[15].

Bajo tal comprensión, se ha sostenido:

> […] la ventaja que se deriva del cumplimiento del protocolo de cadena de custodia es que releva a la parte que presenta el elemento probatorio o la evidencia física del deber de demostrar su autenticidad, pues cuando ello ocurre la ley presume que son auténticos. Y la desventaja de no hacerlo es que traslada la carga de la acreditación de la indemnidad del elemento probatorio o de la evidencia física a quien la presente […]

3.5.3 **Incorporación y autenticación en juicio**. Sin perjuicio de lo expuesto en el punto anterior, a la autenticación de la prueba digital en el juicio oral debe procederse con sujeción a lo previsto en el artículo 426.4 de la Ley 906 de 2004, esto es, mediante *informe de experto*.

En concordancia con lo anteriormente expuesto, la declaración deberá dar cuenta, por lo menos, del procedimiento técnico para la recolección y aseguramiento de la evidencia, lo que supone constatar, entre otras cosas, *(i)* el uso de bloqueadores de escritura —o *write blokers*—, es decir, dispositivos orientados a impedir que el procedimiento de análisis de la información introduzca modificaciones en el dato informático; *(ii)* los *valores hash* del dato digital; y *(iii)* el estado de conservación de la evidencia.

3.6 **Sobre la previsualización de la evidencia digital**. En cuanto es de interés para el presente asunto, la Sala debe realizar

[15] CSJ SP, abr. 17 de 2013, rad. 35127, AP abr. 28 de 2021, rad. 52062 y SP248-2025, rad. 58275, CSJ SP1739-2025, rad. 64342, entre otras.

algunas precisiones en relación con los procedimientos preliminares de observacion de la evidencia digital.

Según se ha explicado, la satisfacción de los protocolos técnicos para el análisis de la evidencia digital constituye una exigencia primordialmente orientada a garantizar la indemnidad del dato informático. Por tal razón, en línea de principio, la observancia de tales reglas debería hacerse extensiva incluso al momento en que los servidores encargados de las labores de indagación preliminar entran en contacto por primera vez con la evidencia, como acontece, por ejemplo, en el desarrollo de una diligencia de allanamiento y registro.

En las actividades de policía judicial que se llevan a cabo en los contextos descritos, se exige, de acuerdo con lo previsto en el artículo 205 de la Ley 906 de 2004, la *identificación* preliminar de los elementos materiales probatorios y evidencia. Así, tratándose de *evidencia digital*, dicha labor reclama una previsualización de los datos informáticos enfilada a seleccionar aquella información que resulte de interés para el caso.

De esta manera, sin perjuicio de que puedan desplegarse desde ese momento los protocolos técnicos necesarios para la extracción y análisis de los datos (§ 3.5.1), cuando ello no fuere posible por las circunstancias concretas del caso, los servidores de policía judicial que intervienen en estas actividades deben *(i)* estar adecuadamente capacitados en el área; *(ii)* limitar sus labores primigenias a la simple *observación*; *(iii)* emplear en la medida de lo posible

procedimientos y dispositivos que garanticen la indemnidad de la información almacenada; *(iv)* preservar las condiciones del dispositivo de almacenamiento —apagado/prendido—, en aras de evitar pérdida o alteración de información volátil (§ 3.3); *(v)* documentar las circunstancias en que se lleva a cabo la operación; y *(vi)* disponer de las actividades necesarias para someter en el menor tiempo posible a cadena de custodia la evidencia recolectada.

4. Sobre los cargos de la demanda

4.1 El recurrente formuló dos cargos por violación indirecta de la ley sustancial: *falso juicio de existencia* y *falso raciocinio*. Más allá de la sindéresis en la selección y fundamentación de las vías de ataque postuladas, la sustancialidad de los reproches converge en un tema central: la *autenticidad* de la evidencia digital y, por consiguiente, su mérito suasorio.

Para una mejor comprensión del asunto, la Sala se referirá en primera medida a los aspectos contextuales del caso, así como a la tipicidad de la conducta objeto de juzgamiento, frente a los cuales no existe controversia.

4.2 **El origen de la investigación y la diligencia de registro y allanamiento.**

4.2.1 A partir de lo expuesto en juicio por los investigadores Brandon Beltrán Larios[16] y Harold Gamajoa

[16] Audiencia de juicio de 21 de junio de 2019, récord 00:08:10.

Velásquez[17], se conoce que para el año 2018, la Fiscalía General de la Nación, en coordinación con agencias internacionales —FBI e Interpol—, recibió información de acuerdo con la cual en un servidor conectado a la red desde la vivienda ubicada en la carrera 25, número 35-07 del municipio de Calarcá, Quindío, se estaba descargando material pornográfico con menores de edad:

> Ese contenido era la información que nos estaban aportando de que, en una casa puntual ubicada en el municipio de Calarcá, pues al parecer se estaba bajando contenido pornográfico con niños, niñas y adolescentes. Se estaba manejando desde ese punto, de esa conexión de Internet. (Declaración de Harold Gamajoa Velásquez)

Harold Gamajoa precisó que, además de la información suministrada por las nombradas agencias, una fuente humana, cuya identidad no reveló en juicio, corroboró dicha información.

