KRTHA BHAYANGKARA, Vol. 20, No. 2 (2026), pp. 443-453
ISSN 1978-8991 (print) | ISSN 2721-5784 (online)
http://ejurnal.ubharajaya.ac.id/index.php/KRTHA

Digital Evidence in Criminal Procedure: A Comparative Legal Analysis Between Indonesia and The Philippines in Cybercrime Cases

Juhaimen Sumala[1], Donasto Samosir[2], Adhalia Septia Saputri[3]*

[1]College of Criminal Justice Education, University of Mindanao, Philippines
[2] Faculty of Law, Universitas Bhayangkara Jakarta Raya, Indonesia
j.sumala.501499@umindanao.edu.ph; 202210115302@mhs.ubharajaya.ac.id
adhalia.septia.saputri@dsn.ubharajaya.ac.id

Corresponding Author

Article info

Received: 28 Apr 2026 | Revised: 16 Jul 2026 | Accepted: 30 Jul 2026

DOI: https://doi.org/10.31599/krtha. v20i2.5484

Abstract : *The acceleration of digital technology development has fundamentally altered the patterns and characteristics of criminal conduct, particularly with the rise of cybercrime that relies predominantly on electronic data as evidence. This shift creates significant challenges within criminal procedural law, especially concerning the admissibility, verification, and credibility of digital evidence in judicial proceedings. This study aims to examine and compare the legal frameworks regulating digital evidence in Indonesia and the Philippines, with an emphasis on procedural aspects in criminal justice systems. The research adopts a normative juridical method utilizing statutory, conceptual, and comparative approaches. The findings reveal that Indonesia's legal structure, primarily regulated by the ITE Law and the Criminal Procedure Code (KUHAP), remains fragmented and lacks detailed procedural guidelines for handling digital evidence. Conversely, the Philippines demonstrates a more coherent and systematic framework through the Cybercrime Prevention Act of 2012 and the Rules on Electronic Evidence, particularly in ensuring forensic validation and maintaining chain of custody. The originality of this research lies in its comparative focus on procedural differences and its proposal for an integrated legal framework model for Indonesia. The study underscores the urgency of legal reform to enhance evidentiary standards and ensure consistency between substantive and procedural law. Ultimately, strengthening the regulatory framework is essential to guarantee legal certainty and improve the effectiveness of cybercrime law enforcement.*

Keywords : *Digital Evidence; Criminal Procedure; Cybercrime; Indonesia; Philippines*

Abstrak : Perkembangan teknologi digital yang semakin pesat telah mengubah secara mendasar pola dan karakter tindak pidana, khususnya melalui munculnya kejahatan siber yang sangat bergantung pada data elektronik sebagai alat bukti utama. Perubahan ini menimbulkan tantangan serius dalam hukum acara pidana, terutama terkait dengan

penerimaan, pembuktian, dan keandalan bukti digital dalam proses peradilan. Penelitian ini bertujuan untuk mengkaji dan membandingkan kerangka hukum yang mengatur bukti digital di Indonesia dan Filipina dengan menitikberatkan pada aspek prosedural dalam sistem peradilan pidana. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Hasil penelitian menunjukkan bahwa sistem hukum Indonesia yang diatur melalui UU ITE dan KUHAP masih bersifat parsial serta belum memiliki pengaturan prosedural yang komprehensif terkait bukti digital. Sebaliknya, Filipina memiliki sistem yang lebih terstruktur melalui Cybercrime Prevention Act of 2012 dan Rules on Electronic Evidence, khususnya dalam menjaga chain of custody dan validasi forensik. Kebaruan penelitian ini terletak pada analisis komparatif yang menekankan perbedaan prosedural serta menawarkan model kerangka hukum terintegrasi bagi Indonesia. Penelitian ini menegaskan urgensi reformasi hukum guna meningkatkan standar pembuktian serta harmonisasi antara hukum materiil dan formil, sehingga dapat menjamin kepastian hukum dan efektivitas penegakan hukum kejahatan siber.

Kata kunci : Bukti Digital; Hukum Acara Pidana; Kejahatan Siber; Indonesia; Filipina

Introduction

Digital transformation has significantly redefined the landscape of criminal activity, shifting it from conventional physical acts to technologically mediated offenses. Cybercrime, as a modern manifestation of criminal behavior, is characterized by its reliance on digital systems and electronic networks, which transcend territorial boundaries and complicate law enforcement mechanisms.[1]

The central role of digital evidence in cybercrime distinguishes it from traditional forms of proof. Digital evidence encompasses any data or information stored, processed, or transmitted electronically that can be used to establish facts in legal proceedings.[2] Unlike conventional evidence, digital data is inherently fragile, easily altered, and highly dependent on technological systems, thereby requiring specialized handling procedures.[3]

