Indonesian Journal of Criminal Law Studies
ISSN 2548-1568 (Print) 2548-1576 (Online)
Vol. 11 Issue 1 (2026) 467-514
DOI: https://doi.org/10.15294/ijcls.v11i1.47067
Online since: May 9, 2026

Indonesian Journal of CRIMINAL LAW STUDIES
https://journal.unnes.ac.id/journals/ijcls/index

Digital Evidence Management in the Criminal Justice System: Towards a Fair and Technology-Responsive Legal Framework

Ismail Marzuki[a] ✉, I Gede Widhiana Suarda[b], Fendi Setyawan[c], Reece Walters[d]

[a] Faculty of Social and Humanities, Universitas Nurul Jadid, Indonesia
[b] Faculty of Law, Universitas Jember, Indonesia
[c] Faculty of Law, Universitas Jember, Indonesia
[d] Faculty of Arts and Education, Deakin University, Australia

✉ Corresponding Email: ismail.hukum@unuja.ac.id

Abstract

The increasing reliance on digital evidence in criminal justice proceedings poses new challenges for legal systems that were traditionally built to deal with physical and conventional evidence. With the development of information technology, digital data such as electronic communications, digital traces, and cyber forensic artefacts have become an important part of criminal case evidence. This article presents a conceptual analysis of the urgency of fair and technology-responsive digital evidence management in the criminal justice system. Through a literature review of legal theory, international practices, and national regulations, this paper identifies significant legal gaps, particularly in data authenticity, the chain of evidence, the validity of evidence, and the protection of privacy rights. In its novelty, this article proposes a five-pillar model for the governance of digital evidence, encompassing the principles of legality, evidence integrity,

procedural justice, legal digital literacy, and institutional accountability, as an integrated framework to strengthen the management of digital evidence in Indonesia. This model provides a systematic approach that not only focuses on the technical aspects of digital forensics but also integrates legal normative standards, institutional capacity building, and the protection of fundamental rights within the criminal justice process. The scientific contribution of this research lies in its effort to bridge the conceptual gap between the principle of procedural justice and digital forensic practices within the criminal justice system, thereby supporting the realization of a legal framework that is responsive, transparent, adaptable to technological advancements, and oriented toward the protection of human rights. Ultimately, this article calls for a legal framework that not only accommodates the characteristics of digital evidence but also protects defendants' fundamental rights in criminal proceedings.

Keywords
Digital Evidence, Criminal Procedure Law, Legal Framework, Procedural Justice, Validity of Evidence.

Introduction

The development of information and communication technology (ICT) in the last two decades has fundamentally changed almost all aspects of human life, including the legal system and criminal justice.[1] In this digital era, evidence presented in law enforcement processes is no longer limited to printed documents, physical evidence, or direct testimony, but increasingly takes the form of electronic data,[2] such as digital

[1] Atikah Mardhiya Rohmy et al., "UU ITE dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi," *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam* 7, no. 2 (2021): 309, https://doi.org/10.54471/dakwatuna.v7i2.1202; Khofidhotur Rovida and Sasmini Sasmini, "Evaluasi Sistem Hukum Indonesia dalam Menangani Cyberbullying Berbasis Teknologi Informasi dan Komunikasi," *DIVERSI : Jurnal Hukum* 10, no. 1 (2024): 169, https://doi.org/10.32503/diversi.v10i1.5223.

[2] H. Eddy Army, *Bukti Elektronik dalam Praktik Peradilan* (Sinar Grafika, 2020).

conversations,[3] metadata,[4] cloud-based CCTV recordings,[5] digital transactions, and network activity logs.[6] This evidence, generally referred to as digital evidence, now plays a crucial role in proving criminal cases at the investigation, prosecution, and trial stages.

Indonesia, as a country with a massive digital population, has more than 213 million internet users as of January 2023,[7] cannot avoid the complexity of digital evidence in law enforcement. On the other hand, Indonesia's criminal justice system, which is based on conventional criminal procedure law (KUHAP 1981), is not yet fully prepared to accommodate the characteristics of digital evidence[8] which is dynamic and unique,[9] easily altered, dispersed, and often difficult to verify without technical expertise. The gap between technological advances and legislative stagnation poses serious challenges in ensuring procedural fairness and protecting human rights in the judicial process.

---

[3] Made Sugi Hartono and Ni Putu Rai Yuliartini, "Penggunaan Bukti Elektronik dalam Peradilan Pidana," *Jurnal Komunikasi Hukum (JKH)* 6, no. 1 (2020): 281, https://doi.org/10.23887/jkh.v6i1.23607.

[4] I. Gede Widhiana Suarda et al., "Illicit Cigarette Trade in Indonesia: Trends and Analysis from the Recent Judgments," *Sriwijaya Law Review*, January 31, 2024, 38–59, https://doi.org/10.28946/slrev.Vol8.Iss1.2726.pp38-59.

[5] Desti Mualfah and Rizdqi Akbar Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi* 11, no. 2 (2020): 257–67, https://doi.org/10.31849/digitalzone.v11i2.5174.

[6] Gresia Wulaning Rum, "Penggunaan Alat Bukti Elektronik dalam Proses Peradilan Perdata," *Jurnal Multidisiplin Ilmu Akademik (JMIA)* 2, no. 1 (2025): 61–68, https://doi.org/10.61722/jmia.v2i1.3151; Trisnawati Trisnawati and Shofia Hanifah, "Perkembangan Alat Bukti Elektronik Hasil Peretasan (Hacker) Sebagai Alat Bukti dalam Tindak Pidana," *Multidisciplinary Indonesian Center Journal (MICJO)* 1, no. 3 (2024): 1344–49, https://doi.org/10.62567/micjo.v1i3.162.

[7] Riziqi Abista Bagaskara and Catur Suratnoaji, "Representasi Kepemimpinan Transformasional Anies Baswedan Sebagai Calon Presiden 2024 di Media Sosial Instagram @aniesbaswedan (Studi Analisis Semiotika Roland Barthes Kepemimpinan Transformasional Anies Baswedan Sebagai Calon Presiden 2024 di Media Sosial Instagram @aniesbaswedan)," *JIIP - Jurnal Ilmiah Ilmu Pendidikan* 7, no. 10 (2024): 11785–92, https://doi.org/10.54371/jiip.v7i10.6132.

[8] Mustalim Lasaka, "Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law," *Jurnal Legalitas* 16, no. 2 (2023): 154–66, https://doi.org/10.33756/jelta.v16i2.20306.

[9] Humaira Arshad et al., "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *Journal of Information Processing Systems* 14, no. 2 (2018): 346–76, https://doi.org/10.3745/JIPS.03.0095.

Cases of cyber and non-cybercrimes involving digital evidence have increased sharply. For example, cases of hate speech through social media that are very harmful to victims and the wider community,[10] illegal transactions through digital platforms, such as the use of digital currency (Bitcoin) in money laundering crimes,[11] to forensic evidence in murder cases involving tracking the victim's location through cell phone signals.[12] However, in practice, law enforcement officials, lawyers, and judges often face dilemmas: Is such digital evidence legally valid? Do the procedures for collecting and verifying such evidence comply with the principles *of due process of law?* And how can the right to privacy and the right not to be prosecuted based on illegally obtained evidence be guaranteed?

Digital evidence has unique characteristics that distinguish it from conventional evidence. It is intangible, instantly replicable (volatile), easily manipulated, and dependent on complex devices and systems.[13] The biggest challenge in digital evidence management is ensuring the integrity, authenticity, and continuity of the chain of custody from the moment the evidence is discovered until it is used in court.[14] Furthermore, in a global context, developed countries have developed new legal approaches to address these challenges, such as the Digital Evidence Guidelines by the Council of Europe,[15] the Electronic Communications Privacy Act (ECPA)

---

[10] Ina Weber et al., "Features for Hate? Using the Delphi Method to Explore Digital Determinants for Online Hate Perpetration and Possibilities for Intervention," *Cyberpsychology, Behavior, and Social Networking* 26, no. 7 (2023): 479–88, https://doi.org/10.1089/cyber.2022.0195.

[11] Ezhilmathi S and Selvakumara Samy S, "Identifying Illicit Transactions in Bitcoin Tumbler Services Using Supervised Machine Learning Algorithms," *2023 12th International Conference on Advanced Computing (ICoAC)*, August 17, 2023, 1–8, https://doi.org/10.1109/ICoAC59537.2023.10249782.

[12] Alexios Mylonas et al., "Smartphone Sensor Data as Digital Evidence," *Computers & Security* 38 (October 2013): 51–75, https://doi.org/10.1016/j.cose.2013.03.007.

[13] David Chaikin, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence," *Crime, Law and Social Change* 46, nos. 4–5 (2006): 239–56, https://doi.org/10.1007/s10611-007-9058-4.

[14] Moch Bagoes Pakarti, "Manajemen Pengelolaan Bukti Digital untuk Meningkatkan Aksesibilitas Laboratorium Forensika Digital" (Universitas Islam Indonesia, 2020), https://dspace.uii.ac.id/handle/123456789/28258.

[15] Remigijus Jokubauskas and Marek Świerczyński, "Is Revision of the Council of Europe Guidelines on Electronic Evidence Already Needed?," *Utrecht Law Review* 16, no. 1 (2020): 13–20, https://doi.org/10.36633/ulr.525.

in the United States,[16] and e-discovery rules in various common law systems.[17]

In Indonesia, although there are several sectoral regulations, such as the ITE Law, the Personal Data Protection Law, and Supreme Court Regulations (Perma) related to e-court,[18] there is still no systematic, comprehensive legal framework grounded in procedural justice principles for handling digital evidence in criminal contexts. This has resulted in inconsistencies in legal practice, potential human rights violations, and low legal certainty. In court proceedings, digital evidence is often deemed valid or invalid solely at the judge's discretion, without reference to technical or ethical standards for digital forensics. Furthermore, in the context of criminal justice that upholds the principles of the presumption of innocence and the right to a fair defense, the unaccountable handling of digital evidence can become a tool for criminalization or for the abuse of power.[19] Therefore, establishing a legal framework that is fair and responsive to technology is a necessity, not an option.

The development of international literature on digital evidence and the criminal justice system shows a paradigm shift in the legal approach to information technology. In traditional legal systems, evidence emphasizes the physical existence of evidence that can be verified directly.[20] However, in the digital context, evidence is intangible, easily replicated, and highly dependent on the integrity of technology. Therefore, legal thinking

---

16 Tri Rudiyanto et al., "Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States," *Lex Publica* 10, no. 1 (2023): 84–100, https://doi.org/10.58829/lp.10.1.2023.84-100.

17 C. G. Shilling, "Electronic Discovery: Litigation Crashes into the Digital Age," *The Labor Lawyer* 22, no. 2 (2006): 207–32.

18 Hafizatul Ulum and M. Dewa Ginting Singaulung, "Implementasi Peraturan Mahkamah Agung Republik Indonesia Nomor 7 Tahun 2022 Tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik: Studi Kasus di Pengadilan Negeri Praya," *JISHUM : Jurnal Ilmu Sosial Dan Humaniora* 2, no. 1 (2023): 75–88, https://doi.org/10.57248/jishum.v2i1.280.

19 Rohman Rohman et al., "Sistem Pembuktian dalam Hukum Pidana Indonesia dan Tantangan dalam Proses Peradilan," *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin* 1, no. 3 (2024): 279–92, https://doi.org/10.71153/jimmi.v1i3.146.

20 Muhammad Humam Makmun, "Transformasi Sistem Pembuktian di Pengadilan: Antara Tradisi dan Modernisasi Digital," *YUDHISTIRA: Jurnal Yurisprudensi, Hukum dan Peradilan* 1, no. 2 (2023): 36–43, https://doi.org/10.59966/yudhistira.v1i2.1694.

regarding validity, chain of evidence, and procedural justice has undergone a significant conceptual shift.

