Evaluation of Digital Evidence in Cybercrimes in The Single-Judge Courts of Tarapoto: Criteria, Legal Treatment And Limitations

Heidy Valentina Bardales Neyra[1] , Ruben Santisteban Seclen[2]

[1] Faculty of Law and Political Science, César Vallejo University, Tarapoto, Peru,
[2] Doctor of Law, professor and researcher at César Vallejo University, Tarapoto branch, San Martín-Peru,
Corresponding author: Heidy Valentina Bardales Neyra, orcid.org/0000-0002-3650-6615 y correo electrónico: E-mail:hbardalesn@ucvvirtual.edu.pe

SUMMARY:
Background: The Peruvian Code of Criminal Procedure does not specifically regulate digital evidence, which in practice is valued as documentary evidence. Therefore, this study analyzed how the Single-Judge Courts of Tarapoto assessed it in cybercrimes between 2022 and 2025; Methods: A qualitative grounded theory study was conducted with thirteen interviews with legal professionals and five case files; Results: Interviewees requested authenticity, integrity, and legality, while three cases ended in acquittal because there was no forensic analysis or records linking the accused to the operation; Conclusions: An authentic file alone does not prove authorship, so its value depends on independent corroboration and a judgment that explains what each piece of evidence proves.

Keywords: digital evidence, cybercrime, sound judgment, chain of custody, criminal procedure.

1. Introduction

The study was linked to SDG 16, which seeks effective institutions and fair resolution mechanisms, as the research focused on examining how jurisdictional bodies are incorporating, interpreting, and weighing digital evidence within criminal proceedings, in such a way that it was related to the need for reasoned, technically supported decisions that are compatible with due process and legal certainty in the face of crime in digital scenarios.

In the international arena, Morante et al. [1], in their postulate, argued that the probative value within Ecuador depends on the technical requirements of authenticity, integrity preservation, and reliability, while, along the same lines, in his postulate, Aguilar [2], warned that the lack of uniform normative criteria within countries such as Peru, Colombia, the United States, Argentina, and China, generates risks of contradictory resolutions and violations of due process.

From a Peruvian perspective, in the postulate of Gonzáles [3], he explained that the lack of specific treatment within the Criminal Procedure Code (CPP) creates gaps, since digital evidence is considered only as documentary evidence. In the same vein, the work of Julca et al. [4] indicated that judges are evaluating it according to the provisions of articles 157, 158 and 185 of the CPP, without recognizing its conceptual autonomy. Thus, although the doctrine developed certain criteria such as authenticity, integrity, legitimacy and immutability, these are not applied uniformly.

From the same perspective, Silva's research [5] determined that the absence of homogeneous guidelines, specialized training and technological tools limited the effectiveness of the investigations, since the need to examine this problem within the Single-Judge Courts of Tarapoto was evident.

1.1 Background

Avemañay et al. [6], in their research, found a gap in Ecuador between legal recognition and practical application, manifested in the absence of technical protocols, deficiencies in the chain of custody, and insufficient forensic infrastructure. Along the same lines, Morante et al. [1] concurred in finding a shortage of certified experts, while Sandoval [7], Acosta [8], and López [9] concluded that digital evidence is admissible according to the principles of sound judgment when its authenticity, integrity, and provenance are established. From the same perspective, Bujosa et al. [10], in their postulate added that its effectiveness depends on legality, judicial control and technical criteria.

Within the national context, the postulates of Julca et al. [4] and Valverde [11] found that these judges value digital evidence as a documentary, with sound criticism, legality, authenticity and integrity, for which reason these authors proposed recognizing its autonomy through specific regulation, while on the other hand in their postulate Ludeña et al. [12], demanded strict protocols on preservation and regarding the chain of custody, from another perspective Ventura and Robles [13], in their work warned about the risks of bias in the use of artificial intelligence to assess the evidence, and the postulates of Aguilar [2] and Gonzáles [3], recommended expert control and better training of legal actors.