En este punto, la Sala no pasa por alto que una fuente *anónima* de información no puede servir, por sí misma, «[…] *como indicio directo y único para la adopción de medidas restrictivas de los derechos fundamentales*»[18]; menos aún, emplearse como sustento basilar de un juicio de responsabilidad penal[19].

Este tipo de elementos, ha sostenido la Sala, puede emplearse para «[…] *realizar labores de verificación»,* e incluso puede «*dar lugar al inicio de una investigación penal*»; de

[17] Audiencia de juicio de 27 de junio de 2023, récord 00:06:22.
[18] CSJ SP7570-2016, rad. 40961.
[19] CSJ SP5798-2016, rad. 41667.

manera que se trata de medios con vocación estrictamente orientativa. [20]

En ese orden, ninguna irregularidad comporta que, en el caso sometido a estudio de la Sala, haya mediado una declaración de fuente anónima —*informante*—, ya que, como pasa de explicarse, los motivos fundados en que se sustentó el operativo de registro y allanamiento no solo comprendían esa declaración, sino la información suministrada por agencias internacionales.

Además, no sobra indicarlo, conforme lo ha precisado la Corte Constitucional[21], precisamente este tipo de información, «[…] *para efectos del decreto de un registro y allanamiento, cumple la única labor de servir de soporte para establecer con verosimilitud que existen motivos fundados para decretar una medida restrictiva del derecho a la intimidad*»; razón que afianza la licitud de la diligencia en que participaron los investigadores Brandon Beltrán Larios y Harold Gamajoa Velásquez.

4.2.2 Con fundamento en tales hallazgos, los investigadores solicitaron a la Fiscalía Primera Seccional CAIVAS de Armenia una orden de registro y allanamiento en el inmueble; procedimiento que se llevó a cabo sobre las 6:00 a.m. del 2 de agosto de 2018, en la carrera 25 n.° 35-07 de Calarcá, Quindío.

[20] Recientemente, CSJ SP598-2026, rad. 70393.
[21] CC C-673 de 2005.

De acuerdo con lo consignado en el informe y el acta de registro y allanamiento, incorporados por el investigador Brandon Lee Beltrán Larios, la diligencia fue atendida por ÁLVARO JAIME OSPINA RAMÍREZ, propietario y residente de la vivienda.

Durante el operativo, se recaudaron *(i)* un disco duro marca Maxtor, de 500 Gb, con número de serie 9QG95BDX —este dispositivo no se encontraba conectado a algún equipo—; *(ii)* un disco duro marca Toshiba de 2 Tb, serie 28P145ZAS 8CE; y *(iii)* un disco duro de de 2 Tb, marca Seagate, serie Z1EON9K6 —estos dos últimos estaban integrados a una torre de cómputo—.

4.3 **El contenido de los elementos incautados y la tipicidad de la conducta**

4.3.1 Sin perjuicio del problema jurídico que se plantea en los cargos (§ 4.1), el casacionista tampoco rebatió el *contenido* de las representaciones digitales contenidas en los dispositivos incautados.

4.3.2 A partir de lo expuesto en juicio por el perito en informática forense, Víctor Andrés Pimienta García[22], se conoce, entonces, que los tres dispositivos de almacenamiento incautados contenían, respectivamente, 68.157, 22.033 y 77.396 archivos de imagen y video.

[22] Audiencia de juicio de 8 de junio de 2023, audio 19:06

La extracción de esa información constituyó uno de los parámetros impartidos por el investigador Harold Gamajoa Velásquez, ya que durante la previsualización de contenidos informáticos que el nombrado funcionario llevó a cabo durante la diligencia de allanamiento y registro, pudo constatar, en sus términos: «*gran cantidad de imágenes fotográficas de una persona con características similares a un menor de edad […] esas imágenes, varias de ellas contenían carpetas al parecer con* ***menores de edad con algún tipo de actividad sexual***».

De acuerdo con el estudio forense realizado, el perito Pimienta García logró establecer que el *usuario* registrado en tales discos —así como su propietario— es ÁLVARO JAIME OSPINA RAMÍREZ.

4.3.3 Una vez que Víctor Andrés Pimienta García extrajo los archivos de los dispositivos de almacenamiento, procedió a copiarlos en ocho CD, elementos que el investigador Gamajoa Velásquez entregó al perito en morfología, Leonardo Castellanos Lopera.

Durante su intervención en juicio[23], el experto detalló las condiciones en que le fueron entregados los elementos para estudio y, seguidamente, se refirió al contenido de los datos informáticos analizados:

> **FISCAL**: usted ya recibe con todos los protocolos los elementos materiales probatorios una vez usted los tiene en su poder ¿cuál es el paso a seguir para realizar el análisis que le están solicitando?