A study by Aidil Putra Dalimunthe shows that one of the biggest challenges in modern criminal procedure law is developing a legal framework that balances the need for digital investigation with the protection of privacy rights and the principle of non-self-incrimination.[21] In his study, he emphasizes that many jurisdictions lack explicit standards for authenticating digital evidence, leading to legal uncertainty and judicial inconsistency. The study[22] discusses digital forensics in ensuring data integrity, namely by ensuring that data remains intact from collection through presentation in court, which can be achieved by using cryptographic hash functions to verify data integrity. This is in line with the chain-of-custody principle common in criminal justice systems. Still, in a digital context, this principle requires technical adaptations, such as hashing, time-stamping, and audit logs.[23]

From a normative perspective, Kerr, in his work "The Digital Fourth Amendment: Privacy and Policing in Our Online World," explains when the government can read your emails or monitor your browsing activity on the internet, and when the police can search your cell phone or copy your computer files. In the United States, the answers to these questions come from the Fourth Amendment to the Constitution and the prohibition against unreasonable searches and seizures.[24] Furthermore,

---

[21] Aidil Putra Dalimunthe, "Legality of The Practice of Wiretapping Methods Against Perpetrators of Criminal Acts of Corruption in The Provisions of The Law on Criminal Acts of Corruption," *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam* 5, no. 2 (2024): 80, https://doi.org/10.58836/al-qanun.v5i2.21762.

[22] Mrunali Chopade et al., "Digital Forensics: Maintaining Chain of Custody Using Blockchain," *2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, December 2019, 744–47, https://doi.org/10.1109/I-SMAC47947.2019.9032693; James Johnson et al., "On the Digital Forensics of Heavy Truck Electronic Control Modules," *SAE International Journal of Commercial Vehicles* 7, no. 1 (2014): 72–88, https://doi.org/10.4271/2014-01-0495.

[23] Juan Vázquez-Pérez and Angélica González-Arrieta, "Implementation of Blockchain in the Digital Chain of Custody to Enhance Digital Data Assurance," in *Blockchain and Applications, 6th International Congress*, vol. 1256, ed. Javier Prieto et al., Lecture Notes in Networks and Systems (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-81928-5_39.

[24] Orin Kerr, *The Digital Fourth Amendment: Privacy and Policing in Our Online World*, 1st ed. (Oxford University PressNew York, NY, 2025), https://doi.org/10.1093/9780190627102.001.0001.

inconsistencies between national legal frameworks and international practices can hinder the validity of digital evidence in extradition or cross-border legal cooperation processes. This is emphasized by[25] that different jurisdictions have varying standards regarding the admissibility and handling of digital evidence. In this context, *mutual legal assistance treaties* (MLATs) and the harmonization of digital evidence standards between countries are important.

However, most of these studies remain partial in nature, as they have not comprehensively integrated the dimensions of the normative validity of digital evidence, procedural justice, institutional capacity of law enforcement agencies, and the responsiveness of the criminal justice system to technological developments within a unified conceptual framework. Consequently, a significant research gap remains regarding the need for an integrated conceptual model that bridges the legal, technical, procedural, and institutional aspects of digital evidence governance in Indonesia.

In response to this gap, this article offers a novel contribution in the form of a five-pillar conceptual model for the governance of digital evidence, consisting of the principles of legality, evidentiary integrity, procedural justice, legal digital literacy, and institutional accountability as a comprehensive framework for the reform of Indonesia's criminal procedure law. This model does not merely examine digital evidence from the perspective of forensic techniques or privacy protection alone; rather, it integrates normative dimensions, procedural safeguards, law enforcement personnel's capabilities, and institutional oversight mechanisms into a systemic approach responsive to the challenges of the digital era. Accordingly, this study provides a new conceptual contribution to strengthening a technology-based criminal evidentiary system that is more adaptive, equitable, and aligned with international standards of practice.

The theoretical framework used in this article refers to two main approaches: (1) *Procedural Justice Theory* and (2) *Respons*ive Legal Theory.

---

[25] Andrea Colaiocco, "The Relevance of Best Practices in the Acquisition of Digital Evidence in Light of the News on Judiciary Cooperation," *Archivio Penale* 71, no. 1 (2019).

Procedural Justice Theory emphasizes that the criminal justice system must guarantee a fair, impartial, transparent legal process that respects the rights of the accused.[26] In the context of digital evidence, this theory requires that the process of collecting, storing, and processing data be conducted ethically, accountably, and without violating constitutional rights such as privacy and the right to a defense.

Meanwhile, the Theory of Legal Responsiveness to Technology states that the law must be adaptive to social and technological changes, rather than static. Rapid technological advances have led to social change, which in turn requires legal framework updates to address new challenges while ensuring justice and equality.[27] Thus, criminal procedure law must be able to respond to the changing characteristics of evidence in the digital age through both normative and technical updates.

Based on these two approaches, the management of digital evidence is not only seen as a technical or procedural issue, but also as an integral part of systemic justice in the criminal justice process. By understanding the dynamics between technology and law, this framework provides a conceptual basis for developing a criminal procedure model that guarantees the validity, fairness, and accountability in the use of digital evidence.

Based on the above background and urgency, this article is designed to address the main issues of this study, namely the main legal challenges in digital evidence management in the current criminal justice system in Indonesia, how the characteristics of digital evidence affect the principles of evidence and procedural justice in criminal procedure law, and what

---

[26] Eva Brems and Laurens Lavrysen, "Procedural Justice in Human Rights Adjudication: The European Court of Human Rights," *Human Rights Quarterly* 35, no. 1 (2013): 176–200, https://doi.org/10.1353/hrq.2013.0000; Tom R. Tyler, "The Legitimacy of Legal Institutions," in *Research Handbook on Law and Psychology*, ed. Rebecca Hollander-Blumoff (Edward Elgar Publishing, 2024), https://doi.org/10.4337/9781800881921.00011.

[27] Diego Bianchi De Oliveira and Rogério Mollica, "A Função Do Amicus Curiae Como Mecanismo De Acesso À Justiça Nas Demandas Judiciais Envolvendo Novas Tecnologias," *Revista Eletrônica de Direito Processual* 25, no. 1 (2024), https://doi.org/10.12957/redp.2024.81888; Agota Czarnecka, "New Questions, Old Problems. Philosophy of Law and Contemporary Challenges," *Prawo i Wiez* 2019, no. 29 (2019): 57–69.

conceptual framework can be offered to address the need for a legal system that is fair and responsive to digital technology.

The main objective of this article is to develop a conceptual analysis of digital evidence management in the criminal justice system, with an emphasis on the importance of establishing a legal framework that guarantees justice and is adaptive to technological developments. Specifically, this article aims to identify and critique legal gaps in the handling of digital evidence in Indonesia based on a review of national and international literature, analyze the technical and normative characteristics of digital evidence in relation to criminal procedure law, and develop a proposed conceptual framework that combines normative, technological, and human rights approaches for fair and transparent digital evidence management.

The main contribution of this article lies in offering an alternative framework for digital evidence governance that has not been systematically explored in Indonesian legal literature. Amidst rapid digital transformation and the challenges posed by technological disruption to the legal system, this article presents a constructive legal perspective based on the values of procedural justice. Thus, this article is expected to serve as a reference for policymakers, academics, and legal practitioners in promoting the reform of the criminal justice system in the digital age.

Method

This study uses a legal-normative approach, a legal research method that analyses legal issues from the perspective of positive law, understood as a collection of rules or norms.[28] This approach was chosen because the issues discussed in this article are theoretical-conceptual in nature and are closely related to the provisions of applicable laws and regulations and universal

[28] Achmad Irwan Hamzani et al., "Implementation Approach in Legal Research," *International Journal of Advances in Applied Sciences* 13, no. 2 (2024): 380, https://doi.org/10.11591/ijaas.v13.i2.pp380-388.

legal principles, particularly those concerning the management of digital evidence in the criminal justice system.

Within the legal-normative framework, this study applies several approaches as follows:

1. *The Statute* Approach, which involves analyzing legal documents and laws to understand the legal framework governing a particular issue.[29] This approach is used to examine positive legal rules on criminal and digital evidence, including the Criminal Procedure Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and their implementing regulations.
2. *Conceptual Approach*: In legal research, the conceptual approach examines legal issues from a theoretical perspective, focusing on the principles and fundamental concepts that shape the law.[30] In this study, the conceptual approach is used to examine the basic concepts in the law of evidence, procedural justice, and the principles of human rights protection in the criminal justice process.
3. *The Comparative* Approach, which involves comparing different legal systems to identify similarities and differences, can help improve, reform, and modernize national legislation.[31] This approach compares how digital evidence management practices are regulated in various countries, such as the United States, the United Kingdom, and Germany, as well as in international instruments, such as *the Budapest Convention on Cybercrime.*

Furthermore, this study employs a qualitative, normative legal-reasoning approach that emphasizes the systematic construction of legal arguments by examining the interrelationships among positive legal

---

[29] Sukri Paluttri, "Comparative Approach in Public Health Social Security: A Legal Case Study of the Indonesian, France, and Singapore Health Systems," *International Journal of Human Rights in Healthcare* 17, no. 5 (2024): 572–87, https://doi.org/10.1108/IJHRH-03-2023-0020.

[30] Alessio Sardo and Allegra Grillo, "Mapping Legal Consciousness in Comparative Law: An Essay on Methodology," in *Legal Consciousness*, vol. 142, ed. Jakob V. H. Holtermann et al., Law and Philosophy Library (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-031-87962-3_6.

[31] Blerton Sinani and Mehmeti Sami, "The Importance of Comparative Law for the Development of Contemporary Law," *Juridical Tribune - Review of Comparative and International Law* 15, no. 1 (2025): 5–23, https://doi.org/10.62768/TBJ/2025/15/1/01.

norms, general principles of law, and relevant legal doctrines. Through this approach, the analysis is conducted not only descriptively with respect to statutory provisions but also interpretatively to identify and articulate the deeper normative meanings underlying the regulation of digital evidence.

This research utilizes primary and secondary legal materials as the main data sources. Primary legal materials consist of national legislation: Criminal Procedure Code, Electronic Information and Transactions Law, Law No. 12 of 2005 concerning Ratification of the International Covenant on Civil and Political Rights, and others, including international legal instruments such as *the Budapest Convention, Electronic Communications Privacy Act (ECPA), Federal Rules of Evidence (FRE), and Police and Criminal Evidence Act (PACE).* Meanwhile, secondary legal materials include scientific literature from national and international journals on digital law, evidence, and human rights, textbooks on criminal procedure and evidence law, and digital forensics practice guidelines from professional institutions such as ENISA (*European Union Agency for Cybersecurity)*.

Data collection techniques included documentation studies and literature reviews of regulations, official documents, scientific journals, and academic publications relevant to the topic. Data were collected systematically, classified by topic, and analyzed according to the formulated legal issues. The analysis of legal materials was conducted qualitatively using legal interpretation methods, including grammatical, systematic, and teleological approaches. This study did not use statistical analysis or quantitative data; instead, it emphasized argumentative construction, logical coherence, and harmony among legal norms, principles of justice, and information technology practices.

With this approach, the study aims to develop a comprehensive, in-depth legal argument for the urgency of updating the legal framework for evidence in the Indonesian criminal justice system to be more responsive to the digital era, without neglecting the principles of procedural justice and the protection of human rights.

Results and Discussion

A. Special Characteristics of Digital Evidence in the Criminal Justice System

The development of digital technology has expanded the scope and forms of evidence available in criminal justice proceedings. *Digital evidence* refers to information or data stored or transmitted in digital format that can support or refute theories about how a crime occurred, including other matters related to the essential elements of a crime, such as intent or alibi.[32] In other words, digital evidence can be used in court to prove legal facts in a case. The characteristics of digital evidence are fundamentally different from those of conventional evidence and pose their own legal challenges that require critical analysis. Here are some characteristics of digital evidence that need to be considered:

1. Intangibility

   Unlike physical evidence such as sharp weapons, printed documents, or physical video recordings, digital evidence does not have a visible physical form. It can only be accessed through certain hardware (computers, mobile phones, servers) and only "exists" to the extent that electronic systems can read and process it (volatile).[33] This invisibility complicates manual verification and requires specialized forensic tools and technical expertise to confirm its existence. For example, *log files* of user activity on a system can be important clues in cases of hacking or digital fraud. Still, this data is not immediately visible and can be easily deleted, falsified, or hidden within the operating system's structure.

