REVISTA INVECOM
ISSN en línea: 2739-0063

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

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

Received: 13/04/2026 - **Accepted:** 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, Peru

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.

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, & 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.

Introduction

The internet, artificial intelligence, and social media were, among other forces, the catalysts that transformed our society, a shift amplified further by the surge of digital information generated through the use of smart digital devices across a wide range of sectors (Vaca & Dulce-Villarreal, 2024). This context has had a direct bearing on the criminal justice sphere, since the information needed to uncover and establish a criminal act is no longer confined to traditional physical media but now extends to electronic records such as web postings, social media content, smart devices, and traces of online activity. This has led justice system operators to take a different view of how evidentiary elements are conceived and demonstrated within criminal proceedings, since proper handling of that information has become decisive for an accurate reconstruction of the facts under investigation (Paredes Chumpitazi & Ladera, 2025).

Comparative studies agree that digital evidence constitutes crucial evidentiary material in criminal proceedings, particularly in offenses linked to virtual environments; however, its nature and structure leave it prone to alteration, modification, and deletion, making it necessary to develop specialized technical procedures to prevent these shortcomings. Added to this are the various tensions that arise between this type of evidence and the fundamental rights it touches upon, such as the right to privacy, the secrecy of communications, and the integrity of personal data, all of which call for specialized procedural treatment (Bujosa, Bustamante, & Toro, 2021); while other authors stress the need to strike a balance between access to records and protection of the right to privacy; (Gamero & Pérez, 2023). For these reasons, the importance emerges of a regulatory framework capable of reconciling the effectiveness of criminal proceedings with respect for the fundamental rights involved (Pineda, 2021).

This situation was no less present at the international and regional level, where regulatory developments have mirrored this concern. In China, for example, a regulatory framework was put in place in 2012 covering everything from the collection and handling of digital evidence to its presentation at trial, including procedural guarantees of the validity, authenticity, and integrity of electronic data (Guo, 2023). The International Organization on Computer Evidence notes that the recovery of electronic data calls for differentiated protocols, since the technique for extracting email messages is not the same as that used to obtain audit trails stored in databases (Ochoa Arévalo, 2018).

Volatility is one of the defining features of digital evidence, and its fragile nature makes it easy to destroy, damage, or alter (Palomo & Guillet, 2021), easy to transmit and duplicate, time-sensitive, and highly susceptible to contamination by new information (Prayudi et al., 2020). For this reason, it becomes necessary to establish operational technical criteria and regulatory changes that make it possible to preserve digital evidence and its custody in criminal settings where its destruction and/or manipulation is readily apparent (Moussa, 2021).

This state of affairs prompted the EU to put forward a regulatory proposal on European production and preservation orders for electronic evidence (Muñoz Rodriguez, 2020) and led Spain to realign its judicial and doctrinal pronouncements with criteria of preservation and traceability for electronic evidentiary material (Jamardo Lorenzo, 2024).

The Budapest Convention on Cybercrime set out guidelines for the handling and preservation of digital evidence; in Europe, the General Data Protection Regulation imposes strict security and authenticity requirements on digital records. In the United States, the *Federal Rules of Evidence* contain provisions that prioritize the traceability and integrity of digital evidence. The Economic Commission for Latin America and the Caribbean notes that regulatory progress on the chain of custody remains a challenge in developing

regions, and that the United Nations is working to unify standards and technical assistance in order to strengthen the custody of digital evidence (Quinche et al, 2025).

At the regional level, Colombia established evidentiary standards based on criteria of integrity, authenticity, and functional equivalence (Imaicela Revilla & Alvarado Ajila, 2024). Ecuador adopted new strategies in response to these technological transformations (Flores, 2024) by incorporating electronic evidence into its criminal justice system under the principles of immediacy, adversarial process, and publicity (Delgado, 2021). In turn, doctrine and case law have driven regulatory adjustments in response to the emergence of new forms of digital evidence (Espinales, 2023).