[23] Audiencia de juicio de 8 de junio de 2023, récord 01:55:22.

> **LEONARDO CASTELLANOS**: se observan todas las carpetas y tienen una cantidad de imágenes, todas con **fotografías de seres humanos, en su mayoría, diría yo, el 98% fotografías de personas de sexo masculino en etapas desde la infancia hasta la adolescencia**. **Son fotografías reales de seres humanos, no son imágenes, caricaturas o de otro tipo**.
>
> […]
>
> **F**: ¿qué contenido tienen esas imágenes?
>
> **L.C**: el contenido es de **exposición de su cuerpo, digamos, de pornografía en menores**.

El análisis y sus conclusiones fueron consignados en el informe de investigador de laboratorio del 16 de octubre de 2018, expuesto por el perito durante el debate contradictorio. De esta manera, a partir de los indicadores morfológicos de desarrollo biológico—relación longitudinal entre ojos y cráneo, la proximidad de la base de la nariz con respecto al eje de los ojos, así como con la boca, la inserción capilar, el desarrollo del cuerpo y de los genitales, la densidad de vello púbico, entre otros—, pudo determinar que las personas fotografiadas, «*en su mayoría*», eran menores de 18 años:

> […] Los puedo ubicar en la etapa infantil porque ya en la etapa preadolescente comienzan a existir características, como el vello púbico, y comienzan a ser de una manera específica, no de cualquier manera, siempre comienza, por ejemplo, en los niños, en la base del pene y cuando ya va tomando mayor edad, este vello púbico se va extendiendo un poco hacia arriba, pero más hacia la parte horizontal, lo que nos va a indicar también en qué etapa pertenece. Y ninguna de estas imágenes de los niños nos muestran una intensidad púbica o digamos, de inserción capilar abundante, lo que nos indica que son menores de 18 años en su mayoría, y es más, menores de 13 años, porque en su gran mayoría de imágenes son niños que ni siquiera tienen esa etapa de inicio del vello púbico, ni sus genitales son totalmente desarrollados, porque consideremos que ya cuando el niño comienza esa edad de la adolescencia, los genitales crecen y son notables y en su gran

> mayoría, estos niños no tienen esas características, ni en otras partes del cuerpo, sus axilas ni su cara.

De hecho, precisó que cerca del 98% de los archivos estaban asociados a representaciones visuales de individuos de sexo masculino y el grueso de dichas imágenes correspondía, a su turno, a menores de edad que, por sus características morfológicas, se encontraban en *«etapa infantil dos»*, es decir, el grupo etario «*que va desde los nueve […] hasta los trece años*».

4.3.4 La Sala constata, en efecto, como bien se advierte en los informes elaborados y expuestos en juicio por los peritos Víctor Andrés Pimienta García y Leonardo Castellanos Lopera, la presencia de representaciones reales de niños y adolescentes completamente desnudos, exhibiendo sugestivamente sus órganos genitales e incluso, ejecutando intercambios eróticos —varias imágenes muestran a los menores practicándose felaciones recíprocamente—.

Algunos de esos archivos muestran a los menores en fotografías individuales, en parejas e incluso grupales, posando —acostados, de pie, abrazándose, sonriendo en algunas de ellas o con disfraces en otras— para quien realizó la toma; se itera, en las imágenes se muestra a las víctimas exhibiendo sus genitales de un modo que facilitaba su visualización.

Se descarta entonces, a partir de lo indicado, que la información recabada se trate de *(i) pornografía infantil técnica* —personas que no tienen la condición de ser menores de edad, pero que aparentan serlo; *(ii) pseudopornografía* —cuando se superponen

imágenes de menores en las representaciones reales de actividad sexual de personas mayores—; o bien, *(iii)* de *pornografía infantil artificial* —representaciones visuales elaboradas completamente a partir del uso de la tecnología—; circunstancias en las que, como se indicó en precedencia, no se configura el elemento normativo del tipo.

Tampoco resultaría oponible, para el caso concreto, el *consentimiento*. Si bien algunas de las imágenes corresponden a jóvenes de entre 14 y 18 años, grupo etario que, según se vio, ante una manifestación expresa de consentimiento, podría autorizar el *uso personal* de sus imágenes por parte de un tercero[24], lo cierto es que el grueso de las imágenes —decenas de miles de ellas— corresponden a menores de 14 años, de quienes no es predicable la capacidad de consentir sobre este tipo de actividades.

En este punto, ÁLVARO JAIME OSPINA RAMÍREZ, quien renunció a su derecho a guardar silencio, aseguró en juicio[25] que algunas de las imágenes contenidas en sus dispositivos de almacenamiento corresponden a un joven que fue su *pareja* y que, además, tenía 18 años.