---

[32] Eoghan Casey, "Reconstructing Digital Evidence," in *Crime Reconstruction* (Elsevier, 2011), https://doi.org/10.1016/B978-0-12-386460-4.00017-5.

[33] Joon-Taik Lee et al., "Gathering and Storage Technique Implementation of Volatility Memory Data for Real-Forensic," *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, 2009, 1076–79, https://doi.org/10.1109/ICCIT.2009.234; Virginia M. Maxwell, "Digital Evidence," in *Investigating Animal Abuse Crime Scenes*, 1st ed., by Virginia M. Maxwell and Martha Smith-Blackmore (CRC Press, 2023), https://doi.org/10.4324/9781003090762-15.

2. Easily Modified and Replicated Without a Trace (Volatile and Easily Altered)

Digital evidence is highly susceptible to alteration; digital files can be changed in seconds without leaving a physical trace, using readily available software, making it difficult to detect manipulations.[34] Digital evidence, especially volatile data such as RAM, can easily be lost when the device is turned off, making it even more difficult to preserve its original state.[35] For example, metadata in a document or photo can be manipulated to change the time, location, or user identity information. Additionally, digital data can be replicated indefinitely, creating legal challenges for courts when they must determine which copies are authentic and which have been modified. These characteristics reinforce the urgency of strict procedures and forensic documentation, such as the use of checksums, hash values (e.g., SHA-256), and logging systems to maintain *the integrity* and *authenticity* of collected digital evidence.[36]

3. Dependent on Specific Technology Infrastructure and Formats

Accessing and reading digital evidence cannot be separated from reliance on specific software and hardware to examine it effectively. Data may not be accessible if certain operating systems or applications are not used. Such dependence can pose challenges when the necessary devices are unavailable or incompatible with the evidence being analyzed.[37] Ultimately, this leads to technical compatibility issues and the risk of "digital *obsolescence*," where data

---

[34] Chien-Lung Hsu et al., "Secure Handwritten Protocol for Protecting Integrity of Digital Evidences," *2024 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, December 10, 2024, 1–4, https://doi.org/10.1109/ISPACS62486.2024.10869225; Rajneesh Rani et al., "A Brief Review on Existing Techniques for Detecting Digital Image Forgery," *2021 Sixth International Conference on Image Information Processing (ICIIP)*, November 26, 2021, 533–38, https://doi.org/10.1109/ICIIP53038.2021.9702688.

[35] Maxwell, "Digital Evidence."

[36] Abdul Muni, *Kriptografi Untuk Keamanan Sistem Informasi* (Penerbit KBM Indonesia, 2024).

[37] Mark Pollitt, "The Key to Forensic Success: Examination Planning Is a Key Determinant of Efficient and Effective Digital Forensics," in *Digital Forensics* (Elsevier, 2016), https://doi.org/10.1016/B978-0-12-804526-8.00002-2.

becomes unreadable because the technology is outdated. This often occurs with old CCTV recordings that require specialized codecs or proprietary formats from specific security devices, which law enforcement cannot open without the manufacturer's intervention.

4. Distributed and Fragmented

Digital evidence is often scattered across multiple locations and not physically concentrated. For example, WhatsApp messages between two parties may be stored on both parties' phones, in the cloud server, and in backup systems, making it difficult to collect and verify the data.[38] This poses challenges in determining *the completeness* of the data, as well as in ensuring that the data presented to the court is an accurate representation of the actual events.[39] Furthermore, in the context *of cloud computing,* data is often stored across countries, which raises challenges of jurisdiction and international legal cooperation. Access to this data is often restricted by service providers' privacy policies or even by the laws of the country where the servers are located.

5. Contains Complex Additional Information (Embedded Metadata)

Digital evidence not only stores primary information but also *hidden* information (such as metadata) that investigators may not be able to access in some cases. Metadata can include the creation time, which indicates when the file or document was created; GPS location, which provides the geographic coordinates of where the file was created; IP address, which identifies the network location where the file was accessed or sent; device ID as a unique identifier; and

---

[38] Kanika Pandit and Renu Mahajan, "Cloud and AI Fusion: Revolutionizing Electronic Evidence Admissibility in the Digital Age," *2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, June 27, 2024, 1–5, https://doi.org/10.1109/ECAI61503.2024.10607551.

[39] Mohammad A. Alsmirat et al., "Digital Video Forensics: A Comprehensive Survey," *International Journal of Advanced Intelligence Paradigms* 15, no. 4 (2020): 437, https://doi.org/10.1504/IJAIP.2020.106040.

identification of the software used.[40] Although it can assist in tracing and validation, metadata is also susceptible to falsification or deletion. For example, in cases of digital pornography or child exploitation, metadata from image files can reveal the location where the image was taken, the device used, and the exact time of capture. However, if this metadata is deleted, it becomes very difficult to reconstruct the incident without in-depth forensic expertise.

6. Volatility and Time-Sensitivity

Digital data can disappear or change automatically due to the system. For example, network logs are only stored for 7 days before being automatically deleted. Some people commonly perform this action to manage storage space while ensuring that only specific data is stored for analysis.[41] Another example is the browser cache, which stores history for a limited period and can quickly retrieve HTML pages, images, and other files stored locally, provided certain conditions are met.[42] This makes digital evidence highly time-dependent. Failure to seize devices or access data quickly can result in the loss of evidence that cannot be recovered.

The above characteristics show that digital evidence cannot be managed using the same standards of proof as physical evidence. Criminal justice systems that wish to accommodate digital evidence lawfully and fairly must develop standards of proof that account for the technological nature of the data and establish cross-disciplinary working procedures between law and digital forensics. Without an

---

[40] Fahad Alanazi and Andrew Jones, "The Value of Metadata in Digital Forensics," *2015 European Intelligence and Security Informatics Conference*, September 2015, 182–182, https://doi.org/10.1109/EISIC.2015.26; Jaehyeok Han et al., "ECo-Bag: An Elastic Container Based on Merkle Tree as a Universal Digital Evidence Bag," *Forensic Science International: Digital Investigation* 49 (June 2024): 301725, https://doi.org/10.1016/j.fsidi.2024.301725.

[41] Yan Li Lv et al., "The Research and Realization of a Kind of Log Management-Oriented Descriptive Language to Describe the Security of Computer Network," *Applied Mechanics and Materials* 556–562 (May 2014): 5765–70, https://doi.org/10.4028/www.scientific.net/AMM.556-562.5765.

[42] Florian Dehling et al., "Rotten Cellar: Security and Privacy of the Browser Cache Revisited," in *Secure IT Systems*, vol. 11875, ed. Aslan Askarov et al., Lecture Notes in Computer Science (Springer International Publishing, 2019), https://doi.org/10.1007/978-3-030-35055-0_2.

adequate normative and technical framework, digital evidence can actually undermine the principle of procedural justice, whether due to manipulation, abuse of authority in collection, or doubts about authenticity in court. Therefore, a deep understanding of the characteristics of digital evidence is the foundation for designing adaptive regulations and an accountable evidence system.

B. Legal Challenges to Digital Evidence in the Criminal Justice System

Although digital evidence has become an integral part of the criminal justice process in the digital era, the legal systems in many countries, including Indonesia, are not yet fully prepared to handle the complexity and dynamics of this type of evidence. The legal challenges that arise are not only related to the normative dimension, but also to the technical, procedural, and institutional dimensions. This unpreparedness risks undermining the principles of procedural justice and defendants' human rights in legal proceedings. The following are some of the legal challenges to digital evidence in the criminal justice system in Indonesia:

1. Legal Vacuum and Uncertainty

   One of the most fundamental challenges is the lack of explicit provisions on digital evidence in applicable criminal procedure law, particularly Indonesia's Criminal Procedure Code (KUHAP). The KUHAP still refers to conventional forms of evidence, as stated in Article 184, paragraph (1), which holds that valid evidence includes witness testimony, expert testimony, documents, clues, and defendant testimony.[43] In these provisions, there is no terminology for digital evidence in an equivalent or separate form as a category of evidence. As a result, the existence of digital evidence must be

[43] Dealita Dwitarani, "Kesesuaian Pembuktian Penuntut Umum dalam Tindak Pidana Penyertaan Disertai Kelalaian yang Menyebabkan Kematian dengan Pasal 184 Ayat (1) KUHAP (Studi Putusan No. 19/Pid.B/2021/Pn.Trk)," *Verstek* 10, no. 2 (2022): 336–43, https://doi.org/10.20961/jv.v10i2.67638.

interpreted as falling under the category of documents or clues,[44] which is prone to inconsistencies in application and broad *discretion* in the hands of judges. This creates legal uncertainty, especially in criminal cases that rely entirely on digital *evidence,* such as cybercrime, illegal online trade, and defamation through social media, and also extends to the processes of tracing, authenticating, and prosecuting corruption cases involving digital assets, as an increasing number of corruption offenders are becoming attracted to the use of cryptocurrencies to conceal the flow of illicit proceeds.[45] This situation is further exacerbated by the absence of a specific regulatory framework in Indonesia that explicitly addresses mechanisms for cryptocurrency governance and oversight.[46]

2. Validity and Authentication Issues

The next important challenge concerns the validity and *authentication* of digital evidence. Legally, evidence must be verifiable to be admissible in court. In the digital context, this process becomes very complex because:

a. Data can be subtly modified without leaving a physical trace.
b. Files can be cloned and falsified through *deepfakes* or metadata manipulation.
c. Evidence can be produced through *screenshots* or screen captures that are easily manipulated.

In many judicial practices in Indonesia, the authentication of digital evidence usually uses various verification methods, such as

---

[44] Iwan Setiawan et al., "Jejak Digital Sebagai Alat Bukti Petunjuk Menurut Pasal 184 Kitab Undang-Undang Hukum Acara Pidana," *Jurnal Ilmiah Galuh Justisi* 10, no. 1 (2022): 119–32, https://doi.org/10.25157/justisi.v10i1.7236.

[45] Dadang Herli Saputra and Fardana Kusuma, "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries," IJCLS (Indonesian Journal of Criminal Law Studies) 10, no. 2 (2025), https://doi.org/10.15294/ijcls.v10i2.28795.

[46] David Hardiago et al., "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law," IJCLS (Indonesian Journal of Criminal Law Studies) 10, no. 1 (2025), https://doi.org/10.15294/ijcls.v10i1.22557.

Secure Hash Algorithm (SHA-256),[47] digital timestamp,[48] encryption and audit trail.[49] However, there are no legally binding technical standards that law enforcement or the judiciary must use, so authentication often still depends on the judge's discretion, who may not always have adequate digital literacy.

3. Uncertainty in Digital Chain of Custody Procedures

The chain of custody is a fundamental principle in maintaining the integrity of evidence from collection to its use in court.[50] In the context of digital evidence, this principle is even more vulnerable because:

a. Digital data can be altered due to technical errors or device malfunctions.
b. Data copies may exist in multiple forms and be stored across various media.
c. Not all law enforcement agencies have adequate digital documentation procedures.

The absence of a national standard protocol for the digital chain of custody in Indonesia often results in evidence collection not being properly documented. This can be used as grounds for a pretrial motion by the defendant, or even invalidate the evidence if it is deemed to have been obtained unlawfully or potentially tampered with.

---

47 Fauzi Maulana Rangkuti et al., "Implementasi Digital Signature pada E-Invoice di UNIQA Digital Invitation Menggunakan Algoritma SHA-256 (Secure Hash Algorithm-256) dan RSA (Rivest Shamir Adleman)," *Jurnal Cyber Tech* 2, no. 7 (2019): 1–14, https://doi.org/10.53513/jct.v2i7.2841.

