¿Debe el código procesal penal reconocer expresamente la evidencia digital? vacíos normativos, propuestas y estándares mínimos de cadena de custodia digital en el proceso penal peruano

Should the criminal procedure code expressly recognize digital evidence? Regulatory gaps, proposals, and minimum standards for digital chain of custody in the Peruvian criminal process

Ismael Escalante Huamani [1]

Resumen

La evidencia digital como (mensajes, registros de geolocalización, correos, videos, fotografías, capturas de pantalla, etc.), se ha vuelto habitual en la litigación penal de nuestra región, pero su tratamiento, si hacemos una mirada a nuestro estatuto procesal, sigue dependiendo en gran medida de las reglas generales de prueba documental, pericia y de cadena de custodia concebidas para evidencias físicas. En este artículo sostendremos que es inminente el reconocimiento expreso y explícito en nuestro estatuto procesal, siempre que se haga con técnica legislativa compatible con la libertad probatoria y con los estándares mínimos internacionales de integridad, autenticidad, trazabilidad, reproducibilidad y auditabilidad.

Palabras clave: *Evidencia digital, cadena de custodia digital, estándares mínimos y estatuto procesal.*

Abstract

Digital evidence (such as messages, geolocation records, emails, videos, photographs, screenshots, etc.) has become commonplace in criminal litigation in our region. However, its treatment, as we examine our procedural code, still largely depends on the general rules of documentary evidence, expert testimony, and the chain of custody designed for physical evidence. In this article, we argue that its express and explicit recognition in our procedural code is imminent, provided it is done with legislative technique compatible with the freedom of proof and with minimum international standards of integrity, authenticity, traceability, reproducibility, and auditability.

Keywords: *Digital evidence, digital chain of custody, minimum standards, procedural code.*

---

[1] Abogado en litigios penales con estudios concluidos de la maestría de ciencias penales en la UNSCH y en derecho constitucional en la UNFV. Correo: Ismael.isbema@gmail.com.

I. Introducción

El punto de partida que me motivó a escribir el presente artículo es, inevitablemente, el artículo 156 inciso 1) del Código Procesal Penal, que formula una cláusula amplia de libertad probatoria, donde se establece como regla general que los hechos que se refieran a la imputación, la punibilidad y la determinación de la pena o medida de seguridad, así como los referidos a la responsabilidad civil, pueden acreditarse por cualquier medio permitido por el estatuto procesal penal y que, en su defecto, se recurra a la adecuación al medio más análogo.

Sin embargo, cuando la fuente probatoria es digital, el litigio penal enfrenta problemas propios como: facilidad de alteraciones sin huella visible, multiplicidad de copias indistinguibles, necesidad de herramientas forenses, riesgos de contaminación por manipulación del dispositivo o del archivo y, últimamente, el uso de inteligencia artificial para la creación de evidencias digitales. Todo ello lo estamos viviendo en el día a día del quehacer jurídico: fiscalía, defensa y juez discutiendo la autenticidad de chats o capturas de pantalla, y la intensidad aumenta en las audiencias de prisión preventiva, donde la libertad está a poco de cruzar la línea de ser restringida, muchas veces con graves y fundados elementos digitales sin seguir un protocolo de custodia propiamente dicho para las evidencias digitales y sin el tratamiento de un perito. Por ello, la evidencia digital es, por definición, más volátil que el cuerpo del delito físico.

Ante este panorama, el procesalista penal no puede seguir mirando de reojo la transformación digital; por ello cabe preguntarse: ¿si el Código Procesal Penal debe reconocer expresamente la evidencia digital y regular un estándar mínimo de cadena de custodia digital?, o ¿seguir adecuando y practicando las reglas que trajo nuestro estatuto procesal para las evidencias físicas más la práctica pericial?

Los problemas descritos permiten adelantar una tesis clara; por lo que, mediante el presente artículo, defendemos que es inminente el reconocimiento expreso y explícito en nuestro estatuto procesal, siempre que se haga con técnica legislativa compatible con la libertad probatoria, así evitar causalidades automáticas de exclusión, y con los estándares mínimos internacionales de integridad, autenticidad, trazabilidad, reproducibilidad y auditabilidad.