1.2 Theoretical framework

The study was based on Alexy's theory of fundamental rights [14], according to which these rights are principles that are resolved by balancing based on proportionality, on Rawls' theory of justice [15], [16], which requires a proportional and respectful prosecution of liberty and equality, on Ferrajoli's guarantees [17], which proposes a minimal criminal law with legality, contradiction, presumption of innocence and burden of proof, and on Devis Echandía's general theory of judicial proof [18], [19], for whom rational conviction is obtained according to logic, technical knowledge and experience.

The assessment of digital evidence is the process by which the jurisdictional body analyzes the validity, credibility and probative force of electronic information, so that it acquires effectiveness when it proves truthfulness, integrity, reliability and adequate chain of custody [20], [21], and includes the types of digital evidence, the chain of custody and admissibility, authenticity and reliability [22]–[27].

Computer crimes encompass unlawful conduct committed by means of, or directed against, computers, networks or digital systems [28], and include legal argumentation, which requires equality of arms, contradiction and evidentiary legality [23], [29], limitations and deficiencies, such as the lack of standardized practices and training [30], and evidentiary performance, which requires verifying the origin of the evidence and ensuring its examination by the defense [23].

1.3 Research gap and objectives

The study is justified by its social relevance, since a poor assessment of digital evidence can affect due process, effective judicial protection and the credibility of the justice system, by its practical utility, since it identifies the obstacles faced by judges, and by its theoretical contribution, since it shows that digital evidence is not understood only from the perspective of documentary evidence.

Since the reviewed literature does not report how the Single-Judge Courts of Tarapoto assess digital evidence, the general objective was to analyze the assessment criteria in computer crimes between 2022 and 2025, while the specific objectives were to analyze the legal treatment of digital evidence, examine the evidentiary assessment criteria of the judges and evaluate the limitations and deficiencies of said assessment.

2. Methodology

The study was of a basic type, with a qualitative approach and a grounded theory design, which builds interpretations inductively [31], [32], with the categories of digital evidence assessment (types of evidence, chain of custody, admissibility, authenticity and reliability) and computer crimes (legal argumentation, limitations and deficiencies, and evidentiary performance).

The unit of analysis comprised thirteen legal operators in the criminal field (E1 to E13), including judges, court clerks, prosecutors and litigating lawyers with at least five years of experience, and five files from the single-judge courts of Tarapoto (EXP1 to EXP5), while those who did not prove involvement in cases with technological evidence were excluded.

Interviews and documentary analysis were used with guides validated by three experts, lawyers with a master's degree in Criminal and Criminal Procedural Law, and the data were analyzed by hermeneutic and analytical triangulation [33], so that the sources were compared and the convergences and divergences were organized in comparative tables, with informed consent, voluntary participation and confidentiality of the identity of participants, files and parties.

3. Results

The results are presented according to the order of the objectives and combine the interviews with the analysis of the files, so that Table 1 summarizes the main convergences and divergences found in the interviews.

Table 1 Convergences and divergences in the interviews (E1 to E13) according to the objectives

Thematic axis	Convergence	Divergence
Assessment criteria (general objective)	Justified assessment; authenticity and integrity (E1, E2, E3, E5, E6, E7, E9 to E13), legality (E1, E3, E4, E5, E6, E7, E9 to E13) and scientific and rational criteria (E1, E2, E8, E9, E10, E12, E13).	In this regard, the interviewee with code E3 prioritizes legality, while from another perspective, interviewee E2 mentioned expert support, and in this regard, interviewee E8 mentioned sound judgment, while from another perspective, interviewees E10 and E12 first examine legality and authenticity.