Al relatar lo acontecido durante la diligencia de allanamiento, así como sus interacciones con el investigador Harold Gamajoa Velásquez, ÁLVARO JAIME explicó:

> […] Lo primero que hace [Gamajoa] es encontrar las fotos del ya mencionado compañero mío, que estaba en la cama mía con unas fotos, que para nada eran pornográficas, acepto que fueran eróticas. Y entonces me dice, «*mírelo, mírelo, 30 años de cárcel*». Y le dije, si mira la otra carpeta, se da cuenta que es mayor de

[24] CSJ SP239-2023, rad. 62461, ya citada.
[25] Audiencia del 13 de febrero de 2024, récord. 02:47:00

> edad, porque ahí le estábamos celebrando los 18 años y era antes de las fotos de la cama, que no hubiera necesitado que fuera mayor de edad para tomarle las fotos de la cama, era mi compañero, y no estaba haciendo nada de pornografía.

En tal contexto, al margen de que algunas de las fotografías hayan sido de una persona mayor de edad, lo cierto es que no por ello puede colegirse consentimiento de la totalidad de adolescentes que aparecen en las imágenes almacenadas en los dispositivos del procesado y, menos aún, justifica la presencia del ingente grupo de representaciones de menores de 14 años.

4.3.5 En síntesis, de los discos duros incautados, en los que estaba registrado como administrador y usuario ÁLVARO JAIME OSPINA RAMÍREZ, se extrajeron más de 160.000 archivos (§ 4.3.2), deliberadamente organizados y almacenados en los referidos dispositivos de hardware, contentivos de representaciones explícitas y reales de actividad sexual que involucraba menores de 18 años y, preponderantemente, de niños de 9 a 13 años.

Así las cosas, como bien lo concluyeron las instancias, estos elementos satisfacen la descripción contenida en el artículo 218 del Código Penal, en tanto elucidan una iconografía de seres humanos que ejecutaron comportamientos y adoptaron gestos orientados, sin dubitación alguna, a la estimulación sexual.

4.4 **Sobre la prueba de cargo y su mérito en el caso concreto**.

4.4.1 Como se ha indicado en precedencia, el casacionista denunció que: *(i)* una de las evidencias, puntualmente un disco duro incautado que no estaba conectado para el momento del allanamiento, se vinculó a los computadores de los investigadores, con lo cual quedó *viciada* la información; *(ii)* las imágenes recopiladas no se verificaron mediante protocolos de comprobación criptográfica —*hashes* MD5 y SHA1—, razón por la cual no existe certeza de que esos archivos sean los mismos que estaban almacenados en los discos duros; *(iii)* las marcas temporales detalladas en el informe de laboratorio elaborado por el perito forense, Víctor Pimienta García, dan cuenta de ingresos a los discos duros posteriores al momento en que se llevó a cabo el operativo de allanamiento; y *(iv)* la prueba digital no se obtuvo con sujeción a los protocolos de cadena de custodia aplicables, pues no se emplearon bloqueadores de escritura, como tampoco software certificado para ese propósito.

4.4.2 Como pasa de verse, los disensos que desarrollan los cargos propuestos conciernen, de un lado, a las actividades desplegadas por los servidores de policía judicial *durante* el procedimiento de allanamiento y registro; de otro, a los cuestionamientos sobre la *autenticidad* de la evidencia, propiamente.

Para un mejor desarrollo del asunto, indistintamente del cargo en que se desarrollen tales embates, la Sala estudiará por separado cada uno de los contextos descritos.

4.4.3 *Primer contexto*: *actividades de policía judicial durante el allanamiento.*

En el marco de la diligencia de allanamiento y registro realizada el 2 de agosto de 2018, participó, entre otros servidores, el investigador Harold Gamajoa Velásquez, ingeniero de sistemas con especialización en gerencia informática y maestría en ciberseguridad.

En cuanto es de interés, durante el contrainterrogatorio practicado por la defensa[26], el policial, entre otras cosas, manifestó haber conectado uno de los discos duros incautados, concretamente el de marca Maxtor —evidencia n.° 1—, que no se encontraba vinculado a ningún dispositivo de cómputo, a los computadores que los servidores de policía judicial llevaban consigo:

> DEFENSA: ¿cómo conectó los elementos para **visualizar** lo que tenían en su interior.
>
> HAROLD: Con una forma esclavo, lo que se hace es conectar un cable de corriente que le va a permitir la corriente al disco duro y un cable que le va a permitir la conexión tipo USB al disco duro.

De acuerdo con lo anterior, las labores de visualización a que aludió el deponente se circunscriben a las actividades de

[26] Audiencia de juicio de 27 de junio de 2023, récord 43:00.

identificación preliminar de la evidencia, de las que ya ha hecho referencia la Sala.

En tal medida, como acertadamente lo expresaron la Fiscalía y la representación del Ministerio Público en condición de no recurrentes, no se trataba de una acción constitutiva de *extracción* o *análisis* forense, sino de una observación preliminar orientada a establecer cuáles elementos se incautarían; precisamente, el profesional Gamajoa Velásquez enfatizó: «*yo no iba a hacer una imagen, o bien, una copia espejo*».