48 Hasanudin Hasanudin et al., "Juridical Analysis of the Use of Information/Electronic Documents as Evidence in Criminal Law Enforcement (Case Study Decision Number: 192/Pid.B/2023/PN Btm)," *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 3, no. 1 (2024): 118–27, https://doi.org/10.57235/aurelia.v3i1.1387.

49 Gladys Lydia Evan and Moody Syailendra, "Keabsahan Tanda Tangan Elektronik Melalui Platform DocuSign Ditinjau dari Hukum Positif di Indonesia," *UNES Law Review* 6, no. 2 (2023): 6512–20, https://doi.org/10.31933/unesrev.v6i2.1513.

50 Iwan Rasiwan, *Pengantar Hukum Forensik Indonesia* (Takaza Innovatix Labs, 2025).

4. Evidence Collection and Seizure That May Violate Privacy Rights

The collection of digital evidence often involves access to personal data, including the contents of messages, emails, calls, cloud documents, and even internet search histories. The legal procedures for accessing such data should be subject to the principle *of due process*, including court warrants (lawful warrants), restrictions on the scope of seizure, and supervision by independent institutions. However, in practice, law enforcement officials still access defendants' or witnesses' digital devices without consent or legal procedures.[51] This can be considered a violation of the right to privacy, the right against self-incrimination, and the right to a fair trial as stipulated in the Indonesian Constitution and various international human rights instruments.[52]

5. Weak Capacity of Law Enforcement and Judicial Authorities

Digital literacy and the technical capacity of law enforcement agencies remain a major challenge. Many investigators, prosecutors, and even judges lack sufficient knowledge and skills to assess the credibility of digital evidence.[53] For example:

a. They do not understand how evidence is collected forensically.
b. Inability to read *data logs* or digital metadata.
c. Not recognizing the potential for digital manipulation.

Without this capacity, the judicial system is vulnerable to misinterpreting, ignoring, or even accepting technologically manipulated evidence.

6. The Mismatch Between National Regulations and Global Challenges

---

[51] Krisna Indrawan and M. Ruhly Kesuma Dinata, "Analisis Yuridis Tindak Pidana Perjudian Online di Indonesia dalam Putusan Nomor 244/Pid.B/2024/PN Kbu," *Arus Jurnal Sosial dan Humaniora* 5, no. 1 (2025): 683–87, https://doi.org/10.57250/ajsh.v5i1.1108.

[52] Bienvenido G. B. Hayer et al., "Pembuktian Pidana Terkait Penipuan Penjualan Produk Impor," *Indonesian Journal of Law and Justice* 2, no. 1 (2024): 15, https://doi.org/10.47134/ijlj.v2i1.3226.

[53] Christa M. Miller, "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point," *Forensic Science International: Synergy* 6 (2023): 100296, https://doi.org/10.1016/j.fsisyn.2022.100296.

Digital evidence often crosses national borders, especially in cases of transnational crime or when data is stored in *clouds* managed by foreign companies. This raises jurisdictional obstacles and inconsistencies between national laws and international practices.[54] Without strong cooperation mechanisms, the process of collecting and legalizing cross-border evidence becomes slow or impossible.

Indonesia currently lacks strong bilateral or multilateral instruments in the context *of cross-border digital evidence sharing*, unlike member states of *the Convention on Cybercrime (Budapest Convention),* which have established a joint framework for the collection and validation of cross-border digital evidence.

C. Implications for Procedural Justice

Procedural justice is a fundamental principle in the criminal justice system that ensures that every legal process is carried out fairly, transparently, and with respect for the rights of the accused.[55] This principle underpins the *due process of law*, which not only ensures that the substance of the law is upheld but also that it is enforced in a lawful and dignified manner. In the context of digital evidence, the principle of procedural justice faces unique and complex challenges due to the intangible nature of digital evidence, which is easily manipulated and prone to abuse without strict, accountable procedures.

In the Indonesian legal system, the principle of procedural justice is reflected in several legal provisions. Article 2(1) of Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP) affirms that criminal procedural mechanisms must be carried out strictly in accordance with statutory procedures. Similarly, Article 90(1) of Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP) stipulates that investigators, in

---

[54] Halefom H. Abraha, "Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives," *International Journal of Law and Information Technology* 29, no. 2 (2021): 118–53, https://doi.org/10.1093/ijlit/eaab001.

[55] Muhammad Alvian Yudistira Chandra Chaerudin et al., "Prinsip Keadilan Prosedural Sebagai Landasan Pertimbangan Hakim dalam Kasus Pencurian Ayam," *JURNAL USM LAW REVIEW* 8, no. 1 (2025): 509–29, https://doi.org/10.26623/julr.v8i1.11770.

determining a person's status as a suspect in relation to an alleged criminal offence, must base such determination on at least two pieces of valid evidence.[56]

This provision indicates that the evidence must be legally valid, and the process of obtaining it cannot disregard the procedures prescribed by law. In addition, Article 28G, paragraph (1) of the 1945 Constitution provides guarantees for the protection of the right to security and against abuse of power, including in the context of evidence collection and use.

However, in practice, the management of digital evidence often violates these principles.[57] In fact, these actions carry a high risk of violating privacy rights and the principle of non-self-incrimination, namely the right not to be compelled to testify against oneself or to be forced to confess guilt,[58] as stipulated in Article 14 paragraph (3) letter g of the International Covenant on Civil and Political Rights (ICCPR), which Indonesia has ratified through Law No. 12 of 2005.

When digital evidence is obtained without due process but still used in court, its validity may be questioned. Evidence obtained in violation of the law must be declared invalid and cannot be used as a basis for a verdict, commonly known as *the exclusionary rule.*[59] The principle of *the exclusionary rule* is commonly applied in many countries, such as the United States, as regulated in Mapp v. Ohio, 367 U.S. 643 (1961) and the Netherlands, where it is regulated in Article 359a WvSv.[60] In Indonesia,

---

[56] Nisa Amalina Adlina, "Analisis Nilai Keadilan pada Syarat Penahanan Tersangka dalam Penyidikan (Perbandingan KUHAP 1981 dan KUHAP 2025)," Al 'Adl: Jurnal Hukum 18, no. 1 (2026): 108–27, https://dx.doi.org/10.31602/al-adl.v18i1.19049.

[57] Hendro Dewanto and Setya Wahyudi, "Defamation Through Social Media as a Cyber Crime," *KnE Social Sciences*, ahead of print, February 24, 2023, https://doi.org/10.18502/kss.v8i3.12854.

[58] Lade Sirjon et al., "Perbandingan Mekanisme Pengakuan Bersalah pada Jalur Khusus dalam RUU KUHAP dan Konsep Plea Bargaining Ditinjau dari Asas Non-Self Incrimination," *Halu Oleo Law Review* 7, no. 2 (2023): 224–35, https://doi.org/10.33561/holrev.v7i2.29.

[59] Adam Ilyas, "Praktik Penerapan Exclusionary Rules di Indonesia," *Masalah-Masalah Hukum* 50, no. 1 (2021): 49–59, https://doi.org/10.14710/mmh.50.1.2021.49-59.

[60] Marfuatul Latifah, "Perlukah Mengatur Prinsip Exclusionary Rules of Evidence dalam RUU Hukum Acara Pidana? (Should We Regulate Exclusionary Rule Principle in the Criminal Procedural Bill?)," *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 1 (2021): 101–22, http://dx.doi.org/10.22212/jnh.v12i1.2123.

however, *the exclusionary rule* has not been strictly enforced because it is often considered to cause legal uncertainty and injustice.

In digital criminal cases, judges often overlook the invalidity of evidence collection procedures due to limited digital literacy. When law enforcement officials are unable to distinguish between original evidence and manipulated evidence, such as edited WhatsApp conversation screenshots, the risk of criminalization is high.[61] Defendants can be convicted based on evidence whose authenticity cannot be verified, thereby compromising the principle *of in dubio pro reo* or presumption of innocence. This condition shows that the lack of credible technical and forensic verification mechanisms for digital evidence directly implies procedural disadvantages for defendants.

Not only at the investigation and trial stages, but procedural justice can also be threatened at the pre-prosecution stage. Prosecutors, as the party authorized to determine whether a case is eligible to proceed to court, often receive case files from investigators without critically examining the completeness of the forensic aspects of digital evidence.[62] This makes prosecutors vulnerable to filing cases with weak evidence, simply because digital evidence that appears convincing visually can be legally flawed. In the long term, this practice can weaken the integrity of the judiciary and reinforce the public perception that the legal system favors power over justice.

Another concrete example can be found in several cases of violations of the Electronic Information and Transactions Law, where law enforcement was too quick to make arrests based solely on evidence posted on social media, without contextual verification or in-depth forensic analysis. In some cases, posts that have been deleted or edited by third parties are still used as evidence, even though there is no guarantee of their authenticity. This demonstrates the law's haste, which sacrifices the defendant's right to a fair and lawful legal process.

---

[61] Ismail Aghababaei Bani and Jabr Khalaf Issa Al-Maliki, "The Effects of Criminal Evidence Obtained Illegally," *Journal of Asian Multicultural Research for Social Sciences Study* 4, no. 1 (2023): 63–72, https://doi.org/10.47616/jamrsss.v4i1.371.

[62] Miller, "A Survey of Prosecutors and Investigators Using Digital Evidence."

This condition reflects a structural weakness in Indonesia's criminal evidentiary system, in which digital evidence continues to be treated analogically rather than normatively as a distinct category of evidence with its own specific characteristics. The Criminal Procedure Code (KUHAP), as the principal instrument governing criminal procedure, has not yet adequately anticipated the digital transformation of evidentiary mechanisms. As a result, law enforcement authorities tend to classify digital evidence within the conventional categories of documentary evidence or indications (circumstantial evidence) without a sufficiently robust framework for technical authentication and verification. Consequently, the standards governing the admissibility and validity of digital evidence often depend on the practical interpretation of law enforcement officials and judges rather than on uniform, objectively verifiable procedural standards. This situation has direct implications for the weakening of procedural justice guarantees, as the evidentiary process is not grounded in clear and well-defined parameters of legality.

Furthermore, challenges to procedural justice in the context of digital evidence also include an imbalance in the capacity between the defendant and the state.[63] In many cases, defendants lack the resources or expertise to challenge the validity of digital evidence presented by prosecutors. Equitable defense tools are limited, and not all lawyers have access to digital forensic experts. This creates a structural imbalance that undermines the principle *of equality of arms,*[64] namely, the equality of position between prosecutors and defenders in criminal trials.

In addition, there have been normative developments concerning the recognition of electronic evidence within Indonesia's criminal procedural law system. Previously, the recognition of electronic evidence largely relied on Article 5 of the Law on Electronic Information and Transactions (ITE Law). However, through Article 235(1)(f) of Law No. 20 of 2025, it has now been explicitly affirmed that electronic evidence constitutes one of the

---

[63] Rio Saputra et al., *Reformasi Hukum Acara Pidana: Menyongsong KUHAP Baru* (Langgam Pustaka, 2025).

[64] Sandra Gradinaru, "Compliance with the Principle of Equality of Arms with Regard to the Expertise and Findings Made during the Prosecution," *Juridica* 19, no. 3 (2023): 69–78.

legally admissible forms of evidence in criminal proceedings. This provision reflects a significant normative advancement in the national evidentiary framework, as electronic evidence is no longer positioned analogically as part of documentary evidence or indications (circumstantial evidence), but rather as an independent category of evidence in its own right. Nevertheless, this normative recognition has not yet been fully accompanied by detailed procedural regulations governing the methods of collection, preservation, authentication testing, and the standards of the chain of custody for digital evidence. As a consequence, a gap remains between normative recognition and procedural implementation in criminal justice practice, which may create opportunities for the use of digital evidence without uniform, scientifically and legally accountable forensic verification standards.