Más aún, si nuestro país ha aprobado y ratificado el Convenio de Budapest en el año 2019, el dato no es solo cronológico sino normativo, porque nuestro país pensó con la ratificación de la convención el deber de adaptar su procedimiento penal en los delitos cibernéticos y, sobre todo, cuenta con la Ley de Delitos Informáticos (Ley Nº 30096). Por tanto, el retraso de nuestro Código Procesal Penal frente a estas obligaciones resulta ya difícil de justificar; por tanto, es momento de que la evidencia digital sea reconocida expresamente por nuestro estatuto procesal para el tratamiento adecuado. Por ello, veremos primero sobre los vacíos y fricciones que tiene nuestro estatuto procesal penal respecto a la evidencia digital, luego las propuestas que surgieron para poder positivizar en el estatuto procesal, y en base a ello haremos saber nuestra postura con los estándares mínimos de cadena de custodia digital.

II. Desarrollo

II.1. Vacíos y fricciones para el tratamiento de la evidencia digital

En nuestro país existen instrumentos institucionales para el manejo técnico de evidencias digitales, como el Manual para el recojo de la evidencia digital aprobado por la Resolución Ministerial Nº 848-2019-IN, orientado a unificar criterios de la PNP para recojo de dispositivos (celular, laptops, USB) y preservar su contenido como evidencia durante la investigación. Sin embargo, se trata de un instrumento administrativo dirigido a la PNP, no a jueces ni fiscales, lo cual inminentemente condiciona su alcance procesal.

La existencia de un manual operativo es valiosa, pero no sustituye la norma procesal:

> El debate probatorio ocurre en sede fiscal y judicial, donde lo decisivo es la admisibilidad, autenticidad y valoración conforme a garantías y estándares de motivación. En el mismo sentido, existe cantidad de procesos que origina lagunas como consecuencia de la aplicación de la normativa procesal escrita para la evidencia física, y no para la evidencia digital (Piccirilli, 2019, pág. 7).

Siguiendo la línea del autor, insistimos en que las categorías pensadas para la evidencia física terminan produciendo zonas ciegas en la evaluación judicial de lo digital, por ejemplo, una situación típica es que no existe impugnación de chats, audios de WhatsApp o videos extraídos sin código hash.

> En la práctica cotidiana, muchos operadores de justicia siguen leyendo la evidencia digital como si fuera papel: capturas impresas, imágenes en pantallas de celular, etc.
> La administración de justicia requiere de profesionales informáticos preparados que examinen y cotejen las pruebas aportadas por las partes, dentro del entorno informático, protegiéndolas de las modificaciones a las que se exponen, dándole un entorno de autenticidad en la fase probatoria, y auxilio a los operadores de justicia incorporando conocimiento técnico en el uso de los medios digitales (Alfonso, 2021, pág. 29-30).

Por ello, en las clases, diplomados, talleres y cursos de litigio penal los casos de chats falsificados generan mayor inseguridad.

> En el Perú no existe norma procesal que estandarice la recolección, obtención, conservación y análisis de la evidencia digital; asimismo, la carencia de tecnología de dispositivos informáticos, aplicaciones, licenciamientos y la demora en el trabajo de pericias sobre evidencia digital, así como la falta de formación de los operadores de justicia y cuerpos policiales en técnicas de tratamiento de la evidencia digital respecto a la obtención, recolección, conservación y análisis, que permitan asegurar su originalidad (Silva, 2021, pág. 26).

En esa línea, cabe indicar que el vacío normativo y déficit tecnológico convierte la cadena de custodia digital en una ficción más que un estándar operativo para llegar a la verdad procesal que todos los sujetos procesales anhelamos.