Bajo esa lógica, los procedimientos que el censor juzga irregularmente pretermitidos, puntualmente el uso de un bloqueador de escritura, la imagen *bit a bit* o la verificación de la integridad de los datos, no eran propios de la referida fase de constatación de la información; y, en todo caso, como se verá más adelante, dichos protocolos sí fueron empleados durante el *análisis* de la información.

De otra parte, las marcas temporales de ingreso posterior a los discos duros, descritas en el informe presentado por el perito forense Víctor Pimienta, que el recurrente capitaliza como indicio de manipulación de la evidencia, carecen del alcance pretendido por el censor.

Aun cuando tales reparos no fueron desarrollados durante el interrogatorio cruzado, un estudio conjunto de esos hallazgos permite deducir fundadamente que los registros de ingreso al disco de marca Toshiba —detallados a página 9 del

informe de laboratorio suscrito por el perito Víctor Pimienta García—, verificados a las 06:16:47, 06:22:59 y 07:50:17 del 2 de agosto de 2018, lejos de conferirle mérito a la hipótesis alternativa de una implantación de evidencia, en realidad son compatibles con las labores lícitas de *visualización previa* llevadas a cabo durante la diligencia de allanamiento.

Así las cosas, contrario a lo expresado por el recurrente, ninguna irregularidad sustancial se verificó en el ámbito de la previsualización de la evidencia. En su lugar, a partir de lo que permiten conocer las pruebas, se puede establecer que:

(i) La previsualización de la evidencia fue dirigida por un profesional capacitado para el manejo de evidencias digitales —el investigador Harold Gamajoa Velásquez—.

(ii) Dicha actividad se limitó a la *observación* del contenido de los discos duros que se encontraban en la vivienda del procesado, con el objetivo de *identificar* la evidencia y determinar su utilidad para la investigación posterior, de conformidad con las previsiones del artículo 205 de la Ley 906 de 2004.

(iii) Aun cuando no se emplearon en ese momento protocolos de bloqueo de escritura o autenticación digital, el profesional Harold Gamajoa expresó, puntualmente durante sus respuestas en el contrainterrogatorio de la defensa, que utilizó el software FTK Lite Imagine, versión 3.1.1, que permite, en sus términos, «*revisar el contenido del archivo como si fuera también una imagen, un programa o un Word, visualizar la*

información, pero ***no se está modificando ningún tipo de archivo***»; aserto que se consignó igualmente en el punto 4° del informe perito de laboratorio —página 1 del documento—, elaborado el 2 de agosto de 2018 por el nombrado profesional.

En tal contexto, el procedimiento de auscultación ejecutado por el investigador estuvo enfilado a preservar la indemnidad de la información recaudada.

(iv) No se verificó la presencia de información digital —por ejemplo, la almacenada en memoria RAM— que, en virtud de un cambio en el estado del dispositivo de almacenamiento, fuera susceptible de alteración ——riesgo de *volatilidad*—.

(v) Los procedimientos adelantados durante la diligencia de allanamiento y registro, por lo que se ha expuesto, quedaron en debida forma documentados —auditabilidad—.

(vi) Como expresamente lo indicó el investigador Gamajoa, en concordancia con las observaciones contenidas en el informe por él elaborado, luego de la visualización preliminar de los archivos levantó la correspondiente acta de incautación y sometió los elementos a cadena de custodia.

De acuerdo con lo anterior, para la Sala es claro que las actividades desarrolladas por los miembros de policía judicial, *durante* el operativo de allanamiento, se plegaron a los estándares técnicos mínimos que garantizan la indemnidad de los datos informáticos (§ 3.5.1, 3.6), a lo cual se suma que, como bien lo expresó el Tribunal, no se constató que durante

dicho operativo se verificara la alteración de los datos informáticos recaudados.

En consecuencia, los reproches que sobre el particular propuso el libelista, devienen infundados.

4.4.4 *Segundo contexto: sobre la extracción, análisis y autenticación de la evidencia digital.*

Los reparos propuestos por el libelista en torno al particular se fundamentaron, esencialmente, en las conclusiones presentadas en juicio por el perito de la defensa, Andrés Felipe Giraldo Montoya[27], ingeniero de sistemas y magister en ciberseguridad.

El demandante, según se anunció en líneas precedentes, denunció que la *autenticidad* de la evidencia digital recabada en la diligencia de allanamiento no se acreditó debido a la falta de aplicación de los protocolos de comprobación criptográfica —*valores hash* MD5 y SHA1—, sumado a lo cual no se aplicaron los reglamentos técnicos para el manejo de ese tipo de elementos.

De acuerdo con las precisiones que se han desarrollado en precedencia (§ 3.3, 3.4, 3.5), la autenticación de la *evidencia digital* constituye una exigencia que la parte interesada en su aducción debe satisfacer en orden a acreditar que lo recaudado en el marco de la investigación corresponde a lo que se

[27] Audiencia de juicio de 13 de febrero de 2024, récord 06:00.

presenta en el debate como sustento de la acusación o de la hipótesis alternativa.

