REVISTA INVECOM
ISSN en línea: 2739-0063

Custodia digital de la evidencia: límites y garantías de su validez en el proceso penal

Digital Evidence Preservation: Limits and Guarantees of Its Validity in Criminal Proceedings

Recibido: 13/04/2026 - **Aceptado:** 29/06/2026

Yosef Yamsem Trejo Minaya
https://orcid.org/0009-0006-5718-5212
ytrejom@unasam.edu.pe
Universidad Nacional Santiago Antúnez de Mayolo. Huaraz, Perú

Resumen

El trabajo desarrolla un estudio reflexivo y estructurado sobre la custodia digital de la evidencia, enfocándose en los márgenes legales y garantías de su validez dentro del sistema penal peruano. La finalidad es reconocer los criterios que le otorgan validez y su compatibilidad con los derechos fundamentales del imputado en el proceso penal. Se usó una metodología cualitativa con un diseño descriptivo-analítico y dogmático-jurídico, compuesta por un muestreo teórico por saturación a través del fichaje sistemático de una muestra teórica de 27 artículos científicos especializados obtenidos de bases de datos indexados: SciElo, Web of Science, Scopus, Dialnet; 04 libros especializados sobre inteligencia artificial; derechos fundamentales; razonamiento probatorio; 01 tesis doctoral; 01 guía integral de empleo de la informática forense; y, un artículo de portal jurídico especializado; el Código Procesal Penal peruano del 2004, y 05 pronunciamientos de la Corte Suprema de Justicia del Perú, cuya muestra se determinó por el principio de saturación teórica. Se usó como técnica el análisis de contenido cualitativo y la triangulación hermeneútica junto a entrevistas semiestructuradas a fiscales y abogados penalistas seleccionados por su experiencia en la materia. Los resultados demostraron que la custodia digital de la evidencia es inconsistente debido a vacíos normativos, limitaciones tecnológicas; y, falta de especialización, afectando su autenticidad, legitimidad y fiabilidad a la hora de su valoración judicial y los derechos fundamentales del imputado.

Palabras clave: Preservación digital, justicia, evidencia digital.

Abstract

This study presents a reflective and structured examination of the digital preservation of evidence, focusing on the legal framework and safeguards ensuring its validity within the Peruvian criminal justice system. The aim is to identify the criteria that confer validity on such evidence and to assess its compatibility with the fundamental rights of the accused in criminal proceedings. A qualitative methodology was used, employing a descriptive-analytical and legal-dogmatic design, consisting of theoretical saturation sampling through the systematic cataloging of a theoretical sample of 27 specialized scientific articles obtained from indexed databases: SciElo, Web of Science, Scopus, and Dialnet; 4 specialized books on artificial intelligence, fundamental rights, and evidentiary reasoning; one doctoral dissertation; one comprehensive guide to the use of computer forensics; and an article from a specialized legal website; the 2004 Peruvian Code of Criminal Procedure; and five rulings by the Supreme Court of Justice of Peru, the sample of which was determined by the principle of theoretical saturation. The research methods employed included qualitative content analysis and hermeneutic triangulation, along with semi-structured interviews with prosecutors and criminal defense attorneys selected for their expertise in the field. The results showed that the digital preservation of evidence is inconsistent due to regulatory gaps, technological limitations, and a lack of

expertise, which affects its authenticity, legitimacy, and reliability during judicial evaluation and impacts the fundamental rights of the accused.

Keywords: Digital preservation, justice, digital evidence.

Introducción

El internet, la inteligencia artificial, y las redes sociales fueron entre otros, el impulso que transformó a nuestra Sociedad, la cual se vio incrementada por la creciente información digital producto del uso de dispositivo digitales inteligentes en diversos sectores (Vaca & Dulce-Villarreal, 2024). Este contexto influyó directamente en el ámbito penal, toda vez que la información para descubrir y acreditar un hecho delictivo ya no se limita a soportes físicos tradicionales, sino a registros electrónicos tales como, las publicaciones web, redes sociales, dispositivos inteligentes y rastros de actividades en línea, lo cual, ha generado en los operadores de justicia una mirada distinta a la hora de concebir y demostrar los elementos probatorios dentro del proceso penal, toda vez que, la manera adecuada de su administración la convierte en determinante para una apropiada reconstrucción de los hechos imputados. (Paredes Chumpitazi & Ladera, 2025).