In Peru, the 2004 Code of Criminal Procedure does not regulate the digital custody of evidence, applying by analogy the rules governing traditional documentary evidence, which generates inconsistencies in its proper treatment and judicial evaluation.

Against this backdrop, the central question guiding this study emerges: how do digital evidence custody practices affect the authenticity, traceability, and reliability of evidentiary elements within criminal proceedings, taking into account the technical limitations and regulatory gaps together with the guarantees that condition their legal validity?

Methodology

This study adopted a qualitative approach aimed at examining how the digital custody of evidence is structured within Peruvian criminal proceedings and at identifying the criteria that condition its validity. This paradigm made it possible to examine the phenomenon from its regulatory dimension through to its concrete practical dimension.

The dogmatic method was adopted, making it possible to build the doctrinal foundations and guidelines governing its application in Peruvian criminal proceedings. In parallel, the hermeneutic method was used to interpret the legislation and the rulings of the Supreme Court of Justice of Peru regarding the authenticity and integrity of the digital chain of custody.

The theoretical framework was built from a review of 27 specialized indexed articles; 4 specialized books on artificial intelligence, fundamental rights, and evidentiary reasoning; one doctoral dissertation on the violation of constitutional rights; one comprehensive guide to the use of computer forensics; and one article from a specialized legal portal, all of which were reviewed systematically during November and December 2025 and from January to March 2026.

Search strings were constructed using Boolean operators *(AND and OR*) such as: ("cadena de custodia digital" OR *"digital chain of custody")* AND ("proceso penal" OR "*criminal procedure")*, and strict exclusion criteria were applied to original legal articles published between 2015 and 2026.

In turn, the review encompassed the 2004 Peruvian Code of Criminal Procedure (Legislative Decree No. 957) with respect to the procedures governing the interception of communications and telecommunications, given their relevance to obtaining digital evidence, along with five rulings by the Supreme Court of Justice of Peru; information lacking scientific support was excluded.

The final theoretical sample, once the level of theoretical saturation had been reached, comprised 34 academic works, three regulatory provisions (Articles 230, 230-A, and 231 of the Peruvian Code of Criminal Procedure), and five rulings by the Supreme Court of Justice of Peru, drawn from an initial search of 80 potential documents that were refined through filters for duplication, abstract review, and relevance.

The digitized cataloging technique was used, drawing on a structured data-extraction matrix built in *Microsoft Excel* under three categories: (i) technical criteria of sameness and reliability; (ii) limits of constitutional impact; and (iii) regulatory gaps, which made it possible to systematize the final documentary sample.

Qualitative content analysis and hermeneutic triangulation were applied, carrying out the corresponding critical comparison between the systematized documentation, forensic technical requirements, and the rational evaluation performed by the courts.

In turn, semi-structured interviews were conducted with six specialists in criminal procedural law; the sample consisted of four criminal prosecutors from the Peruvian Public Prosecutor's Office, one criminal defense attorney from the Public Prosecutor's Office, and one attorney from the Peruvian Ministry of Justice, all selected through purposive sampling based on their direct experience with digital evidence and its custody.

Regarding ethical considerations, the interviewees gave their informed consent prior to participating, and the confidentiality of their identities and the information provided was guaranteed.

The open-ended nature of the questions was designed to gather direct perceptions of technical shortcomings, regulatory gaps, and the practices that ensure the validity of digital evidence custody.

Taken together, the methodology used made it possible to link legal analysis with the perceptions of legal practitioners in their day-to-day work, generating a comprehensive and articulated understanding of the problem posed, and made it possible to highlight the factors that condition the validity and reliability of digital custody in Peruvian criminal proceedings.