A nivel jurisprudencial, el VIII pleno jurisdiccional supremo penal (Acuerdo plenario Nº 06-2012/CJ-116) reconoce la cadena de custodia como procedimiento destinado a garantizar

la autenticidad y conservación de los elementos materiales, y precisa que su ruptura no determina automáticamente la inadmisibilidad o ineficacia probatoria, pues puede ser subsanable por otros medios de autenticación. Este estándar es razonable para la evidencia física, pero resulta insuficiente si no se precisan mínimamente las formas de autentificación digital; por tanto, obliga a los magistrados a reunirse y tratar temas concernientes a las evidencias digitales y su tratamiento.

El problema aparece cuando se intenta trasladar mecánicamente esa doctrina al universo digital, doctrina que fue construida principalmente pensando en el estatuto procesal de 2004 para el tratamiento del cuerpo del delito y evidencia física; trasladarla a evidencia digital sin reglas mínimas de adquisición, verificación y trazabilidad técnica genera incertidumbre, lo cual en el litigio penal no mejora para la búsqueda de la verdad procesal que anhelan los sujetos procesales (fiscales, abogados litigantes y jueces), tampoco protege de manera adecuada los derechos fundamentales.

Ante ello cabe indicar que, mientras escribía este artículo, la Corte Suprema, con la ponencia del juez supremo Luján Túpez, resuelve el siguiente interrogante: ¿Es necesario un perito en la diligencia fiscal de obtención de pantallazos o screenshots cuando el móvil se entrega voluntariamente? La respuesta fue que no, precisando el siguiente argumento:

> (…) la obtención de pantallazos o screenshots de su contenido, es decir, se trata de actos fiscales de naturaleza descriptiva y de constatación, lo cual no requiere conocimientos especializados científicos, técnicos o artísticos. La simple realización de actas de visualización del contenido accesible directamente del dispositivo celular con anuencia de su titular solo constituye un acto documentado. Pues, en realidad, la tarea asignada a la Fiscalía es examinar los documentos y los soportes electrónicos de almacenamiento, cuyo registro implica tomar conocimiento del contenido de los documentos o soportes de almacenamiento para examinar si son admisibles y utilizables en un futuro como prueba de cargo; solo la información pertinente para el procedimiento y utilizable debe permanecer disponible para un análisis permanente y exhaustivo. (Corte Suprema de Justicia de la República. Sala Penal Permanente. Recurso de apelación Nº 38-2025. Suprema; de 18 de noviembre de 2025).

Dicho argumento, tomando los criterios de las evidencias físicas, encajaría perfectamente para resolver el interrogante que hemos realizado líneas arriba; sin embargo, en el presente artículo sostengo que la obtención de las evidencias digitales, sin importar su naturaleza, se debe realizar con un experto o técnico por la sencilla razón: los actos fiscales de naturaleza descriptiva y de constatación, como lo llama la Corte Suprema, que se practica sobre un teléfono o móvil, mínimamente deben respetar los estándares para la obtención de información como la confiabilidad, es decir identificar el dispositivo, contexto, la trazabilidad del contenido observado, forma de registro, más aún si en etapa intermedia se va a postular y se va a actuar en juicio. A ello sumamos que, si se va a tomar como un documento, no cabría la cadena de custodia, pero recordemos que la información está siendo obtenida de un dispositivo, por lo que es necesaria una cadena de custodia para posterior análisis de la integridad.

La revisión de normativa, práctica judicial y literatura especializada permite identificar un vacío central, que es la falta de modificación del tratamiento de la evidencia digital en nuestro país y falta de protocolo de hash (huella digital) obligatorios para garantizar la

integridad. A diferencia de un arma de fuego, un archivo PDF, un video, una captura de pantalla, etc., puede ser modificado sin dejar rastro visible si no se utiliza un software forense desde el inicio del tratamiento de la evidencia digital.