Furthermore, although Article 235(1) of Law No. 20 of 2025 has expanded the categories of admissible evidence by incorporating electronic evidence and by opening the possibility of proof through "anything that may be used for evidentiary purposes, provided that it is obtained lawfully",[65] the provision remains largely declaratory in nature and has not yet been accompanied by detailed technical regulations governing digital search and seizure mechanisms in the investigative process. In practice, law enforcement authorities continue to rely on analogical approaches derived from conventional search procedures to access electronic devices or digital accounts. This approach is problematic because electronic data differ fundamentally from physical objects: they are intangible, easily replicable, dispersed across jurisdictions, and involve significantly more complex dimensions of privacy protection. This continued reliance on analogical reasoning indicates that the recognition of electronic evidence under Article 235 has not yet been followed by a procedural design that is adaptive to the specific characteristics of digital evidence. Such conditions have the potential to generate legal uncertainty in investigative practice

[65] Bhujangga Gede Mahesa Rakanadi, "Legalitas Penyadapan Sebagai Alat Bukti dalam Sistem Peradilan Pidana Indonesia," Jurnal Media Akademik 4, no. 4 (2026): 1–27, https://doi.org/10.62281/c0nzga51.

and to increase the risk of violations of the right to privacy and the right to personal protection within criminal proceedings, thereby directly affecting the quality of the implementation of the due process of law principle in Indonesia's digital evidentiary system.

Accordingly, the issue of procedural justice in the management of digital evidence in Indonesia is not solely attributable to weaknesses in law enforcement practices, but also stems from the limitations of the normative design of criminal procedural law, which has not yet fully responded to the rapid development of information technology.[66] Therefore, a reformulation of the evidentiary legal framework is required—one that not only recognizes digital evidence as a legally admissible form of evidence but also provides detailed procedural standards governing its collection, examination, preservation, and use in criminal proceedings. Such reformulation is essential to ensure that the digital transformation of the criminal justice system proceeds in alignment with the principles of procedural justice and the protection of human rights, thereby strengthening the legitimacy and reliability of technology-based evidentiary practices in Indonesia's criminal justice process.

Thus, it can be concluded that digital evidence has serious implications for procedural justice if it is not handled in a lawful, transparent, and accountable manner. The state needs to formulate clear legal and technical standards for the procedures for collecting, verifying, and using digital evidence, and to equip all law enforcement officials with basic digital forensics competencies. Without these measures, procedural justice will become nothing more than normative jargon, unable to protect defendants' rights in a sophisticated yet manipulation-prone digital era.

---

[66] Soetardi Tri Cahyono et al., "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (*Cyber Crime*) dalam Sistem Peradilan Pidana Indonesia," Dame Journal of Law 1, no. 1 (2025): 1–23, https://doi.org/10.64344/djl.v1i1.6.

D. Comparison with International Practices in Digital Evidence Management

The development of laws governing digital evidence is not only a national issue but also a complex global challenge. Many countries with more advanced legal systems have already formulated normative and technical approaches for comprehensive, transparent, and technology-responsive digital evidence management. Comparisons with these international practices are important not only as normative references but also as benchmarks in formulating an Indonesian national legal framework that is adaptive to the challenges of the times.[67]

One of the most prominent international instruments in this regard is the Budapest Convention on Cybercrime (2001), which is the first multilateral agreement specifically regulating cybercrime and electronic evidence. This convention is globally distributed and serves as a reference in the drafting of regulations on cybercrime in various countries around the world.[68] The Council of Europe issued this convention and has now been ratified by more than 65 countries, including several non-European countries such as the United States, Japan, Australia, and Canada. Articles 14 to 21 of the convention regulate mechanisms for the collection, seizure, and access to digital evidence, including the storage of *traffic data* and electronic data backup systems.

The Budapest Convention not only serves as a normative guide but also mandates the establishment of procedural standards for member states in maintaining the integrity, authenticity, and chain of electronic evidence.[69] In this context, the convention provides a framework for obtaining valid digital evidence, such as the requirement for *lawful access*

---

[67] Carissa Amanda Siswanto et al., "Legal Recognition of Electronic Notarial Acts: A Comparative Study of Indonesia and Rwanda," *Indonesia Private Law Review* 6, no. 2 (2026), https://doi.org/10.25041/iplr.v6i2.4686.

[68] Chat Le Nguyen and Wilfred Golman, "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action,'" *Computer Law & Security Review* 40 (April 2021): 105521, https://doi.org/10.1016/j.clsr.2020.105521.

[69] Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia* (Sada Kurnia Pustaka, 2025).

through a court warrant and the principle *of data preservation,* which is a data storage mechanism to ensure that evidence is not damaged before it is evaluated in court. This provision is highly relevant to countries such as Indonesia, which currently lack national standards for the retention and maintenance of digital data as evidence. In fact, in 2009, Indonesia had prepared a Draft Law on the Ratification of the 2001 Budapest EU Convention on Cybercrime. Still, it failed because the substantive provisions of the convention were not relevant to Indonesian national law, particularly regarding *cyberporn,* even though cyberporn is rampant today and tends to cause public concern.[70]

In the United States, the approach to digital evidence is more structured through the Federal Rules of Evidence (FRE) and the Electronic Communications Privacy Act (ECPA) of 1986.[71] The ECPA provides legal protection for electronic communications and sets out the procedures for the seizure and processing of digital information. Section 2703 of the ECPA, for example, states that law enforcement may access email or other communication data only with a court order, demonstrating a commitment to the principles of *privacy protection* and *due process.* On the other hand, the FRE stipulates that all evidence, including digital evidence, must be authenticated using scientifically accepted methods, such as verification through *digital hash values.*[72]

Practices in the United Kingdom also show a high level of concern for the integrity of digital evidence under the Police and Criminal Evidence Act (PACE) 1984, particularly in Codes B and D, which contain provisions on the seizure and processing of digital devices.[73] All data

---

[70] George Zlati, "Romanian Jurisprudence on Cybercrime: Focus on Illegal Access to an Information System," *ERA Forum* 25, no. 3 (2024): 425–40, https://doi.org/10.1007/s12027-024-00810-y.

[71] Sasha K. Danna, "V. The Impact of Electronic Discovery on Privilege and the Applicability of the Electronic Communications Privacy Act," *Law Review* 38, no. 4 (2005), https://digitalcommons.lmu.edu/llr/vol38/iss4/5/.

[72] Olgun DeğiRmenci, "The Concept of Hash Value and The Collision of Hash Value As The Way To Provide Unassailability Of Digital Evidence," Adalet Dergisi, no. 69 (December 2022): 45–62, https://doi.org/10.57083/adaletdergisi.1217741.

[73] Geoff Coliandris, "Book Review: Zander on PACE: The Police and Criminal Evidence Act 1984, 6th Edition," *The Police Journal: Theory, Practice and Principles* 87, no. 2 (2014): 139–41, https://doi.org/10.1350/pojo.2014.87.2.671.

collected from computers or digital devices must be stored in its original form (*original image copy)* and examined only through a copy (*mirror image*) to avoid damage or unauthorized changes. The UK also requires digital forensic training for police officers and provides standard protocols for all electronic investigations.[74]

Germany, as a country with a continental legal system like Indonesia, emphasizes the *proportionality principle* in digital evidence.[75] In practice, the German Federal Constitutional Court (*Bundesverfassungsgericht),* through several landmark decisions, such as *BVerfGE 120, 274* (2008), stated that the collection of digital evidence that touches on the private sphere must meet the principle of *urgent necessity* and must not violate the right to privacy of personal communications guaranteed in *the Grundgesetz.*[76] This shows that in the European legal system, the protection of human rights is the foundation of every digital evidence management policy.[77]

At the international organizational level, the European Union Agency for Cybersecurity (ENISA) has released Digital Evidence Guidelines that serve as technical guidelines for European Union member states in handling digital evidence.[78] These guidelines emphasize the importance of *chain-of-custody documentation,* the use of certified forensic software, and the principles *of repeatability* and *verifiability* in every digital evidence

---

[74] Dana Wilson-Kovacs, "Digital Media Investigators: Challenges and Opportunities in the Use of Digital Forensics in Police Investigations in England and Wales," *Policing: An International Journal* 44, no. 4 (2021): 669–82, https://doi.org/10.1108/PIJPSM-02-2021-0019.

[75] Pascal Berger, "Proportionality, Evidence and the COVID-19-Jurisprudence in Germany," *European Journal for Security Research* 7, no. 2 (2022): 211–36, https://doi.org/10.1007/s41125-022-00087-7.

[76] Nikolaus Forgó et al., "The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings," in *New Technology, Big Data and the Law*, ed. Marcelo Corrales et al., Perspectives in Law, Business and Innovation (Springer Singapore, 2017), https://doi.org/10.1007/978-981-10-5038-1_10.

[77] Sandra Seubert and Carlos Becker, "The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection," *German Law Journal* 22, no. 1 (2021): 31–44, https://doi.org/10.1017/glj.2020.101.

[78] Melania Tudorica and Jeanne Mifsud Bonnici, "Legal Framework for Digital Evidence Following the Implementation of the EIO Directive: Status Quo, Challenges and Experiences in Member States," in *European Investigation Order*, vol. 55, ed. Maria Angela Biasiotti and Fabrizio Turchi, Law, Governance and Technology Series (Springer International Publishing, 2023), https://doi.org/10.1007/978-3-031-31686-9_9.

handling process. The purpose of this approach is to ensure that all evidence presented in court is scientifically and legally accountable.

When compared with those jurisdictions, Indonesia still lacks a comprehensive procedural framework that explicitly regulates the admissibility, authentication, preservation, and institutional governance of digital evidence within the criminal justice system. While international instruments such as the *Budapest Convention on Cybercrime* have provided procedural standards concerning lawful access and data preservation, and countries such as the United States, the United Kingdom, and Germany have developed detailed evidentiary rules supported by robust privacy safeguards and forensic verification mechanisms, Indonesia's criminal procedural law continues to position digital evidence only partially within the framework of conventional evidentiary categories, which do not yet fully accommodate the distinctive characteristics of electronic evidence.

The absence of explicit regulation in Indonesia's criminal procedural law has led to the practice of managing digital evidence remaining highly dependent on the interpretation of law enforcement authorities and case-by-case judicial practices. In contrast, the United States has established scientific authentication standards through the *Federal Rules of Evidence*; the United Kingdom has developed digital forensic procedures based on mirror imaging techniques supported by a systematic chain of custody; and Germany places the principle of proportionality as a constitutional limitation on access to private data. Indonesia, however, to date has not yet developed a national procedural standard that systematically integrates the dimensions of legality, technical integrity, and human rights protection within a unified framework for digital evidence governance.

Furthermore, compared with European Union member states, which have developed technical guidance through the ENISA Digital Evidence Guidelines, Indonesia still faces significant limitations in standardizing digital forensic software, electronic evidence management and audit systems, and nationally verified chains-of-custody documentation. These conditions have important implications for the potential vulnerability to evidence manipulation, the lack of uniformity in investigative practices,

and the weakened evidentiary position of digital evidence in safeguarding the principle of due process of law within criminal proceedings. Consequently, strengthening technical and procedural standardization remains essential to ensure that digital evidence serves as a reliable and legally robust component of Indonesia's contemporary criminal justice system.

Looking at international practices, there are several important lessons that Indonesia can adopt. First, there is a need for reform of criminal procedure law that explicitly recognizes and regulates the category of digital evidence, along with the procedures and standards for its use as evidence. Second, it is important to strengthen digital forensics capacity through training for law enforcement and judicial officials. Third, it is necessary to establish independent oversight and audit mechanisms for the collection and processing of digital evidence to maintain accountability. Fourth, Indonesia should consider ratifying the Budapest Convention to facilitate international cooperation in the management of cross-border digital evidence.

From this comparative analysis, it is clear that international practices have provided a more progressive and balanced framework between law enforcement and human rights protection. Indonesia needs to respond immediately to this gap so that the national criminal justice system does not fall behind and remains relevant in the era of global digital transformation.