Results and Discussion

As a result of the qualitative analysis and hermeneutic triangulation of the theoretical sample, the regulatory provisions (Articles 230, 230-A, and 231) of the Peruvian Code of Criminal Procedure, and five rulings by the Supreme Court of Justice of Peru, contrasted against the interviews conducted with the six experts, the following results were obtained:

On adjustments in the evaluation of the digital custody of evidence and the instruments that confer its validity

Under the rationalist conception, criminal evidence is defined as the set of activities, inferences, and means (González Lagier, 2022) directed toward ascertaining the truth, understood under the correspondence principle whereby a factual statement will be true if it corresponds to reality (Ferrer Beltrán, 2022). The findings of this study revealed, however, that the volatile nature of digital evidence, together with the ease with which it can be manipulated and/or altered, has given rise to new procedural requirements at the time of its judicial evaluation, which is now subject to technical expert requirements that guarantee its legitimacy and integrity.

Indeed, the doctrinal analysis showed, as a preliminary matter, that specialized scholarship is unanimous in stressing the volatile nature of digital evidence, given that it is subject to “specific risks of possible alteration and/or deletion” (Di Lorio, Ana et al, 2015), since, unlike traditional media, it lacks a stable structure and requires specialized technical controls and certifications (Ledesma Narváez, 2016) to guarantee that its evidentiary weight is preserved throughout the criminal proceeding (Di Lorio, Ana et al, 2015).

This position was echoed by the Permanent Criminal Chamber of the Supreme Court of Justice of Peru in Appeal No. 7-2023/Corte Suprema, which highlighted its volatile nature given the ease with which it can disappear or be altered, emphasizing its dependence on computer forensic examinations as guarantees of its authenticity and integrity.

Second, the findings of this study showed that digital evidence, in order to be properly evaluated in criminal proceedings, must meet certain requirements that guarantee its authenticity, integrity, and legitimacy, in addition to adequate traceability through the proper maintenance of the chain of custody. (González Reyes, 2021)The generation of hash values, the cloning of information, and the detailed logging

of every intervention on the secured evidentiary material have emerged as techniques for this purpose. (González Reyes, 2021).

In turn, the doctrine reviewed revealed that the chain of custody is the mechanism that guarantees that the information contained in digital media has not been modified and/or altered, making it necessary to document it throughout its entire procedural course up to its presentation at trial (Marchal González, 2023).

This position was echoed by the Supreme Court of Justice of Peru through Cassation No. 231-2011-Madre de Dios and Appeal No. 101-2022-Puno, which held that the chain of custody is the formal, legal procedure that guarantees the authenticity and sameness of evidence; and, in Plenary Agreement No. 6-2012/CJ-116, it held as binding legal doctrine that it is a system that guarantees the integrity of physical evidence. Scholarship is nevertheless unanimous in holding that, where doubt exists as to its authenticity and integrity, the evidence must be rejected (Alfaro Valverde, 2024).

At the operational level, the results of the interviews conducted with the four criminal prosecutors from the Peruvian Public Prosecutor's Office and the attorneys from the Public Prosecutor's Office and the Ministry of Justice of Peru showed that digital custody is regarded as an essential component of the validity of digital evidence, even though its application in practice remains uneven, incomplete, and dependent on each practitioner's own interpretation.

This is consistent with the documentary analysis of those who emphasize that the strength of computer-based evidence is weakened when no defined technical criteria exist (Galindo, 2022); while others note that it only becomes effective when practitioners have mastered the technical aspects necessary to interpret and evaluate it properly (González Reyes, 2021).

The triangulation of these findings showed that strict adherence to the digital chain of custody is essential to ensure the reliability of digital evidence, (Paredes Chumpitazi & Ladera, 2025), which rests, among other things, on how it is preserved (Pineda, 2021). This depends on rigorous methodologies, forensic copies, cryptographic hash algorithms, and documented intervention (Ochoa Arévalo, 2018); as well as on the use of advanced tools (Paredes Chumpitazi & Ladera, 2025), such as digital signatures, hash values, and traceability systems that prevent its alteration or modification throughout the entire *iter* of the proceedings (Suárez et al., 2023).