Thematic axis	Convergence	Divergence
Legal treatment (specific objective 1)	Aspects pending consolidation (E1, E2, E3, E5, E9 to E13); rational valuation, legitimacy and defense as guiding principles.	Regarding this, the interviewee with code E8 considered the treatment correct; meanwhile, interviewees E10 and E12 describe offices that require records, forensic copies, and expert opinions, compared to others that accept arrests. From another perspective, interviewee E11 points out that value is given to arrests without analyzing legality or custody.
Evidentiary assessment by judges (specific objective 2)	Reliability linked to verifiable conditions of obtaining, preserving or examining; joint assessment with statements, documents, minutes and expert opinions.	E4, E6 and E7 require independent sources; E9, E10 and E12 emphasize traceability, chain of custody and hash value; E13 considers that an isolated element is hardly enough to convict.
Limitations and deficiencies (specific objective 3)	Deficiencies in extraction, documentation or preservation; need for technical support, training and protocols.	E8 denies difficulties in the courts; E10 and E12 propose a protocol based on the ISO/IEC 27037 standard; E11 and E13 propose strengthening the PNP's cybercrime area; E13 highlights the late reporting.

Note. Prepared by the author based on the matrices of interviews with legal operators (E1 to E13).

3.1 Digital evidence assessment criteria

E1, E2, E3, E5, E6, E7 and E9 to E13 emphasized authenticity and integrity, E1, E3, E4, E5, E6, E7 and E9 to E13 incorporated legality and E1, E2, E8, E9, E10, E12 and E13 applied scientific and rational criteria, while E3 prioritized legality, E2 expert support and E8 the general rules of sound judgment.

In this regard, the interviewees placed the value of digital evidence in the way it was obtained and in the possibility it possesses to reconstruct its path to trial. Along the same lines, interviewee E3 established constitutional limits as a condition of use. From another perspective, interviewees E4, E6, and E7 separated the technical verification of the archive from the decision about what It demonstrates that expert support helps to assess integrity but does not replace the judge's reasoning nor prove authorship.

In this regard, interviewees E9 to E13 identified legality, authenticity, and integrity as the preliminary filters, such that sound judgment is applied to a source that has passed this control. Meanwhile, interviewees E9, E10, E12, and E13 pointed out that express motivation allows the parties to review the judicial reasoning, and E11 emphasized that contradiction safeguards the right to defense.

3.2 Legal treatment of digital evidence

In this regard, the interviewees coded as E1, E2, E3, E5 and E9 to E13, identified the pending aspects of consolidation, such as the disparate criteria such as insufficient expert support and the lack of standardization, while on the other hand interviewee E8 considered the treatment to be correct, and from another perspective interviewees E10 and E12, described offices that require minutes, forensic copy and expert opinion versus others that allow captures with flexibility, so that the local practice is not homogeneous.

The evidentiary conflicts mentioned were the loss of metadata, the lack of the original file and the fragmentation of the conversations, while E10 and E12 added the legality of the unauthorized access to other people's accounts, E11 indicated that in Tarapoto there was no computer forensics area of the PNP, so the forensics were referred to Lima, and E13 highlighted the difficulty of attributing the authorship of an account and the delay of the operators.

3.3 Evidentiary assessment criteria of the judges

E1 and E2 highlighted the forensic image and expert support, E5 the authenticity and origin, and E9, E10, and E12 the traceability, chain of custody, and hash value, while E4, E6, and E7 demanded independent sources, since repeating a screenshot does not confirm anything on its own, and all agreed to value digital evidence along with statements, documents, minutes, and expert opinions.

While interviewees E9, E10, E12, and E13 associated reliability with forensic copying, hash value, expertise, and documented record of the route, such that corroboration with statements, minutes, bank movements, and

operator reports gives greater weight, and isolated evidence received less value, interviewee E11 maintained that support in minutes or expert opinions prevents the evidence from being questioned as illicit.

3.4 Limitations and shortcomings of the assessment

E9 to E13 identified as main limitations insufficient technical training, the shortage of computer experts in the region and the absence of extraction, forensic copying and chain of custody protocols, so E10 specified that it is a structural limitation and not a lack of will on the part of the magistrates, E11 pointed out that the electromagnetic media were stored in the prosecutor's files without chain of custody and E13 highlighted the late complaint by the victims, while E8 denied difficulties in the courts and E1, E6, E7 and E10 clarified that a deficiency does not automatically invalidate the evidence.