E. Proposed Conceptual Framework for Digital Evidence Management in the Criminal Justice System

In the face of the inevitable wave of digitalization, the criminal justice system must adapt not only technologically but also normatively.[79] Digital evidence has become a major component in various criminal cases, ranging from cybercrime to conventional crimes whose traces are recorded electronically. However, the complexity of digital evidence requires a

[79] Tri Cahyono et al., "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (*Cyber Crime*) dalam Sistem Peradilan Pidana Indonesia."

framework that can guarantee integrity, validity, and procedural justice throughout the entire judicial process. Therefore, it is necessary to formulate a conceptual framework for digital evidence management that is systemic and adaptive, capable of responding to technological dynamics while upholding human rights principles.[80]

This study makes a major scientific contribution in the form of a five-pillar framework for the management of digital evidence in the criminal justice system, encompassing (1) legality and legal certainty, (2) integrity and verification, (3) fair procedures, (4) legal digital literacy, and (5) institutional accountability. This framework constitutes the article's primary theoretical contribution, as it transcends the previously fragmented approach between normative regulations and technical digital forensic practices by integrating doctrinal legality, forensic validation mechanisms, guarantees of fair procedures, capacity building for law enforcement professionals, and institutional oversight systems into a unified governance structure.

The first pillar is *legality and legal certainty*. In this context, it is necessary to revise the criminal procedure law to recognize digital evidence as a valid category of evidence explicitly.[81] Until now, due to the lack of normative recognition, digital evidence has often been forced into the category of letters or clues, even though its characteristics are very different. Therefore, the legal framework must establish the definition, limitations, and valid forms of digital evidence, complete with substantial and procedural requirements for its validity in court.

Second, *integrity and verification* form the technical foundation of digital evidence management. Digital data is highly vulnerable to

---

[80] Zul Khaidir Kadir, "Meruntuhkan Pilar Keadilan: Apakah Sistem Peradilan Dapat Berfungsi Tanpa Standar Pembuktian?," *Mandub : Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 40–61, https://doi.org/10.59059/mandub.v3i2.2351.

[81] Rafly Maulana Akbar Akbar and Hudi Yusuf, "Problematika Pembuktian Alat Bukti Digital dalam Hukum Acara Pidana di Indonesia: Analisis Teori Pembuktian dan Praktik Peradilan," *Jurnal Intelek Dan Cendikiawan Nusantara* 2, no. 5 (2025): 9445–53.

manipulation, both technically and administratively.[82] Therefore, technology-based verification mechanisms, such as hash values, authentic timestamps, and digital audit systems, must be standard procedures in every stage of seizure, storage, and presentation of digital evidence.[83] In addition, only standardized and certified forensic software may be used in investigations. This is to ensure that the integrity of the evidence can be tested scientifically and objectively.

The third pillar is *fair procedures* or procedural justice. This includes fulfilling the defendant's right to know how evidence was collected, to have access to refute the evidence, and to ensure that the collection process does not violate the rights to privacy and individual freedom.[84] Digital search and seizure procedures must always be carried out pursuant to a valid court order, with restrictions on the scope and duration of access. In this context, *digital search and seizure* needs to be understood as a highly sensitive legal action that cannot be carried out arbitrarily.

The fourth pillar is *legal digital literacy*, which is the ability of law enforcement officials, prosecutors, judges, and lawyers to understand the technical and legal aspects of digital evidence.[85] Without this capacity, the evidence process will be flawed, as key actors in the legal system will be unable to evaluate or question the validity of evidence. Therefore, specialized training and certification in legal digital forensics need to be made an integral part of legal professional education.

The fifth pillar, which is no less important, is *institutional accountability*. The process of managing digital evidence must be traceable

---

[82] Randiha Divaresky and Hudi Yusuf, "Efektivitas Penggunaan Bukti Elektronik dalam Pembuktian Perkara Pidana di Pengadilan Negeri," *Jurnal Intelek Dan Cendikiawan Nusantara* 2, no. 5 (2025): 9555–68.

[83] Devi Ratnasari, "Membangun Model Informasi Metadata untuk Mendukung Chain of Custody Bukti Digital" (Thesis, Universitas Islam Indonesia, 2018), https://dspace.uii.ac.id/handle/123456789/7590.

[84] Rohman et al., "Sistem Pembuktian dalam Hukum Pidana Indonesia dan Tantangan dalam Proses Peradilan."

[85] Jannati and Ruhly Kesuma Dinata, "Pengaruh Teknologi Terhadap Perkembangan Hukum di Indonesia," *Arus Jurnal Sosial Dan Humaniora* 5, no. 1 (2025): 630–35, https://doi.org/10.57250/ajsh.v5i1.1093.

and auditable.[86] Every stage, from data collection to use in court, must be recorded in a system that allows for public and institutional oversight. This can be achieved through the establishment of an independent institution or the adoption of a technology-based monitoring system, such as *a blockchain evidence management system* that can store activity logs transparently and cannot be altered. To ensure that this framework is not merely theoretical, let us look at two concrete examples of its application:

The first example is in cases of defamation through social media, where evidence in the form of screenshots is often used as the main evidence. In a system without a strong conceptual framework, such evidence is immediately used as the basis for prosecution without integrity testing. However, in the proposed framework, screenshots must be accompanied by original metadata, verified with a hash, and confirmed through forensic software. Evidence cannot be accepted based on its visual appearance alone, but must pass technical authentication tests.

The second example is a case of digital transaction fraud, where the conversation history between the perpetrator and the victim in a chat application is an important element. In current practice, often only one side of the conversation is displayed, with no guarantee that the content has not been edited. Within this conceptual framework, investigators must legally seize devices, make complete forensic copies, and present the entire context of the conversation from both parties with scientifically testable verification. On the other hand, the defendant is also entitled to present a counter-forensic expert to refute or corroborate the evidence.

Through this integrative model, this study develops a legal framework responsive to technological advancements that not only strengthens the reliability and admissibility of digital evidence but also reinforces the protection of due process of law and transparency in the management of digital evidence. Thus, this framework can serve as a systematic reference for the criminal procedure reform agenda, the strengthening of judicial

[86] Jefrul Hanafi, "Interplanetary File System pada Digital Evidence Cabinet Berbasis Hyperledger Fabric untuk Manajemen Bukti Digital" (Universitas Islam Indonesia, 2022), https://dspace.uii.ac.id/handle/123456789/38846.

practices, and the development of interdisciplinary research in the field of digital evidence governance within a criminal justice system undergoing rapid digital transformation.

In addition, by applying these five pillars in the framework of digital evidence governance, the criminal justice system will be better prepared to face the complexities of the digital age. Not only does it emphasize technical accuracy, but it also guarantees the protection of human rights and upholds the principle of justice. Indonesia, as a country with a large digital population, can no longer delay the formulation of an evidence system that is responsive to technology.

Conclusion

This study demonstrates that the absence of a structured and procedurally integrated digital evidence governance framework within Indonesia's criminal procedural law has directly weakened the guarantees of procedural justice and the protection of defendants' rights in the digital era. Although recent regulatory developments have begun to recognize electronic evidence as a legally admissible form of evidence within the criminal evidentiary system, the regulatory framework has not yet been supplemented with detailed procedural standards governing the authentication, acquisition, preservation, and evaluation of digital evidence. As a consequence, in criminal justice practice, digital evidence continues to be treated analogically within conventional evidentiary mechanisms rather than through a normative structure specifically designed to accommodate its technological characteristics. This study further indicates that the challenges surrounding the management of digital evidence in Indonesia are not only the result of regulatory fragmentation but also stem from limitations in institutional capacity and the absence of national standardization in digital forensic verification. When compared with international practices—such as the framework established under the *Budapest Convention on Cybercrime*, the *Electronic Communications Privacy Act* in the United States, and the *PACE Code of*

Practice in the United Kingdom and Indonesia still lacks a comprehensive procedural architecture that integrates the dimensions of legality, forensic reliability standards, privacy protection, and institutional accountability mechanisms in the governance of digital evidence.

As a scientific novelty, this study proposes a five-pillar conceptual framework consisting of legality and legal certainty, evidentiary integrity and verification, procedural justice, legal digital literacy, and institutional accountability. This framework provides a systematic model for the governance of digital evidence that is responsive to technological developments by bridging the gap between the normative recognition of digital evidence and its procedural implementation in criminal justice practice. Through the integration of criminal procedural law reform, digital forensic validation principles, the strengthening of law enforcement personnel's professional capacity, and transparent institutional oversight mechanisms, the framework offers a conceptual reference for reinforcing digital evidentiary systems within criminal justice institutions undergoing digital transformation.

Based on these findings, this study proposes several concrete strategic recommendations. First, reform of criminal procedural law is required to regulate digital search and seizure mechanisms explicitly, standards for the authentication of electronic evidence, and chain of custody procedures in the management of digital evidence. Second, the development of national digital forensic standards is necessary to provide authoritative guidelines that ensure the reliability and admissibility of digital evidence at every stage of criminal proceedings. Third, systematic training and certification programs in digital forensic literacy should be implemented for investigators, prosecutors, judges, and defense counsel to strengthen institutional capacity in evaluating digital evidence. Fourth, establishing independent and transparent oversight mechanisms is essential to ensure accountability at each stage of digital evidence management. Through these measures, the criminal justice system in Indonesia is expected to move toward a more equitable, reliable, and technology-responsive

evidentiary system, while continuing to safeguard the principles of due process of law and the protection of human rights in the digital era.

References

Abraha, Halefom H. "Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives." *International Journal of Law and Information Technology* 29, no. 2 (2021): 118–53. https://doi.org/10.1093/ijlit/eaab001.

Adlina, Nisa Amalina. "Analisis Nilai Keadilan pada Syarat Penahanan Tersangka dalam Penyidikan (Perbandingan KUHAP 1981 dan KUHAP 2025)." *Al 'Adl: Jurnal Hukum* 18, no. 1 (2026): 108–27. https://dx.doi.org/10.31602/al-adl.v18i1.19049.

Akbar, Rafly Maulana Akbar, and Hudi Yusuf. "Problematika Pembuktian Alat Bukti Digital Dalam Hukum Acara Pidana Di Indonesia: Analisis Teori Pembuktian Dan Praktik Peradilan." *Jurnal Intelek Dan Cendikiawan Nusantara* 2, no. 5 (2025): 9445–53.

Alanazi, Fahad, and Andrew Jones. "The Value of Metadata in Digital Forensics." *2015 European Intelligence and Security Informatics Conference*, September 2015, 182–182. https://doi.org/10.1109/EISIC.2015.26.

Alsmirat, Mohammad A., Ruba A. Al Hussien, N. A. Wala', A. T. Al Sarayrah, Yaser Jararweh, and Morad Etier. "Digital Video Forensics: A Comprehensive Survey." *International Journal of Advanced Intelligence Paradigms* 15, no. 4 (2020): 437. https://doi.org/10.1504/IJAIP.2020.106040.

Army, H. Eddy. *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika, 2020.

Arshad, Humaira, Aman Bin Jantan, and Oludare Isaac Abiodun. "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence." *Journal of Information Processing Systems* 14, no. 2 (2018): 346–76. https://doi.org/10.3745/JIPS.03.0095.

Bagaskara, Riziqi Abista, and Catur Suratnoaji. "Representasi Kepemimpinan Transformasional Anies Baswedan Sebagai Calon Presiden 2024 Di Media Sosial Instagram @aniesbaswedan (Studi

Analisis Semiotika Roland Barthes Kepemimpinan Transformasional Anies Baswedan Sebagai Calon Presiden 2024 Di Media Sosial Instagram @aniesbaswedan)." *JIIP - Jurnal Ilmiah Ilmu Pendidikan* 7, no. 10 (2024): 11785–92. https://doi.org/10.54371/jiip.v7i10.6132.