The advent of artificial intelligence has introduced new challenges for criminal justice, given the large volumes of information that are difficult to trace and that, in most cases, make it impossible to demonstrate criminal participation (López, 2023), making it necessary to build a regulatory framework around how such evidence is obtained, controlled, offered, and evaluated, in a manner that safeguards the fundamental rights of persons under investigation in automated criminal scenarios (Garmendia Prieto, 2025),

On the tensions between fundamental rights and digital evidence within criminal proceedings

The findings of the doctrinal analysis showed that the lawfulness of how digital evidence is obtained constitutes another indispensable requirement for its admission and judicial evaluation, since only evidence obtained through procedures established by law, in strict observance of fundamental rights such as privacy or the secrecy of communications, may be evaluated (Ortego Pérez, 2022).

The doctrine reviewed agrees that fundamental rights in criminal proceedings are called into question whenever evidentiary means are used at their expense (Gonzáles Obando, 2021). For this reason, the use of digital evidence in criminal proceedings requires rigorous scrutiny to rule out any impairment of a fundamental right, and where such impairment is present, the evidence must be excluded (Gómez-Agudelo, 2020).

The documentary analysis revealed that the right to privacy of the accused is seriously affected when information contained on digital media is accessed improperly (Gómez-Agudelo, 2020). Unauthorized access to personal information contained in digital devices directly affects personal privacy and, as such,

warrants applying exclusionary criteria to safeguard the right to privacy and the right to due process (Landa Arroyo, 2017).

The regulatory analysis of the 2004 Peruvian Code of Criminal Procedure showed that Articles 230, 230-A, and 231 govern the procedures for intercepting communications and telecommunications; they do not, however, expressly address the procedure for the digital chain of custody of evidence, giving rise to procedural gaps regarding its proper treatment.

The findings show that intervention on electronic data without strict parameters can seriously compromise the privacy of the parties and, in doing so, undermine due process in criminal matters, given that the loss of control and transparency over digital evidence can result in the impairment of fundamental rights (Castellano, 2021), and, as such, in nullities arising from a presumed arbitrary intrusion on the part of the authority that obtained it (Bernard, 2021).

Within this context, the study revealed that introducing digital evidence into criminal proceedings, together with its custody, requires reinforced controls on the part of legal practitioners in order to guarantee the lawfulness, privacy, and due process rights of the accused (Bernard, 2021).

On the regulatory absence of digital custody within Peruvian procedural law

The regulatory analysis of the 2004 Peruvian Code of Criminal Procedure revealed that Peruvian procedural law does not regulate specialized legal treatment for the digital custody of evidence, instead equating it with conventional documents despite their evident technical differences (Gonzáles Obando, 2021), which gives rise to interpretive gaps at the time of its evaluation. This was confirmed upon reviewing the rulings of the Supreme Court of Justice of Peru in Appeal No. 101-2022-Puno, which treated audio and video recordings contained on a CD as though they were documentary evidence, holding that, under the principle of evidentiary freedom, a break in the chain of custody could be established through another item of evidence; and in Nullity Appeal No. 1714-2023-Lima Sur, which held that a break in the chain of custody did not in itself determine its nullity, inadmissibility, or unusability, and could be remedied through an alternative item of evidence; this notwithstanding that scholarship is unanimous in holding that, wherever doubt exists that compromises its authenticity and integrity, the evidence must be rejected (Alfaro Valverde, 2024).

The interviewees agreed that the proper preservation of electronic data is decisive for guaranteeing its integrity; however, they pointed to the absence of an express regulation in the Peruvian Code of Criminal Procedure governing the proper treatment of digital evidence custody, as well as the lack of protocols capable of standardizing criteria or practices for its proper handling.

This regulatory absence, according to the expert interviews, results in decisions that depend on the individual judgment and experience of the prosecutor, judge, or expert witness rather than on technical standards, a situation that is compounded by the lack of specialization and the absence of technological resources across different jurisdictions, which leads to the inadequate use of digital custody, heightening questions surrounding its validity, authenticity, and legitimacy.