La observancia de esa ruta metodológica, pues, más que una obligación formal, constituye un presupuesto ligado al reconocimiento de la eficacia y el mérito suasorio del elemento —más que su admisibilidad como prueba— que, en el ámbito de la prueba digital, en tanto equivalente funcional del documento, se itera, se satisface idealmente con la intervención del experto, en los términos del art. 426.4 del C.P.P.

Ahora bien, contrario a lo expresado por el casacionista, la Fiscalía satisfizo tal carga.

En efecto, luego de que los discos duros se aseguraran en desarrollo del operativo, la extracción y el análisis de la información allí contenida estuvo a cargo, como se dijo (§ 4.3.2), del perito Víctor Andrés Pimienta García.

De acuerdo con lo manifestado por el experto, quien expuso el contenido del informe de investigador de laboratorio FPJ-13 de 24 de septiembre de 2018[28], tales elementos se le entregaron embalados y rotulados, en virtud de su sometimiento previo a cadena de custodia. Tras fijar fotográficamente e identificar los dispositivos puestos a su disposición, explicó el procedimiento de análisis y extracción.

[28] Audiencia de 8 de junio de 2023, récord 00:28:19.

a. Conectó los discos duros examinados a un *bloqueador contra escritura*, es decir, «*un dispositivo físico de hardware*» que protege la evidencia digital de modificaciones o su eliminación.

b. Realizó una copia *bit a bit* de los discos, es decir, una *imagen forense* del dispositivo que, en términos del profesional, consiste en una *clonación* del contenido. De acuerdo con lo expuesto por el perito, el análisis y extracción de este tipo de evidencia no se realiza directamente sobre el disco, sino sobre una copia, metodología que se emplea para «*proteger esa evidencia digital*».

c. Obtenida la imagen forense, procedió a verificar la integridad de los datos informáticos copiados «*a través de unos procedimientos que se denominan sumas de verificación*», esto es, en sus términos, una suerte de «*firmas digitales*» o valores Hash —que el informe de laboratorio identificó como *«formato Hash MD5 y SHA1»*[29]—, es decir, como se ha visto, secuencias algorítmicas que permiten establecer si un dato ha sido modificado.

d. Sobre la imagen forense, el perito extrajo la información requerida por el investigador Harold Gamajoa Velásquez, concretamente, imágenes y videos de contenido sexual, información que, a su turno, aquel exportó en 8 CD, que fueron sometidos a cadena de custodia y remitidos, como antes se detalló, ante el perito en morfología, Leonardo Castellanos Lopera (§ 4.3.3).

[29] Página 2 del informe de investigador de laboratorio elaborado por el perito forense Víctor Pimienta García.

A partir de lo expuesto, la Sala encuentra que la Fiscalía autenticó, en desarrollo del debate contradictorio, la evidencia digital recuperada en los discos de propiedad de ÁLVARO JAIME OSPINA RAMÍREZ. Ciertamente, se pudo comprobar:

(i) El origen de la información. La prueba reseñada permite conocer que las representaciones de actividad sexual en la que aparecen menores de 18 años —circunstancia que el casacionista no controvirtió—, se encontraban almacenadas en los tres discos duros incautados en la vivienda del procesado, dispositivos que, además, estaban registrados a su nombre y en los que ÁLVARO JAIME OSPINA RAMÍREZ figuraba como *administrador* o *usuario*.

(ii) La integridad de los datos. De acuerdo con el procedimiento de análisis de la información digital, en el que se emplearon *sumas de verificación*, se estableció que los archivos no fueron modificados. La implementación de la aludida secuencia algorítmica le permitió al perito Víctor Pimienta García constatar, de un lado, que la copia *bit a bit* de la información fue satisfactoria, de otro, generar una «*firma digital*» de los archivos que exportó a los CD que, ulteriormente, se remitirían ante el perito en morfología. Precisamente en el acápite de anexos del informe suscrito por Pimienta García, uno de los elementos relacionados fue, precisamente, el archivo «*sumas de verificación información exportada.xlsx* ».

(iii) La mismidad de la evidencia. Por lo anterior, la evidencia incorporada a instancia de la Fiscalía y que sirvió de base al Tribunal para estructurar las correspondientes

inferencias probatorias, fue la misma que se incautó durante la diligencia de allanamiento realizada el 2 de agosto de 2018, en la vivienda de ÁLVARO JAIME.

Por lo que pasa de explicarse, no es cierto, como lo denuncia el libelista, que en el proceso de análisis y extracción de la evidencia digital los servidores de policía judicial hayan pretermitido la aplicación de las medidas técnicas de protección necesarias para garantizar la indemnidad de la información recaudada.