Estudios comparados coinciden en señalar que la evidencia digital constituye un medio de prueba de crucial importancia dentro del proceso penal, especialmente en aquellos delitos vinculados a entornos virtuales; sin embargo, su naturaleza y estructura la hacen pasible de ser alterada, modificada y borrada, obligando a generar procedimientos técnicos especializados que permitan evitar estas falencias, a lo cual se suma, las diversas tensiones que surgen entre este tipo de evidencia y los derechos fundamentales que la involucran, tales como el derecho a la vida privada, el secreto de las comunicaciones y la integridad de los datos personales, los cuales requieren de un tratamiento procesal especializado (Bujosa, Bustamante, & Toro, 2021); en tanto que otros, destacan la necesidad de encontrar un equilibrio entre el acceso a los registros y la protección del derecho de la privacidad; (Gamero & Pérez, 2023). Por estas razones, surge la importancia de un marco regulatorio que convenga entre la eficacia del proceso penal y el respecto de los derechos fundamentales involucrados (Pineda, 2021).

Esta situación no fue ajena en el plano internacional y regional, donde el desarrollo normativo reflejó esta preocupación. Así, en China se integró en el año 2012 un marco regulatorio que abarcó desde la recopilación y manejo hasta la presentación de la evidencia digital en juicio, incluyendo garantías procesales de validez, autenticidad e integridad de los datos electrónicos (Guo, 2023). La Organización Internacional de Evidencia Computacional señala que la recuperación de datos electrónicos demanda protocolos diferenciados, toda vez que no es lo mismo, la técnica de extracción de mensajes de correo a la obtención de trazas de auditoria alojados en bases de datos (Ochoa Arévalo, 2018).

La volatilidad es una de las características de la evidencia digital, y su naturaleza frágil la convierte en fácil de destruir, dañar o alterar (Palomo & Guillet, 2021), fácil de transmitir y duplicar, sensible al tiempo; y, altamente contaminable por nueva información (Prayudi et al., 2020). Por esta razón, se hace necesario establecer criterios técnicos operativos y cambios normativos que permitan preservar la evidencia digital y su custodia en entornos delictivos donde su destrucción y/o manipulación es evidente (Moussa, 2021).

Esta situación hizo que la UE presentara una propuesta reglamentaria sobre las órdenes europeas de entrega y conservación de pruebas electrónicas (Muñoz Rodriguez, 2020) y que España, reajuste sus pronunciamientos judiciales y doctrinales a criterios de conservación y trazabilidad de los medios probatorios electrónicos (Jamardo Lorenzo, 2024).

El Convenio de Budapest sobre Ciberdelincuencia estableció directrices para el manejo y preservación de evidencia digital; en Europa, el Reglamento General de Protección de Datos exige medidas estrictas de seguridad y autenticidad de los registros digitales. En Estados Unidos la *Federal Rules of Evidence* contiene disposiciones que prioriza la trazabilidad y la integridad de pruebas digitales. La Comisión Económica para América Latina y el Caribe afirma que el avance normativo de la cadena de

custodia es un desafío en regiones en vías de desarrollo, y las Naciones Unidas busca unificar estándares y asistencia técnica para fortalecer la custodia de evidencia digital (Quinche et al, 2025).

A nivel regional, Colombia fijó parámetros de valoración probatoria bajo criterios de integridad, autenticidad y equivalencia funcional (Imaicela Revilla & Alvarado Ajila, 2024). Ecuador adoptó nuevas estrategias frente a estas transformaciones tecnológicas (Flores, 2024) incorporando la prueba electrónica a su sistema penal bajo principios de inmediación, contradicción y publicidad (Delgado, 2021). A su vez, la doctrina y la jurisprudencia impulsaron reajustes normativos ante la aparición de nuevas modalidades de evidencia digital (Espinales, 2023).

En el Perú, el Código Procesal Penal del 2004 no regula la custodia digital de la evidencia, aplicando análogamente las reglas de la prueba documental tradicional, lo cual genera inconsistencias a la hora de su debido tratamiento y valoración judicial.

Bajo este panorama surge la cuestión principal que orienta el trabajo de investigación: ¿Cómo impactan en el proceso penal la autenticidad, trazabilidad y fiabilidad de los elementos probatorios las prácticas de custodia de la evidencia digital, tomando en cuenta los límites técnicos y vacíos normativos junto a las garantías que condicionan su validez jurídica?

Metodología

La investigación tuvo un enfoque cualitativo destinado a examinar cómo se configura la custodia digital de la evidencia en el proceso penal peruano e identificar los criterios que condicionan su validez. Este paradigma permitió examinar el fenómeno desde su dimensión normativa hasta su dimensión práctica concreta.

Se adoptó el método dogmático que hizo posible construir las bases doctrinales y las pautas que regulan su aplicación en el proceso penal peruano. Paralelamente se usó el método hermeneútico para interpretar la legislación y las decisiones de la Corte Suprema de Justica del Perú en torno a la autenticidad e integridad de la cadena de custodia digital.