On the other hand, the findings of this study revealed the ongoing need to train judges, prosecutors, and defense attorneys in the proper management of digital evidence and in procedural transparency within digitalized environments, so that judicial evaluation of such evidence is beyond question and, above all, respectful of the fundamental rights of the person under investigation (Gómez-Agudelo, 2020).

On technical shortcomings and technological limitations surrounding the proper handling of digital evidence

From an operational standpoint, interviewees pointed to shortcomings in the proper handling of digital evidence, as well as a lack of training for handling and securing it, and even noted technological limitations in areas with limited internet access; a lack of equipment, and prosecutors' offices and police units without specialized personnel, or rural areas without internet access, which renders any form of digital-

securing practice essentially void. These concrete experiences bring out nuances that theory does not always manage to capture.

The study revealed that, while operational shortcomings affect the integrity of the digital chain of custody, the regulatory absence surrounding its treatment amplifies these effects, exposing weaknesses that are both technical and normative by revealing the material difficulties involved and the evidentiary validity of such evidence in the face of its legal instability.

As for its reliability, a majority of the scholarship reviewed underscored that digital evidence does not, on its own, guarantee the integrity of the information it contains or, by extension, the fact it is meant to prove, absent prior technical expert verification (Alfaro Valverde, 2024).

Taken together, this panorama suggests that digital custody in Peru is going through a transitional stage: there is consensus on its importance, yet the country still lacks both the regulatory framework and the technical capacity needed for its uniform application across all levels of the criminal justice system.

The interviewees highlighted the need to revise the Code of Criminal Procedure so as to incorporate clear, precise rules on the proper treatment of digital evidence custody, stressing the need for specialization as well as the creation of specialized units and teams. This position is supported by the scholarship reviewed, which found that technical and regulatory strengthening has made it possible to justify appropriate criteria for admitting and properly evaluating digital evidence.

Within this context, the Peruvian criminal justice system is at an important and pivotal moment for adjusting its evidentiary model to technical standards appropriate for the treatment of digital evidence and its custody, making its operational handling more transparent and, in doing so, strengthening its legal validity at the time of judicial evaluation, in full respect of fundamental rights.

The convergence of technology, procedural legal rules, and specialized technical training constitutes an appropriate strategy for reinforcing the treatment of digital evidence within criminal proceedings and strengthening the legitimacy of the judicial system, giving rise to a scenario of greater transparency, equality, objectivity, and efficiency in an environment that is increasingly automated by the digital era (Suárez et al., 2023).

Conclusions

Digital evidence in Peruvian criminal proceedings has significantly altered the structure of evidentiary activity within criminal proceedings, giving rise to questions regarding the authenticity, integrity, traceability, and reliability of the data it contains, owing to the volatile nature that characterizes it. And while it is true that the use of digital evidence has considerably broadened the means available for reconstructing a criminal act, it is equally true that its use has demanded stricter technical and legal standards capable of guaranteeing its validity throughout the entire *iter* of the proceedings, as well as the need to provide reinforced protection for the constitutional guarantees it engages.

In the Peruvian criminal justice system, the absence of regulatory precision, the lack of specialized training, and limited technology hinder the proper use of digital custody. Both the literature and the empirical evidence agree that, despite the importance of digital evidence within the criminal evidentiary system, its treatment remains inconsistent and subject to objections regarding its authenticity, lawfulness, or validity, generating legal instability and undermining the legitimacy of judicial decisions.

Given this scenario, it becomes necessary to strengthen the treatment of the digital chain of custody by refining its procedural regulation, unifying technical protocols, and training legal practitioners so as to establish clear, precise rules governing its operational treatment and, by extension, its legal validity, thereby guaranteeing the legitimacy of judicial decisions.

The Peruvian criminal justice system is at an important and pivotal moment for adjusting its evidentiary model to technical standards appropriate for the treatment of digital evidence and its custody,

making its operational handling more transparent and, in doing so, strengthening its legal validity at the time of judicial evaluation, in full respect of the fundamental rights of persons under investigation.

References

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, & 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., & 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., & 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., & 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., & 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