The rapid integration of digital technologies into social, economic, and governmental sectors has intensified the complexity of criminal activities. As a result, traditional criminal procedure frameworks are increasingly inadequate in addressing evidentiary challenges arising from digital environments.[4] Indonesia has responded to these developments through legislative reforms, particularly the amendment of the ITE Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of

[1] Jonathan Clough, Principles of Cybercrime, 3rd ed. (Cambridge: Cambridge University Press, 2022), p. 45.
[2] United Nations Office on Drugs and Crime (UNODC), Digital Evidence and Cybercrime: Recent Developments and Emerging Threats (Vienna: United Nations Publication, 2024), p. 19.
[3] Mahrus Ali, "Digital Evidence dalam Sistem Peradilan Pidana Indonesia," Jurnal RechtsVinding: Media Pembinaan Hukum Nasional, Vol. 11, No. 1 (2022), p. 12.
[4] Organisation for Economic Co-operation and Development (OECD), Cybercrime and Digital Evidence (Paris: OECD Publishing, 2023), p. 61.

2016 and most recently by Law No. 1 of 2024 and the enactment of Law No. 20 of 2025 on Criminal Procedure. While these reforms signify progress, they also reveal structural gaps in procedural regulation.[5]

In contrast, the Philippines has established a more comprehensive framework through the Cybercrime Prevention Act of 2012 and the Rules on Electronic Evidence, which provide detailed procedural guidance.[6] This study aims to critically analyze and compare these frameworks to identify normative gaps and propose legal reforms.

This study adopts a normative juridical approach and is limited to doctrinal analysis of statutory law, jurisprudence, and recent legal literature. It does not include empirical fieldwork, interviews, or forensic laboratory analysis, and is therefore confined to the interpretation and comparison of legal norms.

Methods

This research adopts a normative juridical method that focuses on examining legal norms, doctrines, and statutory regulations governing digital evidence within criminal procedural law. This approach is particularly appropriate because the core issue of this study lies in evaluating the adequacy, coherence, and effectiveness of legal frameworks rather than analyzing empirical data.[7]

Normative legal research conceptualizes law as a structured system of norms consisting of written rules, legal principles, and doctrinal interpretations. Therefore, this study not only describes existing legal provisions but also formulates prescriptive recommendations aimed at improving Indonesia's regulatory framework on digital evidence.[8]

Research Approaches: 1) Statutory Approach. The statutory approach is applied to analyze legislative frameworks in both jurisdictions. In Indonesia, the primary legal instruments include Law No. 1 of 2024 concerning amendments to the ITE Law and Law No. 20 of 2025 on the Criminal Procedure Code. This approach aims to examine the scope, structure, and limitations of these regulations, particularly regarding admissibility standards and procedural safeguards for digital evidence.[9] 2) Conceptual Approach. The conceptual approach is used to explore legal doctrines and theoretical foundations relevant to digital evidence, including evidentiary principles, authenticity, integrity, chain of custody, and forensic validation. This approach is essential in assessing whether current legal provisions align with modern evidentiary standards in digital environments.[10] 3) Comparative Approach. A comparative legal analysis is conducted by examining the legal system of the Philippines, particularly Republic Act No. 10175 and the Rules

[5] Eddy O.S. Hiariej, Prinsip-Prinsip Hukum Pidana (Yogyakarta: Cahaya Atma Pustaka, 2021), p. 98.
[6] Lorraine V. Aragon, "Digital Evidence and Standards of Proof in Cybercrime Cases," International Journal of Law and Information Technology, Vol. 29, No. 1 (2021), p. 77.
[7] Johnny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif (Malang: Bayumedia, 2022), p. 57.
[8] Dyah Ochtorina Susanti & A'an Efendi, Penelitian Hukum (Jakarta: Sinar Grafika, 2022), p. 34
[9] Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana, 2021), p. 133.
[10] Widodo Ekatjahjana, Hukum Pembuktian (Jakarta: Sinar Grafika, 2021), p. 145.

on Electronic Evidence. This comparison aims to identify best practices, procedural differences, and potential models for legal reform in Indonesia.[11]

Result And Discussion

The Urgency of Digital Evidence in Contemporary Criminal Justice

The emergence of cybercrime has significantly altered the orientation of criminal justice systems worldwide. In the contemporary digital era, criminal activities are no longer limited to conventional physical conduct but increasingly involve electronic systems, digital platforms, and internet-based communication. Consequently, digital evidence has become one of the most essential forms of proof in criminal proceedings, particularly in cases involving cyber fraud, identity theft, hacking, financial technology crimes, online defamation, and digital exploitation.[12]

Digital evidence possesses unique characteristics that distinguish it from traditional forms of evidence. Unlike physical evidence, digital evidence is intangible, highly volatile, and vulnerable to modification or deletion. This condition requires specialized procedures in collection, preservation, examination, and presentation before the court.[13]

The reliability of digital evidence depends heavily on the integrity of the forensic process. Improper handling may result in contamination or manipulation, which can ultimately reduce its evidentiary value in judicial proceedings. Therefore, modern criminal justice systems increasingly emphasize the importance of digital forensic science as an integral component of evidentiary law.