II.2. Propuestas

El 1 de julio de 2025 el Congreso ha recibido el proyecto de Ley Nº 11815/2024-CR, suscrito por el congresista José Luna Gálvez, que busca incorporar la evidencia digital al Código Procesal Penal, regulando su tratamiento, identificación, adquisición, preservación, análisis y presentación. Según este texto divulgado, se plantea definir la evidencia como prueba documental en soporte electrónico, regular la cadena de custodia digital con obligación de documentar actos, software, medios de almacenamiento y códigos hash y, finalmente, exigir que el peritaje informático forense lo realice un especialista con métodos y programas reconocidos por la comunidad científica.

Asimismo, esta iniciativa legislativa insiste en trabajar con la fuente original para evitar cuestionamientos de confiabilidad y propone restricciones como impedir la traducción, transcripción o visualización cuando no existe esa fuente original.

Efectivamente, esta iniciativa es de suma importancia para el tratamiento de la evidencia digital, pero peca en proponer la rigidez de la fuente original, porque prohíbe pericias o visualizaciones si no existe la fuente original.

En la práctica se ha visto que la fuente original puede ser volátil, porque se puede encontrar en servidores en la nube, mensajes efímeros o datos en memorias caché, por lo que impedir el uso de copias espejo que pueden preservar la integridad del dato original podría invalidar investigaciones legítimas donde el dispositivo físico se perdió o fue destruido.

De la misma forma, cabe indicar que el proyecto y los futuros no solo deben centrarse en los dispositivos físicos, sino también en incluir un apartado sobre la obtención de evidencias en la nube, porque la práctica digital nos ha enseñado que actualmente ya nadie usa o almacena su información en los famosos USB o memorias, sino en la nube, correo, drive, etc. Y, finalmente, precisar que no se puede ver a la inteligencia artificial como una amenaza, sino un aliado más para luchar contra los mismos.

Por otro lado, «el Ministerio de Justicia informó que el Consejo Nacional de Política Penal aprobó un proyecto de ley orientado a regular la preservación, obtención y aseguramiento de evidencia digital, lo que evidencia que el tema ya está en agenda estatal y no académica» (Ministerio de Justicia, 2025, 07 de noviembre de 2025).

II.3. Nuestra postura

En un contexto donde las relaciones interpersonales y las conductas delictivas se manifiestan predominantemente a través de las tecnologías de la información y comunicación (TIC), resulta imperativo que nuestro estatuto procesal penal incorpore un reconocimiento expreso de la evidencia digital. Dicha positivización no solo fortalecería la predictibilidad jurídica, sino que permitiría delimitar con precisión su alcance, los estándares mínimos de acreditación y el trato documental exigible desde la incautación hasta su valoración en juicio.

La inclusión de disposiciones específicas sobre evidencia digital garantiza la seguridad al establecer un marco reglado para su obtención y tratamiento; también reduce el margen de decisiones dispares basadas solo en instituciones tecnológicas y permite que los sujetos procesales, básicamente fiscalía y defensa, litiguen con reglas claras sobre autenticidad, integridad y trazabilidad.

No obstante, el diseño normativo debe ser cuidadoso, porque si se absolutiza la fuente original como condición rígida, se puede volver impracticable probar hechos digitales y se corre el riesgo de exclusiones probatorias desproporcionadas.

En esa línea, es fundamental que la reforma armonice con el criterio vinculante del Acuerdo Plenario Nº 06-2012/CJ-116, bajo la premisa de que las irregularidades en la cadena de custodia no deben precipitar una nulidad automática. Por el contrario, estas deben activar un escrutinio reforzado de autenticidad y confiabilidad, garantizando siempre el principio de contradicción y una debida motivación judicial.

Es decir, el juzgado debe optar por un control riguroso de la integridad del elemento de prueba antes que por la exclusión formal, salvaguardando el derecho de defensa mediante un debate contradictorio y la justificación de la decisión judicial.

II.4. Estándares mínimos de cadena de custodia digital

La propuesta legislativa líneas arriba ya apunta a elementos claves como registro de actos, software, medios de almacenamiento, códigos hash y responsables, como parte de la cadena de custodia digital.