El marco teórico se construyó a partir de una revisión de 27 artículos especializados indexados; 04 libros especializados sobre inteligencia artificial; derechos fundamentales; razonamiento probatorio; 01 tesis doctoral sobre la vulneración de los derechos constitucionales; 01 guía integral de empleo de la informática forense; y, un artículo de portal jurídico especializado; los cuales se ejecutaron de manera sistemática durante los meses de noviembre y diciembre del 2025 y de enero a marzo del 2026.

Se usaron ecuaciones de búsqueda mediante operadores booleanos *(AND y ORD*) tales como: (“cadena de custodia digital” OR *“digital chain of custody”)* AND (“proceso penal” OR “*criminal procedure”)* y se aplicaron estrictos criterios de exclusión de artículos jurídicos originales publicados entre los años 2015 a 2026.

A su vez, comprendió la revisión del Código Procesal Penal Peruano del 2004 (D.L. 957) relativo a los procedimientos de intervención de las comunicaciones y telecomunicaciones por estar relacionadas a la obtención de evidencias digitales, y 05 resoluciones de la Corte Suprema de Justica del Perú, excluyéndose información carente de respaldo científico.

La muestra teórica final quedó conformada, tras alcanzar el nivel de saturación teórica por 34 trabajos académicos, 03 dispositivos normativos (artículos 230°;230-A y 231° del Código Procesal Penal Peruano; y, 05 resoluciones de la Corte Suprema de Justicia del Perú, tras una búsqueda inicial de 80 documentos potenciales depurados a través de filtros de duplicidad, resúmenes de lectura y de pertinencia.

Se utilizó la técnica del fichaje digitalizado a través de una matriz de vaciado de datos estructurados en *Microsoft Excel* bajo tres categorías: i) criterios técnicos de mismidad y fiabilidad; ii) límites de afectación constitucional; y, iii) vacíos normativos, lo cual permitió sistematizar la muestra documental final.

Se aplicó la técnica de análisis de contenido cualitativo y la triangulación hermeneútica realizándose el contraste crítico respectivo con la documentación sistematizada, las exigencias técnicas forenses y la valoración racional efectuada por los órganos jurisdiccionales.

A su vez, se realizaron entrevista semiestructuradas a 06 especialistas en derecho procesal penal, la muestra estuvo conformado por cuatro fiscales penales del Ministerio Público peruano, una abogada penal del Ministerio Público y una abogada del Ministerio de Justicia del Perú, los cuales fueron seleccionados a través de un muestreo deliberado basado en su experiencia directa de la evidencia digital y su custodia.

En cuanto a los aspectos éticos, los entrevistados mostraron su consentimiento informado antes de su participación, garantizándose la confidencialidad de sus identidades y de la información proporcionada.

El carácter abierto de las preguntas formuladas estuvo dirigidas a recoger la percepción directa sobre las falencias técnicas; vacíos normativos; y, las practicas que garantizan la validez de la custodia de la evidencia digital.

La metodología usada, en su conjunto, permitió vincular el análisis jurídico con las percepciones de los operadores jurídicos en su quehacer diario generando una percepción integral y articulada del problema planteado y permitió remarcar los factores que condicionan la validez y fiabilidad de la custodia digital en el proceso penal peruano.

Resultados y discusión

Como resultado del análisis cualitativo y la triangulación hermeneútica de la muestra teórica, los dispositivos normativos (artículo 230°; 230-A y 231°) del Código Procesal Penal Peruano; y, de 05 resoluciones de la Corte Suprema de Justicia del Perú, contrastadas con las entrevistas realizadas a los 06 expertos, se obtuvieron los siguientes resultados:

Sobre los reajustes en la valoración de la custodia digital de la evidencia y los instrumentos que le otorgan validez

Bajo la concepción racionalista, la prueba penal se define como el conjunto de actividades, inferencias y medios (González Lagier, 2022) dirigidos a la averiguación de la verdad, entendida bajo el principio de correspondencia que un enunciado fáctico será verdadero si se condice con la realidad (Ferrer Beltrán, 2022). Sin embargo, el resultado de la investigación reveló que la naturaleza volátil de la prueba digital, y su fácil manipulación y/o alteración, ha generado nuevas exigencias procesales a la hora de su valoración judicial sujeta ahora, a exigencias técnicas periciales que garanticen su legitimidad e integridad.

En efecto, el resultado del análisis doctrinal demostró en principio que, la doctrina especializada es unánime en destacar la naturaleza volátil de la evidencia digital al estar sujeta a “riesgos específicos de posible alteración y/o eliminación” (Di Lorio, Ana et al, 2015), toda vez que, a diferencia de los soportes tradicionales carecen de una estructura estable, y requieren de controles técnicos y certificaciones especializadas (Ledesma Narváez, 2016) que garanticen el aseguramiento de su fuerza probatoria en el proceso penal (Di Lorio, Ana et al, 2015).