Bani, Ismail Aghababaei, and Jabr Khalaf Issa Al-Maliki. "The Effects of Criminal Evidence Obtained Illegally." *Journal of Asian Multicultural Research for Social Sciences Study* 4, no. 1 (2023): 63–72. https://doi.org/10.47616/jamrsss.v4i1.371.

Berger, Pascal. "Proportionality, Evidence and the COVID-19-Jurisprudence in Germany." *European Journal for Security Research* 7, no. 2 (2022): 211–36. https://doi.org/10.1007/s41125-022-00087-7.

Bianchi De Oliveira, Diego, and Rogério Mollica. "A Função Do Amicus Curiae Como Mecanismo De Acesso À Justiça Nas Demandas Judiciais Envolvendo Novas Tecnologias." *Revista Eletrônica de Direito Processual* 25, no. 1 (2024). https://doi.org/10.12957/redp.2024.81888.

Brems, Eva, and Laurens Lavrysen. "Procedural Justice in Human Rights Adjudication: The European Court of Human Rights." *Human Rights Quarterly* 35, no. 1 (2013): 176–200. https://doi.org/10.1353/hrq.2013.0000.

Budiyanto. *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Sada Kurnia Pustaka, 2025.

Casey, Eoghan. "Reconstructing Digital Evidence." In *Crime Reconstruction*. Elsevier, 2011. https://doi.org/10.1016/B978-0-12-386460-4.00017-5.

Chaikin, David. "Network Investigations of Cyber Attacks: The Limits of Digital Evidence." *Crime, Law and Social Change* 46, nos. 4–5 (2006): 239–56. https://doi.org/10.1007/s10611-007-9058-4.

Chopade, Mrunali, Sana Khan, Uzma Shaikh, and Renuka Pawar. "Digital Forensics: Maintaining Chain of Custody Using Blockchain." *2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, December 2019, 744–47. https://doi.org/10.1109/I-SMAC47947.2019.9032693.

Colaiocco, Andrea. "The Relevance of Best Practices in the Acquisition of Digital Evidence in Light of the News on Judiciary Cooperation." *Archivio Penale* 71, no. 1 (2019).

Coliandris, Geoff. "Book Review: Zander on PACE: The Police and Criminal Evidence Act 1984, 6th Edition." *The Police Journal: Theory, Practice and Principles* 87, no. 2 (2014): 139–41. https://doi.org/10.1350/pojo.2014.87.2.671.

Czarnecka, Agota. "New Questions, Old Problems. Philosophy of Law and Contemporary Challenges." *Prawo i Wiez* 2019, no. 29 (2019): 57–69.

Dalimunthe, Aidil Putra. "Legality Of The Practice Of Wiretapping Methods Against Perpetrators Of Criminal Acts Of Corruption In The Provisions Of The Law On Criminal Acts Of Corruption." *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam* 5, no. 2 (2024): 80. https://doi.org/10.58836/al-qanun.v5i2.21762.

Danna, Sasha K. "V. The Impact of Electronic Discovery on Privilege and the Applicability of the Electronic Communications Privacy Act." *Law Review* 38, no. 4 (2005). https://digitalcommons.lmu.edu/llr/vol38/iss4/5/.

DeğīRmencī, Olgun. "The Concept of Hash Value and the Collision of Hash Value As the Way to Provide Unassailability of Digital Evidence." *Adalet Dergisi*, no. 69 (December 2022): 45–62. https://doi.org/10.57083/adaletdergisi.1217741.

Dehling, Florian, Tobias Mengel, and Luigi Lo Iacono. "Rotten Cellar: Security and Privacy of the Browser Cache Revisited." In *Secure IT Systems*, vol. 11875, edited by Aslan Askarov, René Rydhof Hansen, and Willard Rafnsson. Lecture Notes in Computer Science. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-35055-0_2.

Dewanto, Hendro, and Setya Wahyudi. "Defamation Through Social Media as a Cyber Crime." *KnE Social Sciences*, ahead of print, February 24, 2023. https://doi.org/10.18502/kss.v8i3.12854.

Divaresky, Randiha, and Hudi Yusuf. "Efektivitas Penggunaan Bukti Elektronik Dalam Pembuktian Perkara Pidana Di Pengadilan Negeri." *Jurnal Intelek Dan Cendikiawan Nusantara* 2, no. 5 (2025): 9555–68.

Dwitarani, Dealita. "Kesesuaian Pembuktian Penuntut Umum dalam Tindak Pidana Penyertaan Disertai Kelalaian yang Menyebabkan Kematian dengan Pasal 184 Ayat (1) KUHAP (Studi Putusan No. 19/Pid.B/2021/Pn.Trk)." *Verstek* 10, no. 2 (2022): 336–43. https://doi.org/10.20961/jv.v10i2.67638.

Evan, Gladys Lydia, and Moody Syailendra. "Keabsahan Tanda Tangan Elektronik Melalui Platform DocuSign Ditinjau dari Hukum Positif di Indonesia." *UNES Law Review* 6, no. 2 (2023): 6512–20. https://doi.org/10.31933/unesrev.v6i2.1513.

Forgó, Nikolaus, Christian Hawellek, Friederike Knoke, and Jonathan Stoklas. "The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings." In *New Technology, Big Data and the Law*, edited by Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó. Perspectives in Law, Business and Innovation. Springer Singapore, 2017. https://doi.org/10.1007/978-981-10-5038-1_10.

Gradinaru, Sandra. "Compliance with the Principle of Equality of Arms with Regard to the Expertise and Findings Made during the Prosecution." *Juridica* 19, no. 3 (2023): 69–78.

Hamzani, Achmad Irwan, Tiyas Vika Widyastuti, Nur Khasanah, and Mohd Hazmi Mohd Rusli. "Implementation Approach in Legal Research." *International Journal of Advances in Applied Sciences* 13, no. 2 (2024): 380. https://doi.org/10.11591/ijaas.v13.i2.pp380-388.

Han, Jaehyeok, Mee Lan Han, Sangjin Lee, and Jungheum Park. "ECo-Bag: An Elastic Container Based on Merkle Tree as a Universal Digital Evidence Bag." *Forensic Science International: Digital Investigation* 49 (June 2024): 301725. https://doi.org/10.1016/j.fsidi.2024.301725.

Hanafi, Jefrul. "Interplanetary File System pada Digital Evidence Cabinet Berbasis Hyperledger Fabric untuk Manajemen Bukti Digital." Universitas Islam Indonesia, 2022. https://dspace.uii.ac.id/handle/123456789/38846.

Hardiago, David, Rani Fadhila Syafrinaldi, Syafrinaldi Syafrinaldi, M. Musa, and Kim Hyeonsoo. "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law." *IJCLS (Indonesian*

Journal of Criminal Law Studies) 10, no. 1 (2025). https://doi.org/10.15294/ijcls.v10i1.22557.

Hasanudin, Hasanudin, Soerya Respationo, Erniyanti Erniyanti, Bachtiar Simatupang, and Ramon Nofrial. "Juridical Analysis of the Use of Information/Electronic Documents as Evidence in Criminal Law Enforcement (Case Study Decision Number: 192/Pid.B/2023/PN Btm)." *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 3, no. 1 (2024): 118–27. https://doi.org/10.57235/aurelia.v3i1.1387.

Hayer, Bienvenido G. B., Ni Kadek Lely Kamani, Naily Aridah, et al. "Pembuktian Pidana Terkait Penipuan Penjualan Produk Impor." *Indonesian Journal of Law and Justice* 2, no. 1 (2024): 15. https://doi.org/10.47134/ijlj.v2i1.3226.

Hsu, Chien-Lung, Wei-Qian Lin, and Sheng-Hsin Tso. "Secure Handwritten Protocol for Protecting Integrity of Digital Evidences." *2024 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, December 10, 2024, 1–4. https://doi.org/10.1109/ISPACS62486.2024.10869225.

Humam Makmun, Muhammad. "Transformasi Sistem Pembuktian di Pengadilan: Antara Tradisi dan Modernisasi Digital." *YUDHISTIRA : Jurnal Yurisprudensi, Hukum dan Peradilan* 1, no. 2 (2023): 36–43. https://doi.org/10.59966/yudhistira.v1i2.1694.

Ilyas, Adam. "Praktik Penerapan Exclusionary Rules di Indonesia." *Masalah-Masalah Hukum* 50, no. 1 (2021): 49–59. https://doi.org/10.14710/mmh.50.1.2021.49-59.

Indrawan, Krisna, and M. Ruhly Kesuma Dinata. "Analisis Yuridis Tindak Pidana Perjudian Online di Indonesia dalam Putusan Nomor 244/Pid.B/2024/PN Kbu." *Arus Jurnal Sosial Dan Humaniora* 5, no. 1 (2025): 683–87. https://doi.org/10.57250/ajsh.v5i1.1108.

Jannati, and Ruhly Kesuma Dinata. "Pengaruh Teknologi Terhadap Perkembangan Hukum di Indonesia." *Arus Jurnal Sosial dan Humaniora* 5, no. 1 (2025): 630–35. https://doi.org/10.57250/ajsh.v5i1.1093.

Johnson, James, Jeremy Daily, and Andrew Kongs. "On the Digital Forensics of Heavy Truck Electronic Control Modules." *SAE*

International Journal of Commercial Vehicles 7, no. 1 (2014): 72–88. https://doi.org/10.4271/2014-01-0495.

Jokubauskas, Remigijus, and Marek Świerczyński. "Is Revision of the Council of Europe Guidelines on Electronic Evidence Already Needed?" *Utrecht Law Review* 16, no. 1 (2020): 13–20. https://doi.org/10.36633/ulr.525.

Kadir, Zul Khaidir. "Meruntuhkan Pilar Keadilan: Apakah Sistem Peradilan Dapat Berfungsi Tanpa Standar Pembuktian?" *Mandub : Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 40–61. https://doi.org/10.59059/mandub.v3i2.2351.

Kerr, Orin. *The Digital Fourth Amendment: Privacy and Policing in Our Online World*. 1st ed. Oxford University PressNew York, NY, 2025. https://doi.org/10.1093/9780190627102.001.0001.

Lasaka, Mustalim. "Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law." *Jurnal Legalitas* 16, no. 2 (2023): 154–66. https://doi.org/10.33756/jelta.v16i2.20306.

Latifah, Marfuatul. "Perlukah Mengatur Prinsip Exclusionary Rules of Evidence Dalam RUU Hukum Acara Pidana? (Should We Regulate Exclusionary Rule Principle in the Criminal Procedural Bill?)." *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 1 (2021): 101–22. http://dx.doi.org/10.22212/jnh.v12i1.2123.

Lee, Joon-Taik, Hyoung Kee Choi, and Kwang-Jong Kim. "Gathering and Storage Technique Implementation of Volatility Memory Data for Real-Forensic." *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, 2009, 1076–79. https://doi.org/10.1109/ICCIT.2009.234.

Lv, Yan Li, Yuan Long Li, Shuang Xiang, and Chun He Xia. "The Research and Realization of a Kind of Log Management-Oriented Descriptive Language to Describe the Security of Computer Network." *Applied Mechanics and Materials* 556–562 (May 2014): 5765–70. https://doi.org/10.4028/www.scientific.net/AMM.556-562.5765.

Maxwell, Virginia M. "Digital Evidence." In *Investigating Animal Abuse Crime Scenes*, 1st ed., by Virginia M. Maxwell and Martha Smith-Blackmore. CRC Press, 2023. https://doi.org/10.4324/9781003090762-15.

Miller, Christa M. "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point." *Forensic Science International: Synergy* 6 (2023): 100296. https://doi.org/10.1016/j.fsisyn.2022.100296.

Mualfah, Desti, and Rizdqi Akbar Ramadhan. "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital." *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi* 11, no. 2 (2020): 257–67. https://doi.org/10.31849/digitalzone.v11i2.5174.