Estos elementos claves deben tener una armonía con estándares internacionales como la norma ISO/IEC 27037, que ofrece guías y directrices para la identificación, recolección, adquisición y preservación de evidencias digitales, y resalta la necesidad de procedimientos repetibles y auditables en el manejo de evidencias.

Asimismo, los principios del IOCE (aprobados en 1999) insisten en que las acciones no deben cambiar la evidencia, que quien accede al original debe ser competente, que todo debe documentarse y preservarse para revisión y que existe un responsable por las acciones realizadas sobre la evidencia bajo su custodia.

Los estándares mínimos recomendables para nuestro estatuto procesal peruano, tomando algunas reglas y principios de las evidencias físicas que puedan ser verificables en juicio, son:

A. **Legalidad de obtención:** Este principio-regla está impregnado para la adquisición de las evidencias físicas, pero también es de suma importancia para la adquisición y/o incautación, extracción y acceso de las evidencias digitales, porque todo debe ser legal y controlable de la mano con el debido proceso y, sobre todo, sometido al control judicial cuando corresponda. En términos prácticos, si la primera intervención sobre el dispositivo no cuenta con autorización válida o controlable (orden fiscal o judicial, salvo supuestos de flagrancia claramente documentados), todo el sofisticado tratamiento técnico posterior queda expuesto a exclusiones probatorias por parte de los sujetos procesales; asimismo, puede ser cuestionada su convicción en juzgamiento.

B. Integridad verificable: Obligación de consignar mecanismos de verificación (códigos hash o equivalentes) para fuente y copias de trabajo, con registro de cuándo, quién y con qué herramientas se obtuvo. La pregunta clave para el litigio es sencilla: si la defensa y fiscalía no obtienen el mismo código hash al verificar el archivo, ¿sobre qué elemento decidirá el juez? Por ello, sin un mecanismo objetivo de verificación, la discusión sobre integridad se vuelve una cuestión de fe en el perito y no de contraste técnico reproducible.

C. Trazabilidad completa: Permitir accesos, transferencias, almacenamiento y análisis, identificando responsables, fecha/hora y lugar en línea con la lógica de auditabilidad. Ahora, si lo llevamos a la praxis, en el caso de que el juez no pueda reconstruir quién accedió al archivo y cuándo, la trazabilidad no tendría sentido; tampoco existiría cuando el fiscal no realiza la identificación del dispositivo pensando que es un acto de constatación descriptivo.

D. Separación del original con la copia: La regla práctica que deben seguirse es que el análisis se realice sobre copias, preservando el original, alineada con principios internacionales de no alterar la evidencia digital. Llevando a la práctica, indicamos que si el perito no puede señalar dónde se encuentra el soporte digital, bajo qué custodia y con qué código hash fue resguardado antes de iniciar el análisis, entonces la afirmación de que solo se trabajó sobre copias pierde la credibilidad demostrable.

E. Competencia técnica: La manipulación de evidencias digitales debe ser por peritos especializados y métodos aceptados por la comunidad científica. Ahora, desde la perspectiva de control judicial, no basta con que alguien de informática haya intervenido; el juez debe poder verificar que la persona y las herramientas empleadas cumplen estándares reconocidos, como por ejemplo formación, certificación y software forense validado, porque de lo contrario el informe no supera el escrutinio mínimo de confiabilidad técnica.

F. Contradicción técnica: Este principio es de suma importancia para los colegas que litigan, porque permite controlar la metodología, la trazabilidad y la reproducibilidad de los resultados, sin obligar a creer en el informe pericial. La evidencia aquí es sencilla: ¿la defensa cuenta con la información necesaria (logs, códigos hash, versión de software, parámetros de búsqueda) para intentar replicar el análisis o formular una contrapericia? Si la metodología no puede ser revisada ni discutida técnicamente, la contradicción se vacía de contenido y el informe pericial se transforma en un dictamen prácticamente inmune al debate.