Esta postura fue recogida por la Sala Penal Permanente de la Corte Suprema de Justicia del Perú en el Recurso de Apelación N°7-2023/Corte Suprema, donde destacó su naturaleza volátil debido a la facilidad con la que puede desaparecer o alterarse, resaltando su dependencia a pericias informáticas como garantías de su autenticidad e integridad.

En segundo lugar, el resultado de la investigación demostró que la evidencia digital para ser debidamente valorada en el proceso penal, requiere de ciertos requisitos que garanticen su autenticidad, integridad y legitimidad, además de una adecuada trazabilidad a través del correcto mantenimiento de la

cadena de custodia. (González Reyes, 2021) Emergiendo como técnicas para dicho fin, la generación de valores hash, la clonación de la información y el registro pormenorizado de toda intervención en el material probatorio asegurado. (González Reyes, 2021).

A su vez, la doctrina analizada reveló que la cadena de custodia es el mecanismo que garantiza que la información contenida en los soportes digitales no ha sido modificada y/o alterada, haciendo necesaria su documentación durante todo su recorrido procesal hasta su presentación en juicio (Marchal González, 2023).

Postura que fue recogida por la Corte Suprema de Justicia del Perú a través de la Casación N°231-2011-Madre de Dios y la Apelación N°101-2022-Puno, donde señaló que la cadena de custodia es el procedimiento formal y legal que garantiza la autenticidad y mismidad de las evidencias; y, en el Acuerdo Plenario N°6-2012/CJ-116, señaló como doctrina legal que es un sistema que garantizar la integridad de la prueba material. Sin embargo, doctrina es unánime al señalar que, ante la duda sobre su autenticidad e integridad esta debe ser rechazada (Alfaro Valverde, 2024).

En el plano operativo, los resultados de las entrevistas realizadas a los cuatro fiscales penales del Ministerio Público peruano, las abogadas del Ministerio Público y del Ministerio de Justicia del Perú evidenciaron que la custodia digital es concebida como un componente imprescindible para la validez de la prueba digital, aun cuando su aplicación en la práctica continúa siendo desigual, incompleta y condicionada a la interpretación de cada operador.

Ello coincide con el análisis documental de quienes subrayan que la solidez de la prueba informática se debilita cuando no existen criterios técnicos definidos (Galindo, 2022); y otros, destacan que solo se vuelve eficaz cuando los operadores dominan los aspectos técnicos necesarios para interpretarla y valorarla adecuadamente (González Reyes, 2021).

La triangulación de estos resultados, demostró que, el respeto irrestricto de la cadena de custodia digital es indispensable para asegurar la confiabilidad de la evidencia digital, (Paredes Chumpitazi & Ladera, 2025), la cual descansará entre otros, en la forma de su conservación (Pineda, 2021). Dependiendo de metodologías rigurosas, copias forenses, algoritmos hash criptográficos; intervención documentada (Ochoa Arévalo, 2018); así, como el uso de herramientas avanzadas (Paredes Chumpitazi & Ladera, 2025), como la firma digital, valores hash y sistemas de trazabilidad que eviten su alteración y modificación durante todo el *iter* procesal (Suárez et al., 2023).

La llegada de la inteligencia artificial introdujo nuevos retos para la justicia penal, con grandes cantidades de información de difícil trazabilidad que impiden en la mayoría de los casos demostrar la participación delictiva (López, 2023), deviniendo en necesario, su construcción normativa en torno la forma de su obtención; su control, ofrecimiento y valoración, de forma tal, que permita garantizar la protección de derechos fundamentales de los investigados en escenarios delictivos automatizados (Garmendia Prieto, 2025),

Sobre las tensiones entre los derechos fundamentales y la evidencia digital dentro del proceso penal

El resultado de la investigación doctrinal demostró que la legitimidad en la obtención de la evidencia digital constituye otro requisito indispensable de su admisión y valoración judicial, toda vez que sólo podrán ser valoradas aquellas evidencias obtenidas mediante procedimientos establecidos por ley en estricto respeto a los derechos fundamentales como la intimidad o el secreto de las comunicaciones (Ortego Pérez, 2022).

La doctrina analizada coincide en señalar que los derechos fundamentales en el procesal penal se ponen en tela de juicio cuando los medios de prueba son utilizados por encima de ellos (Gonzáles Obando, 2021). Por esta razón, el uso de la evidencia digital en el proceso penal supone un examen riguroso que descarte cualquier tipo de afectación a un derecho fundamental, y ante su presencia debe producirse su exclusión (Gómez-Agudelo, 2020).