The proposals were varied, as E1 requested a plenary agreement, E2 judicial experts and best practices, E3 national regulation and jurisprudence, E8 a computer laboratory in Tarapoto, E10 and E12 a mandatory protocol based on the ISO/IEC 27037 standard and E11 and E13 the strengthening of the PNP's cybercrime area and immediate preservation protocols.

3.5 Documentary analysis of the files

The analysis of the five files (table 2) showed computer fraud, foreseen in article 8 of Law No. 30096, in four cases and aggravated fraud in one, with two convictions, both with suspended prison sentences, and three acquittals, two by application of in dubio pro reo and one for insufficient evidence.

Table 2 Documentary analysis of computer crime files

Code	Crime and digital evidence offered	Assessment and decision	Limitations detected
EXP1	Computer fraud (Law No. 30096, art. 8). Captures of messages and calls, record of reading the memory of the cell phone of a co-defendant, police reports and statements of co-defendants (transfer of S/ 5,432.40).	Sound criticism with individual and joint assessment; sentence of four years of suspended imprisonment and civil damages of S/ 1,000.00.	The digital evidence served as corroboration and not as direct proof of authorship; the defense alleged the absence of expert reports and bank statements.
EXP2	Aggravated fraud (Penal Code, arts. 196 and 196-A, inc. 2). Screenshots of SMS messages that simulated being from a bank, bank letters and reports of lost cards (S/ 20,000.00).	Sound judgment, freedom of proof, and circumstantial evidence. Conviction of two co-authors with suspended sentences; joint and several civil damages of S/ 3,500.00.	The perpetrators of the scam were not identified; there was no computer forensics or identification of the fake advisor's number.
EXP3	Computer fraud (art. 8), primary accomplice. Report of bank transactions and letters, lifting of bank secrecy, proof of withdrawal at an ATM in Tarapoto.	Joint assessment and reasonable doubt. Acquittal (in dubio pro reo); civil claim based on S/ 3,480.00.	Account ownership and withdrawal were isolated clues; without expertise, IP address or geolocation.
EXP4	Computer fraud (art. 8). Proof of interbank transfer, account statement and bank letters; report of loss of ID and cards submitted forty-eight hours earlier (defense).	Joint assessment and reasonable doubt. Acquittal (in dubio pro reo); no civil damages due to lack of causal link.	The prior complaint opened a reasonable alternative hypothesis; receipt of the payment did not prove authorship; digital technical evidence was lacking.
EXP5	Computer fraud (art. 8, modified by Law No. 30171). Testimonial, call and SMS captures, bank and operator letters (transfer of S/ 1,880.00).	Individual and joint assessment, presumption of innocence and peripheral corroboration (Plenary Agreement No. 2-2005/CJ-116). Acquittal due to insufficient evidence; civil claim founded for S/ 2,500.00.	The bank letters proved the transfer and ownership, but not who accessed the system or used the key; no expert analysis identified the perpetrator.

Note: Prepared by the author based on the document analysis guide; files and parties are identified by codes.

In the documentary analysis, the accreditation of the bank transfers was not enough to convict the holders of the receiving accounts, since the acquittals of EXP3, EXP4 and EXP5 were due to the fact that the accused was not linked to the manipulation of the system since alternative hypotheses remained, such as the complaint about

the loss of the cards presented forty-eight hours before the fact in EXP 4 and that the alleged prior theft of the card in EXP5, while on the other hand in the convictions of EXP1 and EXP2, the court relied on testimonies, communications and banking evidence assessed together.