Por el contrario, el tratamiento que los investigadores le impartieron a los datos informáticos supuso la implementación de *bloqueadores de escritura* —como medida de protección para evitar eliminación o alteración del dato— y, asimismo, la aplicación de *sumas de verificación* en formato *Hash MD5 y SHA1*, como herramienta para establecer la huella digital de los archivos y comprobar su inalterabilidad.

4.4.5 En lo que concierne a la falta de aplicación de la Guía n.º 13 de Evidencia Digital del MinTIC y el Manual del Sistema de Cadena de Custodia de la Fiscalía, el reproche tampoco elucida aptitud sustancial.

Por un lado, el casacionista pretermitió explicar si las disposiciones contenidas en tales compendios resultaban temporalmente aplicables al procedimiento de análisis de evidencia digital realizado en el caso concreto —vigencia—; tampoco precisó cuáles eran los protocolos puntuales que debían aplicarse de conformidad con tales reglamentos y,

menos aún, explicó, con sujeción al principio de trascendencia, cómo la implementación de tales derroteros habría incidido en el sentido de la decisión adoptada por los falladores.

Al margen de tales deficiencias, los reglamentos técnicos, en tanto lineamientos enfilados a mejorar —en este caso— las prácticas forenses, no se instituyen como mandatos cuya pretermisión tenga entidad para viciar la prueba —como parece comprenderlo el libelista—.

Así pues, en lo que atañe a la valoración de la *prueba digital*, los parámetros que debe observar el funcionario judicial al momento de determinar su eficacia (§ 3.3) y evaluar su mérito, como ya se indicó y lo ha decantado la Sala[30], corresponden a los de confiabilidad, integralidad, inalterabilidad, accesibilidad, auditabilidad y repetibilidad.

Por tanto, más que la aplicación de determinados protocolos, métodos o recomendaciones para el manejo de la evidencia, lo relevante es que la parte interesada en su aducción acredite:

> […] las condiciones técnicas en las que la recolectó, [describa] de forma completa las características que la identifican, [garantice] que la evidencia no presentó alteraciones en su embalaje o transporte y [muestre] la trazabilidad de su conservación en orden a probar que la evidencia es lo que la parte dice que es.[31]

En el asunto que concita la atención de la Sala, la Fiscalía acreditó que la información recaudada durante el allanamiento

[30] CSJ SP248-2025, rad. 58275.
[31] CSJ SP1284-2025, rad. 38784.

y registro fue sometida al procedimiento de cadena de custodia en el marco de la investigación y, adicionalmente, como se ha expuesto, *autenticó* el contenido de la evidencia digital durante el juicio oral.

En tales condiciones, satisfizo las exigencias técnicas necesarias para demostrar la eficacia y el mérito demostrativo de las representaciones fotográficas incorporadas.

4.4.6 Con todo, el Tribunal no incurrió en yerros de contemplación o valoración probatoria, al conferirle pleno valor demostrativo a la prueba digital practicada por la Fiscalía.

Por el contrario, el razonamiento entronizado en la demanda, esto es, en esencia, la supuesta existencia de «*indicios claros de alteración de la evidencia*», no trasciende del plano especulativo, pues la información digital incorporada y los métodos de los que se sirvieron los investigadores de policía judicial para obtenerla, extraerla y analizarla, se adecuaron a las exigencias procedimentales inherentes a la naturaleza de tales elementos.

Ahora bien, que el Tribunal no le haya conferido mérito a la intervención del perito Andrés Felipe Giraldo, convocado por la defensa, tampoco constituye un yerro censurable en sede casacional.

Por un lado, como bien lo resaltó el *ad quem*, el perito nombrado admitió, en su intervención en el debate[32], no haber verificado directamente la evidencia recabada por la Fiscalía.

[32] Audiencia de juicio de 13 de febrero de 2024, récord. 06:23.

> **DEFENSA**: ¿qué elementos recibió para esa misión de trabajo?
>
> **ANDRÉS GIRALDO**: Recibí el informe del investigador de campo de fecha del 2 de agosto del 2018. El registro fotográfico de la orden de allanamiento y el informe del investigador de laboratorio de fecha del 16 de octubre del 2018. Esos fueron los documentos para la misión de trabajo de los cuales se hizo el análisis y la revisión. **Cabe aclarar que nunca tuve acceso a los discos duros ni a las unidades de almacenamiento de las que habla este informe** porque hacían parte de la reserva del del proceso.

De tal suerte, al limitar el análisis a los informes aludidos, el profesional no estuvo en capacidad de determinar si en el marco de la diligencia de allanamiento se verificó una *alteración* o *implantación* de la evidencia digital presentada por la acusación —hipótesis en la que se sustenta primordialmente la demanda—. Precisamente, en el contrainterrogatorio practicado por la Fiscalía, el testigo admitió:

> **FISCAL**: Y respecto de la incautación del elemento realizado por Harold, **usted no puede asegurar que hubo alteración, modificación o supresión de esa información, ¿cierto que no?**
>
> **ANDRÉS GIRALDO**: **Ni yo ni el perito de Manizales podría determinarlo**.