El análisis documental reveló que el derecho a la intimidad del imputado se ve seriamente afectada cuando se accede de manera inadecuada a información contenida en soportes digitales (Gómez-Agudelo, 2020). Donde una intervención no autorizada a información personal contenida en dispositivos digitales afecta de manera directa la intimidad personal y como tal, autoriza a aplicar los criterios de exclusión en resguardo al derecho a la privacidad y el derecho al debido proceso (Landa Arroyo, 2017).

El análisis normativo del Código Procesal Penal peruano del 2004, dio cuenta que los artículos 230°; 230-A; y 231° regulan los procedimientos de intervención de las comunicaciones y telecomunicaciones; sin embargo, no señalan de manera expresa el procedimiento sobre la cadena de custodia digital de la evidencia, generando vacíos procedimentales en tormo a su debido tratamiento.

Los resultados demuestran que la intervención sobre datos electrónicos con carentes parámetros estrictos puede comprometer seriamente la privacidad de las partes y vulnerar con ello el debido proceso en materia penal, donde la pérdida de control y transparencia sobre la evidencia digital puede derivar en la afectación de derechos fundamentales (Castellano, 2021), y como tal, en nulidades ante la presunta intrusión arbitraria por parte de la autoridad que la obtuvo (Bernard, 2021).

Dentro de este contexto, la investigación reveló que la introducción de la evidencia digital al proceso penal y su custodia requiere de controles reforzados por parte de los operadores jurídicos a finde garantizar la legalidad, privacidad y el debido proceso del imputado (Bernard, 2021).

Sobre la ausencia normativa de la custodia digital en la normativa procesal peruana

El resultado del análisis normativo del Código Procesal Penal peruano del 2004, reveló que la norma procesal peruana no regula un tratamiento jurídico especializado sobre la custodia digital de la evidencia, equiparándola a documentos convencionales a pesar de sus notorias diferencias técnicas (Gonzáles Obando, 2021), generando vacíos interpretativos al momento de su valoración. Tal como se comprobó al analizar los pronunciamientos de la Corte Suprema de Justicia del Perú en la Apelación N°101-2022-Puno, donde equiparó las grabaciones de audio y video contenidos en un CD como si fueran una prueba documental; y que, bajo el principio de libertad probatoria, el rompimiento de la cadena de custodia podría ser acreditada por otro medio de prueba; y, en el Recurso de Nulidad N°1714-2023-Lima Sur señaló que la ruptura de la cadena de custodia no determinaba su nulidad, inadmisibilidad o inutilización, pudiendo ser salvada con un medio de prueba alternativo; pese a que, la doctrina es unánime en señalar que, ante cualquier duda que comprometa su autenticidad e integridad esta debe ser rechazada (Alfaro Valverde, 2024).

Los entrevistados coincidieron en que la conservación adecuada de los datos electrónicos es determinante para garantizar su integridad; sin embargo, señalan la ausencia de una regulación expresa en el Código Procesal Penal Peruano sobre el debido tratamiento de la custodia de la evidencia digital, así como la falta protocolos que uniformicen criterios o prácticas estandarizadas sobre su debido manejo.

Esta ausencia normativa, conforme a las entrevistas realizadas a los expertos, genera decisiones dependientes del criterio y la experiencia del fiscal, juez o perito que, de estándares técnicos, situación que se agudiza ante la falta de especialización y la ausencia de los recursos tecnológicos en diversas jurisdicciones, lo cual genera un uso inadecuado de la custodia digital, incrementado los cuestionamientos en torno a su validez, autenticidad, y legitimidad.

Por otro lado, el resultado de la investigación reveló la necesidad constante de preparación de jueces, fiscales y abogados para una adecuada gestión de la evidencia digital y transparencia procesal en entornos digitalizados, de modo tal, que su valoración judicial resulte incuestionable y sobre todo respetuoso de los derechos fundamentales del investigado (Gómez-Agudelo, 2020).

Sobre las falencias técnicas y limitaciones tecnológicas en torno al debido manejo de la evidencia digital

Desde el plano operativo, los entrevistados señalaron falencias en torno al debido manejo de la evidencia digital, así como la falta de capacitación para el tratamiento de la evidencia digital y su aseguramiento, dando cuenta incluso de limitaciones tecnológicas en lugares de poco acceso al internet; ausencia de equipos, fiscalías y unidades policiales carentes de personal especializado o zonas rurales sin acceso a internet, volviendo en nulas cualquier tipo de práctica de aseguramiento digital. Estas vivencias concretas aportan matices que la teoría no siempre alcanza a registrar.