4. Discussion

In this regard, these findings show that the Single-Judge Courts belonging to Tarapoto value digital evidence with the criteria of authenticity, integrity, legality and contradiction, although they do not apply them in a homogeneous way, which coincides with the approach of Julca et al. [4], Bujosa et al. [10] and Acosta 's [8], although in Tarapoto this assessment also depends on linking the evidence with authorship, an aspect that expands these backgrounds.

Devis Echandía 's theoretical postulate , demanding authenticity and integrity equates to better rational control prior to the judge's conviction, and from Ferrajoli's theoretical postulate of guarantees, the acquittals in the analyzed files, EXP3, EXP4 and EXP5, due to reasonable doubt, show us that the burden of proof, the contradiction and the presumption of innocence prevent us from an arbitrary assessment, while from Alexy's postulate, the requirement of legality raised by interviewee E3 results from a proportional balancing between criminal prosecution and the protection of communications.

Regarding the legal treatment, these results reveal a gap between the recognition of general evidentiary rules and their application within digital evidence, which is related to the postulate of Aguilar [2] and that of Avemañay et al. [6], so that the treatment appears fragmented, since there are recognized principles but no specific parameters regarding admission, verification and attribution, so that legal certainty depends more on the experience of the judge than on pre-established guidelines.

Regarding the evaluation criteria, these findings coincide with the approach of Gonzáles [3], for whom the evidence must be suitable, relevant, useful, and lawful, and with the postulates of Sandoval [7] and Acosta [8] regarding expert authentication, although here the need for expertise depends on the technical controversy, and that the decisive criterion is not the presence of digital evidence, but its capacity to prove authorship and intent, since the ownership of accounts, bank reports, and screenshots were indications that are insufficient without proper technical corroboration, as Bujosa maintains. et al. [10], repeating the same content on different media does not constitute autonomous confirmation.

Regarding the limitations, this documentary analysis supports the shortage of experts and insufficient training noted by interviewees E9, E10, E12, and E13, since several files lacked computer forensics, IP address records, and device reviews, which coincides with Avemañay 's postulate. et al. [6], Morante et al. [1], Silva [5] and Bérubé et al. [30], while the position of interviewee E8, places the problem only in the fiscal investigation, differs from those backgrounds, which describe it as institutional and technical, since its impact reaches the judicial examination.

Limitations of the study

These findings come from thirteen legal operators and with respect to the five files analyzed from Tarapoto, that is, from the perceptions and the cases that do not allow us to affirm that all the courts present the same deficiencies, so that this scope is descriptive and its transfer to other judicial districts requires caution.

5. Conclusions

Regarding the identified evaluation criteria, these included sound judgment, authenticity, integrity, legality, and joint evaluation, so that said probative effectiveness does not depend only on the existence of the digital records but on a foundation that manages to explain its context, its corroboration, and its capacity to link the accused to the investigated conduct.

This legal treatment is based on the general procedural principles of legitimacy, rational assessment, defense and contradiction, although in this regard the operators described it as unequal between offices and distinguished about the illicit obtaining of technical irregularities, without equating any deficiency with automatic invalidity.

Regarding the criteria for assessing evidence, these included the verification of the conditions of obtaining and preserving the evidence, independent corroboration, and the comparison between hypotheses, since in the acquittals, the ownership of accounts and the receipt of money were insufficient to prove criminal involvement.

Regarding these limitations, they encompassed the shortage of experts, the lack of training and extraction protocols, forensic copying and chain of custody, and the absence of expert reports, access logs and examination of devices in the files, thus confirming their structural nature.

5.1 Recommendations and future directions

In this regard, judges are advised to base their rulings on questions about the origin, preservation, attribution, and demonstrative scope of digital evidence. Along the same lines, the Judiciary is advised to standardize the criteria of authenticity, integrity, and legality through a plenary agreement.

Judges, prosecutors, and lawyers are advised to demand independent corroboration and to distinguish between admissibility and probative value. The Public Prosecutor's Office and the Judiciary are encouraged to strengthen technical support in Tarapoto with computer experts, continuous training, a computer lab, and protocols aligned with ISO/IEC 27037. It is also suggested that the analysis be expanded to include a larger set of local resolutions, thereby contrasting perceptions with jurisdictional practice.