III. Conclusión

1. El Código Procesal Penal debería reconocer expresamente la evidencia digital, porque el incremento de fuentes digitales de prueba requiere reglas claras de integridad, autenticidad y trazabilidad que hoy se resuelven de manera dispersa entre prácticas periciales, manuales institucionales y litigios caso por caso.

2. El reconocimiento expreso es necesario para salvaguardar el derecho a la prueba y la presunción de inocencia. Mientras no exista una norma de rango legal que exija estándares mínimos de cadena de custodia digital, la valoración de estas pruebas quedará

al arbitrio del juzgador, aumentando el riesgo de impugnaciones por manipulación de datos.

3. Otorgar un tratamiento distinto a la evidencia digital con relación a la evidencia física; para ello es de suma importancia la reforma al estatuto procesal vigente que permita regular de manera independiente, considerando todas las aristas para la obtención, tratamiento, actuación y valoración.

4. La propuesta legislativa de Ley Nº 11815/2024-CR es un avance relevante al introducir definición, cadena de custodia digital y peritaje informático forense, pero su redacción debe cuidarse para no generar exclusiones automáticas basadas en formalismos; además, debe flexibilizarse en el tratamiento de la fuente original aceptando copias espejo, autorizar el uso de inteligencia artificial para la detección de evidencias creadas por IA y obligar a que los proveedores de servicios digitales preserven datos específicos por orden del juez o fiscal por un tiempo determinado.

5. El estándar mínimo debe alinearse con la doctrina del Acuerdo Plenario Nº 06-2012/ CJ-116 y, a la vez, incorporar buenas prácticas internacionales (IOCE e ISO/IEC 27037) centradas en documentación completa, no cambios, competencia y auditabilidad.

IV. Referencias bibliográficas

Alfonso, S. (2021). La prueba electrónica en el proceso penal. [Tesis para optar el Grado de Maestro, Universidad de la Laguna]. Recuperado de: https://bit.ly/3FWWbFN

Corte Suprema de Justicia de la Republica. VIII Pleno jurisdiccional de las salas penales permanente y transitoria - 2012. Acuerdo Plenario Nº 06-2012/ CJ-116 (07 de marzo de 2012): https://img.lpderecho.pe/wp-content/uploads/2021/02/Acuerdo-Plenario-6-2012-CJ-116-LP.pdf

ISO/IEC 27037 (2012). Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27037:ed-1:v1:en

Ley N° 30096/2013, 27 de septiembre de 2013. Ley de Delitos Informáticos: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Ministerio del Interior. (2020). Manual para el recojo de la evidencia digital: https://cdn.www.gob.pe/uploads/document/file/1303962/DWP-ManualParaRecojo-EVIDENCIA.DIGITAL.pdf?v=1600289472

Ministerio de Justicia. (2025, 07 de noviembre de 2025). Consejo Nacional de Política Criminal aprueba proyecto de ley que regula la preservación, obtención y aseguramiento de la evidencia digital. [Nota de prensa]. https://www.gob.pe/institucion/minjus/noticias/1284322-consejo-nacional-de-politica-criminal-aprueba-proyecto-de-ley-que-regula-la-preservacion-obtencion-y-aseguramiento-de-la-evidencia-digital

Organización internacional de evidencia informática (1999). Principios para el manejo de

evidencia digital: https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Proyecto de Ley N 11815/2024, de junio de 2025. Evidencia digital: https://img.lpderecho.pe/wp-content/uploads/2025/07/PL-11815-2024-CR-LPDerecho.pdf

Piccirilli, M. (2019). Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos: legislación vigente, anteproyectos y Convenio de Budapest. [Trabajo final de especialización Universidad de Buenos Aires]. Recuperado de: http://repositoriouba.sisbi.uba.ar/gsdl/cgibin/library.cgi?a=d&c=adrespe&cl=CL1&d=HWA_6501

Silva, G. (2021). La obtención de la prueba digital en los delitos informáticos en el distrito fiscal de Lima Norte, 2021. Universidad César Vallejo. Recuperado de: https://hdl.handle.net/20.500.12692/96824