Muhammad Alvian Yudistira Chandra Chaerudin, Ali Maskur, and Arina Hukmu Adila. "Prinsip Keadilan Prosedural Sebagai Landasan Pertimbangan Hakim Dalam Kasus Pencurian Ayam." *JURNAL USM LAW REVIEW* 8, no. 1 (2025): 509–29. https://doi.org/10.26623/julr.v8i1.11770.

Muni, Abdul. *Kriptografi Untuk Keamanan Sistem Informasi*. Penerbit KBM Indonesia, 2024.

Mylonas, Alexios, Vasilis Meletiadis, Lilian Mitrou, and Dimitris Gritzalis. "Smartphone Sensor Data as Digital Evidence." *Computers & Security* 38 (October 2013): 51–75. https://doi.org/10.1016/j.cose.2013.03.007.

Nguyen, Dr. Chat Le, and Dr. Wilfred Golman. "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action.'" *Computer Law & Security Review* 40 (April 2021): 105521. https://doi.org/10.1016/j.clsr.2020.105521.

Pakarti, Moch Bagoes. "Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Laboratorium Forensika Digital." Universitas Islam Indonesia, 2020. https://dspace.uii.ac.id/handle/123456789/28258.

Paluttri, Sukri. "Comparative Approach in Public Health Social Security: A Legal Case Study of the Indonesian, France, and Singapore Health Systems." *International Journal of Human Rights in Healthcare* 17, no. 5 (2024): 572–87. https://doi.org/10.1108/IJHRH-03-2023-0020.

Pandit, Kanika, and Renu Mahajan. "Cloud and AI Fusion: Revolutionizing Electronic Evidence Admissibility in the Digital Age." *2024 16th International Conference on Electronics, Computers*

and Artificial Intelligence (ECAI), June 27, 2024, 1–5. https://doi.org/10.1109/ECAI61503.2024.10607551.

Pollitt, Mark. "The Key to Forensic Success: Examination Planning Is a Key Determinant of Efficient and Effective Digital Forensics." In *Digital Forensics*. Elsevier, 2016. https://doi.org/10.1016/B978-0-12-804526-8.00002-2.

Rakanadi, Bhujangga Gede Mahesa. "Legalitas Penyadapan Sebagai Alat Bukti Dalam Sistem Peradilan Pidana Indonesia." *Jurnal Media Akademik* 4, no. 4 (2026): 1–27. https://doi.org/10.62281/c0nzga51.

Rangkuti, Fauzi Maulana, Nurcahyo Budi Nugroho, and Zaimah Panjaitan. "Implementasi Digital Signature Pada E-Invoice Di Uniqa Digital Invitation Menggunakan Algoritma SHA-256 (Secure Hash Algorithm-256) Dan RSA (Rivest Shamir Adleman)." *Jurnal Cyber Tech* 2, no. 7 (2019): 1–14. https://doi.org/10.53513/jct.v2i7.2841.

Rani, Rajneesh, Akshay Kumar, and Amrita Rai. "A Brief Review on Existing Techniques for Detecting Digital Image Forgery." *2021 Sixth International Conference on Image Information Processing (ICIIP)*, November 26, 2021, 533–38. https://doi.org/10.1109/ICIIP53038.2021.9702688.

Rasiwan, Iwan. *Pengantar Hukum Forensik Indonesia*. Takaza Innovatix Labs, 2025.

Ratnasari, Devi. "Membangun Model Informasi Metadata Untuk Mendukung Chain of Custody Bukti Digital." Thesis, Universitas Islam Indonesia, 2018. https://dspace.uii.ac.id/handle/123456789/7590.

Rohman, Rohman, Muliadi Muliadi, Farhan Pratama, et al. "Sistem Pembuktian dalam Hukum Pidana Indonesia dan Tantangan dalam Proses Peradilan." *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin* 1, no. 3 (2024): 279–92. https://doi.org/10.71153/jimmi.v1i3.146.

Rohmy, Atikah Mardhiya, Teguh Suratman, and Arini Indah Nihayaty. "UU ITE Dalam Perspektif Perkembangan Teknologi Informasi Dan Komunikasi." *Dakwatuna: Jurnal Dakwah Dan Komunikasi Islam* 7, no. 2 (2021): 309. https://doi.org/10.54471/dakwatuna.v7i2.1202.

Rovida, Khofidhotur, and Sasmini Sasmini. "Evaluasi Sistem Hukum Indonesia dalam Menangani Cyberbullying Berbasis Teknologi

Informasi dan Komunikasi." *DIVERSI : Jurnal Hukum* 10, no. 1 (2024): 169. https://doi.org/10.32503/diversi.v10i1.5223.

Rudiyanto, Tri, Halley Kunda, Amy Dunn, Sharon Shenderovskiy, and Rondarrius Gibson. "Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States." *Lex Publica* 10, no. 1 (2023): 84–100. https://doi.org/10.58829/lp.10.1.2023.84-100.

Rum, Gresia Wulaning. "Penggunaan Alat Bukti Elektronik dalam Proses Peradilan Perdata." *Jurnal Multidisiplin Ilmu Akademik (JMIA)* 2, no. 1 (2025): 61–68. https://doi.org/10.61722/jmia.v2i1.3151.

S, Ezhilmathi, and Selvakumara Samy S. "Identifying Illicit Transactions in Bitcoin Tumbler Services Using Supervised Machine Learning Algorithms." *2023 12th International Conference on Advanced Computing (ICoAC)*, August 17, 2023, 1–8. https://doi.org/10.1109/ICoAC59537.2023.10249782.

Saputra, Dadang Herli, and Fardana Kusuma. "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries." *IJCLS (Indonesian Journal of Criminal Law Studies)* 10, no. 2 (2025). https://doi.org/10.15294/ijcls.v10i2.28795.

Saputra, Rio, Lufsiana, and Dharma Setiawan Negara. *Reformasi Hukum Acara Pidana: Menyongsong KUHAP Baru*. Langgam Pustaka, 2025.

Sardo, Alessio, and Allegra Grillo. "Mapping Legal Consciousness in Comparative Law: An Essay on Methodology." In *Legal Consciousness*, vol. 142, edited by Jakob V. H. Holtermann, Mario Krešić, and Marko Novak. Law and Philosophy Library. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-87962-3_6.

Setiawan, Iwan, Ibnu Rusydi, Anisa Rahmawati, and Siti Hasanah. "Jejak Digital Sebagai Alat Bukti Petunjuk Menurut Pasal 184 Kitab Undang-Undang Hukum Acara Pidana." *Jurnal Ilmiah Galuh Justisi* 10, no. 1 (2022): 119–32. https://doi.org/10.25157/justisi.v10i1.7236.

Seubert, Sandra, and Carlos Becker. "The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The

Example of Privacy Protection." *German Law Journal* 22, no. 1 (2021): 31–44. https://doi.org/10.1017/glj.2020.101.

Shilling, C. G. "Electronic Discovery: Litigation Crashes into the Digital Age." *The Labor Lawyer* 22, no. 2 (2006): 207–32.

Sinani, Blerton, and Mehmeti Sami. "The Importance of Comparative Law for the Development of Contemporary Law." *Juridical Tribune - Review of Comparative and International Law* 15, no. 1 (2025): 5–23. https://doi.org/10.62768/TBJ/2025/15/1/01.

Sirjon, Lade, La Ode Muhamad Sulihin, and Yan Fathahillah Purnama. "Perbandingan Mekanisme Pengakuan Bersalah pada Jalur Khusus dalam RUU KUHAP dan Konsep Plea Bargaining Ditinjau dari Asas Non-Self Incrimination." *Halu Oleo Law Review* 7, no. 2 (2023): 224–35. https://doi.org/10.33561/holrev.v7i2.29.

Siswanto, Carissa Amanda, Septhian Eka Adiyatma, Uche Nnawulezi, and Jacques Kabano. "Legal Recognition of Electronic Notarial Acts: A Comparative Study of Indonesia and Rwanda." *Indonesia Private Law Review* 6, no. 2 (2026). https://doi.org/10.25041/iplr.v6i2.4686.

Suarda, I. Gede Widhiana, Evan Hamman, Bayu Dwi Anggono, Fendi Setyawan, Moch. Marsa Taufiqurohman, and Zaki Priambudi. "Illicit Cigarette Trade in Indonesia: Trends and Analysis from the Recent Judgments." *Sriwijaya Law Review*, January 31, 2024, 38–59. https://doi.org/10.28946/slrev.Vol8.Iss1.2726.pp38-59.

Sugi Hartono, Made, and Ni Putu Rai Yuliartini. "Penggunaan Bukti Elektronik dalam Peradilan Pidana." *Jurnal Komunikasi Hukum (JKH)* 6, no. 1 (2020): 281. https://doi.org/10.23887/jkh.v6i1.23607.

Tri Cahyono, Soetardi, Wina Erni, and Taufik Hidayat. "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (*Cyber Crime*) dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 1–23. https://doi.org/10.64344/djl.v1i1.6.

Trisnawati, Trisnawati, and Shofia Hanifah. "Perkembangan Alat Bukti Elektronik Hasil Peretasan (Hacker) Sebagai Alat Bukti dalam Tindak Pidana." *Multidisciplinary Indonesian Center Journal (MICJO)* 1, no. 3 (2024): 1344–49. https://doi.org/10.62567/micjo.v1i3.162.

Tudorica, Melania, and Jeanne Mifsud Bonnici. "Legal Framework for Digital Evidence Following the Implementation of the EIO Directive: Status Quo, Challenges and Experiences in Member States." In *European Investigation Order*, vol. 55, edited by Maria Angela Biasiotti and Fabrizio Turchi. Law, Governance and Technology Series. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-31686-9_9.

Tyler, Tom R. "The Legitimacy of Legal Institutions." In *Research Handbook on Law and Psychology*, edited by Rebecca Hollander-Blumoff. Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781800881921.00011.

Ulum, Hafizatul, and M. Dewa Ginting Singaulung. "Implementasi Peraturan Mahkamah Agung Republik Indonesia Nomor 7 Tahun 2022 Tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik: Studi Kasus di Pengadilan Negeri Praya." *JISHUM : Jurnal Ilmu Sosial Dan Humaniora* 2, no. 1 (2023): 75–88. https://doi.org/10.57248/jishum.v2i1.280.

Vázquez-Pérez, Juan, and Angélica González-Arrieta. "Implementation of Blockchain in the Digital Chain of Custody to Enhance Digital Data Assurance." In *Blockchain and Applications, 6th International Congress*, vol. 1256, edited by Javier Prieto, Rafael Pastor Vargas, Oscar Lage, José Manuel Machado, and Molnár Bálint. Lecture Notes in Networks and Systems. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-81928-5_39.

Weber, Ina, Heidi Vandebosch, Karolien Poels, and Sara Pabian. "Features for Hate? Using the Delphi Method to Explore Digital Determinants for Online Hate Perpetration and Possibilities for Intervention." *Cyberpsychology, Behavior, and Social Networking* 26, no. 7 (2023): 479–88. https://doi.org/10.1089/cyber.2022.0195.

Wilson-Kovacs, Dana. "Digital Media Investigators: Challenges and Opportunities in the Use of Digital Forensics in Police Investigations in England and Wales." *Policing: An International Journal* 44, no. 4 (2021): 669–82. https://doi.org/10.1108/PIJPSM-02-2021-0019.

Zlati, George. "Romanian Jurisprudence on Cybercrime: Focus on Illegal Access to an Information System." *ERA Forum* 25, no. 3 (2024): 425–40. https://doi.org/10.1007/s12027-024-00810-y.

***

DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

None

ACKNOWLEDGMENT

None

GENERATIVE AI STATEMENT

During the preparation of this manuscript, the author utilized generative artificial intelligence as a supportive tool to assist in translation and to improve the quality of English writing. Following its use, the author conducted a thorough critical review, editing, and validation to ensure accuracy and scientific integrity. Full responsibility for the final content remains with the author. The use of artificial intelligence was limited to a supportive role and is not recognized as constituting authorship. No data analysis or substantive interpretation was carried out by artificial intelligence without human oversight.

This page intentionally left blank