La investigación reveló que, mientras las dificultades operativas afectan la integridad de la cadena de custodia digital, la ausencia normativa sobre su tratamiento amplia sus efectos, evidenciando como tal, su debilidad tanto técnica como normativa al evidenciar sus dificultades materiales y su validez probatoria ante su inestabilidad jurídica.

En cuanto a su fiabilidad, un sector mayoritario de la doctrina subrayó que la evidencia digital no garantiza por sí sola la integridad de la información que la contiene y como tal, el hecho que pretende probar sin una previa verificación de carácter técnico pericial (Alfaro Valverde, 2024).

En conjunto, el panorama sugiere que la custodia digital en el Perú atraviesa una etapa de transición: existe consenso sobre su importancia, pero aún no se dispone de una construcción normativa ni de capacidades técnicas que permitan su aplicación uniforme en todos los niveles del sistema penal.

Los entrevistados resaltaron la necesidad de revisar el CPP a efectos de incorporar reglas claras y precisas sobre el tratamiento adecuado de la custodia digital de la evidencia, resaltando la necesidad de especialización, así como la creación de unidades y equipos especializados. Postura que se encuentra respaldada por la doctrina analizada, los cuales dieron cuenta que el fortalecimiento técnico y normativo ha permitido justificar criterios adecuados para admitir y valorar adecuadamente la evidencia digital.

Dentro de este contexto, el modelo procesal penal peruano se encuentra en un momento importante y crucial para ajustar su modelo probatorio a estándares técnicos adecuados en el tratamiento de la evidencia digital y su custodia, haciendo más transparente su tratamiento operacional y como tal, fortaleciendo su validez jurídica a la hora de su valoración judicial con pleno respeto a los derechos fundamentales.

La convergencia entre tecnología, reglas jurídicas procesales, y formación técnico especializada configuran estrategias adecuadas para afianzar el tratamiento de la evidencia digital dentro del proceso penal y fortalecer la legitimidad del sistema judicial, presentando un escenario de mayor transparencia, igualdad, objetividad y eficiencia en un entorno cada vez más automatizado por la era digital (Suárez et al., 2023).

Conclusiones

La evidencia digital en el proceso penal peruano ha modificado de manera significativa la estructura de la actividad probatoria dentro del proceso penal generando cuestionamientos sobre su autenticidad, integridad, trazabilidad y fiabilidad de los datos que la contienen por la naturaleza volátil que la caracteriza. Y si bien es cierto, con el uso de la evidencia digital se amplió significativamente las formas de reconstruir un hecho delictivo; también lo es, que su uso demandó la necesidad de establecer normas técnicas y jurídicas más estrictas que garanticen su validez durante todo el *iter* procesal, así como la necesidad de proteger de manera reforzada las garantías constitucionales que la involucren.

En el sistema procesal penal peruano, la ausencia de precisión normativa, la falta de formación especializada y la limitada tecnología dificulta el uso adecuado de la custodia digital. La literatura como la evidencia empírica coinciden en señalar que, pesar de la importancia de la evidencia digital dentro del sistema probatorio penal, su tratamiento aún sigue siendo inconsistente y sujeto a objeciones sobre su autenticidad, legalidad o validez, generando inestabilidad jurídica y legitimidad de las decisiones jurisdiccionales.

Ante tal escenario, deviene en necesario fortalecer el tratamiento la cadena de custodia digital, haciendo precisiones a su regulación normativa procesal, unificando protocolos técnicos y capacitando a los operadores jurídicos a efectos de establecer reglar claras y precisas sobre su tratamiento operacional y como tal, su validez jurídica, garantizando de esta forma, la legitimidad de las decisiones judiciales.

El sistema procesal penal peruano se encuentra en un momento importante y crucial para ajustar su modelo probatorio a estándares técnicos adecuados en el tratamiento de la evidencia digital y su custodia, haciendo más transparente su tratamiento operacional y como tal, el fortalecimiento de su validez jurídica a la hora de su valoración judicial con pleno respeto a los derechos fundamentales de los investigados.