6. Declarations

Funding. This research did not receive external funding.

Authors' contributions. Conceptualization, HVBN; methodology, HVBN and RSS; formal analysis, HVBN; research, HVBN; drafting of the original manuscript, HVBN; writing, revision and editing, RSS; supervision, RSS. All authors have read and accepted the published version of the manuscript.

Data availability. Only the convergence and divergence matrices of the interviews (E1 to E13) and the synthesis of the files (EXP1 to EXP5) are disclosed; the interview guide and the document analysis guide can be provided as supplementary material; the study was not pre-registered .

Conflict of interest. The authors declare that they have no conflict of interest.

7. References

[1] Morante, L., Safadi , J., & Gómez, P. (2025). Computer crimes and digital evidence in the COIP: Validity, chain of custody and forensic expertise in Ecuador. Tesla Scientific Journal, 5 (2), e542. https://doi.org/10.55204/trc.v5i2.e542

[2] Aguilar, D. (2024). Artificial intelligence in justice: Protocols for the presentation and evaluation of digital evidence obtained through AI. Official Journal of the Judiciary, 16 (22), 475–497. https://doi.org/10.35292/ropj.v16i22.1018

[3] Gonzáles, G. (2021). Criminal procedural guarantees in digital evidence. Research Journal of the Academy of the Judiciary, 3 (5), 165–174. https://doi.org/10.58581/rev.amag.2021.v3n5.09

[4] Julca, I., Segura, M., & Ordeano , D. (2025). The challenge of cyberjustice : Criteria for evaluating digital evidence in Peru. Llalliq , 5 (2), 287–300. https://doi.org/10.32911/llalliq.2025.v5.n2.1306

[5] Silva, G. (2022). Obtaining digital evidence in cybercrimes in the Lima Norte prosecutor's office, 2021 [Undergraduate thesis, César Vallejo University]. https://hdl.handle.net/20.500.12692/96824

[6] Avemañay , S., Avemañay , A., & Duarte, M. (2025). Digital evidence in the Ecuadorian criminal process: Constitutional, technical, and comparative challenges in light of Ibero-American standards of technological evidence. Ciencia Latina Multidisciplinary Scientific Journal, 9 (5), 17880–17900. https://doi.org/10.37811/cl_rcm.v9i6.21212

[7] Sandoval, R. (2025). Cybercrimes and investigative measures in cybercrimes, the undercover agent in the criminal procedure code and the practice of evidence. Digital Journal of Criminal Sciences of Costa Rica, 5 (36), 1–43. https://doi.org/10.15517/xx9z3843

[8] Acosta, C. (2023). Documentary evidence from computer sources based on digital documents with certified electronic signatures: An analysis from the perspective of information technologies and the principle of freedom of proof in the Venezuelan criminal process. Chilean Journal of Law and Technology, 12 (5), 1–40. https://doi.org/10.5354/0719-2584.2023.68567

[9] López, Z. (2023). Legal validity of digital evidence in Guatemala. Revista Ciencia Multidisciplinaria CUNORI, 7 (2), 203–214. https://doi.org/10.36314/cunori.v7i2.238

[10] Bujosa , L., Bustamante, M., & Tor, L. (2021). Digital evidence resulting from secret surveillance: Obtaining, admissibility and evaluation in criminal proceedings in Spain and Colombia. Revista Brasileira de Direito Criminal Procedure , 7 (2), 1347. https://doi.org/10.22197/rbdpp.v7i2.482

[11] Valverde, L. (2024). Computer evidence: The problem of its reliability. Ius et Veritas, (68) , 66–79. https://doi.org/10.18800/iusetveritas.202401.005

[12] Ludeña, L., Diaz, H., & Calixto, D. (2025). Handling digital evidence in the investigation of child pornography crimes. Revista Escpogra PNP, 4 (2), 205–220. https://doi.org/10.59956/escpograpnpv4n2.14