En similar sentido, manifestó no conocer con certeza si se utilizó en algún momento el software FTK —empleado por Harold Gamajoa para proteger de alteraciones la evidencia digital en el momento de la previsualización de los archivos— («*pues yo creería que no se usó*», dijo); tampoco estuvo en capacidad de establecer si los rótulos de cadena de custodia de las evidencias eran coincidentes, al punto de admitir que «*esa parte no está consignada dentro del informe que realicé*».

De igual forma, en lo que concierne a la *integridad* de la información, el experto reprochó —como lo hace ahora el casacionista— que «*las sumas de comprobación [debían] haberse tomado con los equipos especializados* ***en el momento en que se hizo el procedimiento de allanamiento***». No obstante, en ulterior respuesta aseguró, contradictoriamente, que dicho método de autenticación «***generalmente, [...] no se hace en campo****, a no ser que yo tenga los dispositivos especializados para tal misión*».

De hecho, en respuestas posteriores, el testigo reconoció que, de acuerdo con la información contenida en el informe de laboratorio elaborado por el perito forense Víctor Pimienta García, durante el procedimiento de análisis de evidencia digital «*se cumplieron [...] los requisitos técnicos*»; aseguró asimismo que Pimienta García sí realizó las sumas de comprobación; y ratificó que el FTK, utilizado por el investigador Gamajoa Velásquez durante el allanamiento, «*es un software que en realidad* ***apoya las labores de campo***».

En las condiciones descritas, contrario a lo pretendido por la defensa y como acertadamente lo enfatiza la Fiscalía en condición de no recurrente, el valor demostrativo del dictamen presentado como sustento de la hipótesis alternativa, resultaba sin lugar a duda escaso. Además, lo que en ciertos fragmentos de la declaración del experto se da a entender es que los servidores de policía judicial satisficieron las exigencias técnicas para la previsualización de la evidencia, así como para su análisis y extracción.

4.4.7 Por lo expuesto en precedencia, los cargos formulados por el defensor de ÁLVARO JAIME OSPINA RAMÍREZ no están llamados a prosperar.

5. Conclusiones

5.1 Tras delimitar las reglas normativas y jurisprudenciales aplicables al tratamiento de la evidencia y la prueba digital (§ 3.2 - 3.6), la Sala pudo establecer, para el caso concreto, que tanto en la fase de *previsualización* de la información recaudada (§ 4.4.3), como en su análisis forense, su extracción y la autenticación en juicio (§ 4.4.4), la Fiscalía acreditó el cumplimiento de los parámetros técnicos dispuestos para asegurar la integridad, confiabilidad, autenticidad y la accesibilidad de la información digital recabada.

A partir de tal análisis, se concluye que los reparos formulados por el casacionista, al margen de las deficiencias técnicas de las que adolece, resultan sustancialmente infundados.

5.2 En tales circunstancias, ningún desafuero concita la decisión proferida en segunda instancia por el Tribunal, habida cuenta que las pruebas con fundamento en las cuales halló demostrada la materialidad de la conducta objeto de juzgamiento (§ 4.3) y la responsabilidad del procesado, aspectos que no cuestionó el libelista, contaban con eficacia y mérito demostrativo.

5.3 De este modo, la Fiscalía demostró, más allá de duda razonable, que ÁLVARO JAIME OSPINA RAMÍREZ almacenaba una significativa cantidad de representaciones *reales* —más de 160.000— de actividad sexual explícita que involucraba menores de edad, principalmente, niños de 9 a 13 años.

5.4 La Sala, en consecuencia, no casará la sentencia demandada.

En mérito de lo expuesto, la **SALA DE CASACIÓN PENAL DE LA CORTE SUPREMA DE JUSTICIA**, administrando justicia en nombre de la República de Colombia y por autoridad de la ley,

VIII. RESUELVE

1. NO CASAR la sentencia demandada.

Contra esta decisión no proceden recursos.

Notifíquese y cúmplase.

CARLOS ROBERTO SOLÓRZANO GARAVITO
Presidente de la Sala

MYRIAM ÁVILA ROLDÁN

GERARDO BARBOSA CASTILLO

FERNANDO LEÓN BOLAÑOS PALACIOS

GERSON CHAVERRA CASTRO

DIEGO EUGENIO CORREDOR BELTRÁN

JORGE HERNÁN DÍAZ SOTO
No firma en comisión de servicios

HUGO QUINTERO BERNATE

JOSÉ JOAQUÍN URBANO MARTÍNEZ

Este documento fue generado con firma electrónica y cuenta con plena validez jurídica, conforme a lo dispuesto en artículo 103 del Código General del Proceso y el artículo 7 de la ley 527 de 1999

Código de verificación: B50FE7068B704944E67AAD58218C6535CF3F28C513D7203F5E1EA32126D8120B
Documento generado en 2026-08-21