Referencias

Alfaro Valverde, L. (2024). Prueba informática: el problema de su fiabilidad. *IUS ET VERITAS*, (68), 66–79. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/29552

Bernard, J. (2021). Equilibrio entre el derecho a la intimidad y el poder investigativo del Estado en la era digital*. Revista Jurídica de la Universidad de Palermo, (2), 33-62.* https://revistas-colaboracion.juridicas.unam.mx/index.php/rjup/article/view/41998

Bujosa, L., Bustamante, M y Toro, L (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal,* 7(2), 1347. https://doi.org/10.22197/rbdpp.v7i2.482

Castellano, P. S. (2021). Inteligencia Artificial y valoración de la prueba: las garantías Jurídico-Constitucionales del órgano de control. *THEMIS Revista De Derecho, (79),* 283–297. https://doi.org/10.18800/themis.202101.015

Corte Suprema de Justicia del Perú. (2023) Apelación N°101-2022-Puno. (Sala Penal Permanente). *Poder Judicial del Perú.* https://lpderecho.pe/cd-prueba-documental-consecuencias-rompimiento-cadena-custodia-apelacion-101-2022-puno/

Corte Suprema de Justicia del Perú. (2012). Casación N.°231-2011-Madre de Dios (Sala Penal Permanente). *Poder Judicial del Perú.* https://lpderecho.pe/concepto-cadena-custodia-casacion-231-2011-madre-de-dios/

Corte Suprema de Justicia del Perú. (2024). Apelación N°7-2023/Corte Suprema (Sala Penal Permanente). *Plataforma Digital Única del Estado Peruano.* https://www.gob.pe/institucion/pj/normas-legales/5007406-7-2023

Corte Suprema de Justicia del Perú. (2024) Recurso de Nulidad N°1714-2023-Lima Sur. (Sala Penal Transitoria). *Poder Judicial del Perú.* https://lpderecho.pe/reafirman-ruptura-cadena-custodia-acto-irregular-defectuoso-determina-nulidad-inadmisibilidad-inutilizacion-recurso-nulidad-1714-2023-lima-sur/

Corte Suprema de Justicia del Perú. (2013). Acuerdo Plenario N°6-2012/CJ-116. VIII Pleno Jurisdiccional de las Salas Penales Permanentes y Transitorias-2012. *Poder Judicial del Perú.* https://www.pj.gob.pe/wps/wcm/connect/cij-juris/s_cij_jurisprudencia_nuevo/as_jurisprudencia_sistematizada/as_acuerdos_plenarios/as_AcuerdosPlenariosenMateriaPenal/as_AcuerdosPlenarios2012/

Congreso de la República del Perú. (2004) Decreto Legislativo N°957: Código Procesal Penal (22 de julio del 2004*). Sistema Peruano de información jurídica (SPIJ*). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H682695

Di Lorio, Ana H., Constanzo Bruno, Waimann Julián, Podestá Ariel, Greco Fernando, Cistoldi Pablo, Lamperti Sabrina, Núñez Luciano, y Giaccaglia María F. (2015). Guía integral de empleo de la informática forense en el proceso penal. 2° edición revisada. *Universidad FASTA*. https://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf

Delgado, J. (2021). Reflexiones sobre el estado actual de la transformación digital de la justicia. *Revista Acta Judicial, 8*, 27-42. https://dialnet.unirioja.es/descarga/articulo/8486157.pdf

Espinales, J. (2023). Análisis del derecho procesal y los entornos jurídicos. *Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa, REICOMUNICAR, 6*(12), 89-97. https://reicomunicar.org/index.php/reicomunicar/article/view/263

Ferrer Beltrán, J. (2022). Los momentos de la actividad probatoria en el proceso. *Manual de razonamiento probatorio*; 49. *Suprema Corte de Justicia de la Nación*. https://www.scjn.gob.mx/derechos-humanos/sites/default/files/Publicaciones/archivos/2024-02/Manual%20de%20razonamiento%20probatorio_0.pdf

Flores, M. (2024). La vulneración de los derechos constitucionales por falla técnica de los jueces en Ecuador. En el juicio de admisibilidad de prueba. *Universidad de Salamanca.* https://gredos.usal.es/handle/10366/159236

Galindo, GM (2022). Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista electrónica de ciencia penal y criminología, 24 (*23), 1-38. http://criminet.ugr.es/recpc/24/recpc24-23.pdf

Gamero, E y Pérez, F (2023). Inteligencia artificial y sector público: Retos, límites y medios. *Tirant lo Blanch.* https://www.cvca.es/wp-content/uploads/2023/11/Libro-completo_Inteligencia-Artificial-y-Sector-Publico.pdf

Garmendia Prieto, A. (2025). La irrupción de la inteligencia artificial en el proceso civil: retos y oportunidades. *Revista de Privacidad Y Derecho Digital*, *9*(33), 122–160. https://revista.proeditio.com/rpdd/article/view/7948

Gómez-Agudelo, D. S. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. *Ratio Juris (UNAULA)*, *15*(30), 220–240. https://doi.org/10.24142/raju.v15n30a11

Gonzáles Obando, G. L. (2021). Garantías procesales penales en la evidencia digital. *Revista de Investigación de la Academia de la Magistratura, 3*(5), 165-174. https://doi.org/10.58581/rev.amag.2021.v3n5.09