[13] Ventura, C., & Robles, M. (2024). Artificial intelligence and the evaluation of evidence in the Peruvian criminal process. CienciaMatria , 10 (19), 303–314. https://doi.org/10.35381/cm.v10i19.1393

[14] Alexy, R. (1985). Theory of fundamental rights . Fareso . https://www.pensamientopenal.com.ar/system/files/2014/12/doctrina37294.pdf
[15] Rawls, J. (1971). A Theory of Justice . Cambridge. https://www.pensamientopenal.com.ar/system/files/2019/12/doctrina48358.pdf
[16] Osorio, S. (2010). John Rawls: A theory of social justice and its claim to validity for a society like ours. Journal of International Relations, Strategy and Security, 5 (1), 137–160. https://doi.org/10.18359/ries.136
[17] Ferrajoli, L. (1989). Theory of Penal Guarantees . Faculty of Law, UNAM. https://biblio.juridicas.unam.mx/bjv/detalle-libro/4122-garantismo-penal-coleccion-facultad-de-derecho
[18] Devis Echandía, H. (1970). General Theory of Judicial Evidence (6th ed.). Editorial Temis. https://es.scribd.com/doc/79035479/Teoria-General-de-La-Prueba-Judicial-Tomo-i-Hernando-Devis-Echandia-2
[19] Bustamante, R. (1997). The fundamental right to present evidence and its essential content. Ius et Veritas, 8 (14), 171–185. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15713
[20] Ismail, I., & Zainol , K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLoS ONE, 20 (9), 1–26. https://doi.org/10.1371/journal.pone.0331683
[21] Miller, C. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. Forensic Science International: Synergy, 6 (6), 1–22. https://doi.org/10.1016/j.fsisyn.2022.100296
[22] Stoykova , R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, 42 (5), 1–20. https://doi.org/10.1016/j.clsr.2021.105575
[23] Stoykova , R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. Computer Law & Security Review, 49 , 1–26. https://doi.org/10.1016/j.clsr.2023.105801
[24] Alruwaili , F. (2021). CustodyBlock : A distributed chain of custody evidence framework. Information, 12 (2), 1–12. https://doi.org/10.3390/info12020088
[25] Bonomi, S., Csini , M., & Ciccotelli , C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. International Conference on Blockchain Economics, Security and Protocols, 71 (12), 1–15. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12
[26] Insa , F. (2007). The admissibility of electronic evidence in court (AEEC): Fighting against high-tech crime—-Results of a European study. Journal of Digital Forensic Practice, 1 (4), 285–289. https://doi.org/10.1080/15567280701418049
[27] Moussa, A. (2021). Electronic evidence and its authenticity in forensic evidence. Egyptian Journal of Forensic Sciences, 11 (20), 1–10. https://doi.org/10.1186/s41935-021-00234-6
[28] Maimon , D., & Louderback , E. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2 (4), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057
[29] Stoykova , R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. Computer Law & Security Review, 55 (6), 1–16. https://doi.org/10.1016/j.clsr.2024.106040
[30] Bérubé, M., Beaulieu, L., Allard, S., & Denault , V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. Science & Justice, 65 (5), 1–11. https://doi.org/10.1016/j.scijus.2025.101306
[31] Chun Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. SAGE Open Medicine, 7 , 1–8. https://doi.org/10.1177/2050312118822927
[32] Bazen , A., Barg , F., & Takeshita, J. (2021). Research techniques made simple: An introduction to qualitative research. Journal of Investigative Dermatology, 141 (2), 241–247. https://doi.org/10.1016/j.jid.2020.11.029
[33] Esquivel, J., & Reyes, S. (2025). Triangulation in qualitative and mixed methods research: A strategy for scientific validity and reliability. International Journal of Educational Technologies, 10 (2), 13–26. https://doi.org/10.62701/revedutech.v10.5480