González Lagier, D. (2022). Prueba, hechos y verdad. En J. Ferrer Beltrán, *Manual de Razonamiento Probatorio*; 1- 44. *Suprema Corte de Justicia de la Nación.* https://www.scjn.gob.mx/derechos-humanos/sites/default/files/Publicaciones/archivos/2024-02/Manual%20de%20razonamiento%20probatorio_0.pdf

González Reyes, J. M. (2021). La prueba pericial digital y la cadena de custodia. *Anales de la Facultad de Derecho, (38),* 43-79. https://doi.org/10.25145/j.anfade.2021.38.03

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review, 48,* 105774. https://www.sciencedirect.com/science/article/abs/pii/S0267364922001170?via%3Dihub

Imaicela Revilla, J. A., & Alvarado Ajila, L. A. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano. *Revista Lex*, *7*(27), 1338–1350. https://doi.org/10.33996/revistalex.v7i27.247

Jamardo Lorenzo, A. (2024). La configuración de la cadena de custodia tecnológica en el ordenamiento jurídico español. *IUS ET SCIENTIA*, *10*(2), 101–122. https://doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Landa Arroyo, C. (2017). Los derechos fundamentales. *Fondo Editorial PUCP.* https://doi.org/10.18800/9786123172312

Ledesma Narváez, M. (2016). La prueba documental electrónica. *Foro Jurídico* (15), 17–25. https://repositorio.pucp.edu.pe/items/9fd03d78-c074-48d5-bae5-faf1beb7c63e

López, Z. A. (2023). Validez jurídica de la prueba digital en Guatemala. *Revista Ciencia Multidisciplinaria CUNORI, 7*(2), 203-214. https://doi.org/10.36314/cunori.v7i2.238

Marchal González, A. N. (2023). La cadena de custodia y su impacto en el proceso judicial. *Revista Vía Iuris*, *35*, 113-130. https://doi.org/10.37511/viaiuris.n35a6

Moussa, A. (2021). La evidencia electrónica y su autenticidad en la evidencia forense. *Egyptian Journal Forensic Sciences*, *11*(20). https://doi.org/10.1186/s41935-021-00234-6

Muñoz Rodríguez, A (2020). El impacto de la inteligencia artificial en el proceso penal. *Anuario de la Facultad de Derecho Universidad de Extremadura*, *36,* 695-728. https://doi.org/10.17398/2695-7728.36.695

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía Y Política*, *2*(28), 35–44. https://doi.org/10.25097/rep.n28.2018.03

Ortego Pérez, F. (2022). Investigación y prueba digital de los ciberdelitos. *Justicia, (2),* 89-132. https://vlex.es/vid/investigacion-prueba-digital-ciberdelitos-924077816

Palomo, L. E., & Guillet, S. M. (2021). Evidencia digital de la nube. El aporte probatorio en Santiago del Estero. *Difusiones*, *21*(2), 59–75. https://ediciones.ucse.edu.ar/index.php/difusiones/article/view/394

Paredes Chumpitazi, A., & Ladera, Y. (2025). El uso de las pruebas digitales en los procesos penales: Límites y garantías. *Lex Certa.* https://lexcerta.pe/el-uso-de-las-pruebas-digitales-en-los-procesos-penales-limites-y-garantias/

Pineda, J. E. (2021). Garantías procesales en la aplicación de la inteligencia artificial y el Big Data en el estándar de la prueba penal. *Revista CES Derecho*, *12*(1), 108–125. https://doi.org/10.21615/cesder.12.1.6

Prayudi, Y., Ashari, A. y Priyambodo, TK (2020). Marco para el manejo de evidencia digital: Estudio de caso sobre los procedimientos de gestión de evidencia en Indonesia. *Journal of Cases on Information Technology (JCIT), 22(*3), 51-71. https://doi.org/10.4018/JCIT.2020070104

Quinche-Alvarez, F.G; Endara-Almeida, L. M. y Herrera-Herrera, G. C. (2025). La cadena de custodia en la producción de la prueba digital. *Journal Scientific MQRInvestigar*, *9*(3), 1-21. https://doi.org/10.56048/MQR20225.9.3.2025.e1004

Suárez Manrique, W. Y., De León Vargas, G. I., & Monsalve Pinto, J. J. (2023). Un análisis sobre la aplicabilidad de la inteligencia artificial en el derecho colombiano. *Prolegómenos*, *26*(52), 11–23. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-182X2023000200011

Vaca P. A. y Dulce-Villarreal E.R. (2024). Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático. *TecnoLógicas*, *27*(60), e3049. https://doi.org/10.22430/22565337.3049