Furthermore, the globalization of information technology has created jurisdictional complexities because cybercrime frequently transcends national boundaries. A cyberattack conducted in one country may produce legal consequences in another jurisdiction, thereby creating challenges concerning territorial authority, evidence sharing, and international cooperation.

From the perspective of criminal procedural law, the increasing dependence on digital evidence demonstrates the necessity of reforming traditional evidentiary frameworks. Conventional procedural systems were originally designed to regulate tangible forms of proof such as witness testimony, documents, and physical objects. However, digital transformation requires legal systems to adopt more adaptive procedural standards capable of accommodating technological developments.

[11] Jonathan Clough, Principles of Cybercrime (Cambridge, 2022), p. 88.
[12] *Ibid.*, p. 45.
[13] UNODC), p. 19.

Legal Recognition and Constitutional Protection of Digital Evidence in Indonesia

Indonesia has gradually strengthened the legal status of digital evidence through legislative reform. The enactment of Law No. 11 of 2008 concerning Electronic Information and Transactions represented the initial recognition of electronic information and electronic documents as lawful evidence. This recognition was subsequently reinforced through amendments under Law No. 19 of 2016 and Law No. 1 of 2024.[14]

The latest amendment demonstrates Indonesia's effort to modernize its legal framework by accommodating rapid technological developments and strengthening legal certainty in electronic transactions. Nevertheless, although substantive recognition has been established, procedural regulation concerning digital evidence remains relatively fragmented.

The enactment of Law No. 20 of 2025 concerning the new Criminal Procedure Code (KUHAP) constitutes a significant development in Indonesian criminal procedural law. Unlike the previous Criminal Procedure Code, which primarily focused on conventional forms of evidence, KUHAP 2025 explicitly recognizes electronic evidence as an independent category of admissible proof.[15]

However, the implementation of these reforms continues to encounter practical challenges. Indonesian law enforcement institutions still face limitations in technological infrastructure, digital forensic expertise, and standardized operational procedures. These institutional weaknesses often affect the consistency of evidentiary handling and judicial interpretation. Moreover, the absence of comprehensive implementing regulations creates legal uncertainty regarding technical procedures such as digital seizure, forensic examination, authentication standards, and preservation mechanisms. As a result, judicial practices involving digital evidence may differ significantly between courts and law enforcement agencies.

The admissibility of digital evidence must not only fulfill procedural legality but also comply with constitutional principles and human rights standards. In democratic legal systems, the use of electronic surveillance and digital investigation mechanisms frequently raises concerns regarding privacy rights, proportionality, and due process of law. The Indonesian Constitutional Court has emphasized that electronic evidence may only be admitted when obtained through lawful procedures that respect constitutional guarantees. In Constitutional Court Decision No. 20/PUU-XIV/2016, the Court affirmed that the collection of electronic information must balance the interests of law enforcement with the protection of individual rights.

This constitutional perspective is particularly important because digital investigations often involve interception, access to private communications, and electronic monitoring. Without strict legal limitations, these mechanisms may potentially violate fundamental rights guaranteed under the Constitution. In this context, the principle of due process of law serves as a

[14] Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana* , Yogyakarta: Cahaya Atma Pustaka, 2021, p. 98.
[15] KUHAP.

fundamental safeguard against arbitrary state action. Evidence obtained illegally or through unlawful interception should be excluded from judicial proceedings to preserve the integrity of the criminal justice system.

Comparative and Theoretical Analysis of Digital Evidence Regulation: Lessons from the Philippines and Indonesia

Compared to Indonesia, the Philippines has developed a more structured procedural framework concerning digital evidence. The Cybercrime Prevention Act of 2012 and the Rules on Electronic Evidence provide comprehensive regulation regarding admissibility standards, authentication mechanisms, and evidentiary procedures.[16]

One of the major strengths of the Philippine system lies in its detailed procedural standards concerning chain of custody and forensic validation. Courts in the Philippines consistently emphasize the necessity of preserving the integrity of electronic data from the initial collection process until courtroom presentation. Philippine jurisprudence also demonstrates a progressive judicial approach toward balancing cybercrime enforcement with constitutional rights. The Supreme Court of the Philippines has repeatedly stressed that electronic evidence must satisfy reliability and legality standards before being accepted in criminal proceedings.[17]

Nevertheless, despite its relatively advanced framework, the Philippines continues to face challenges concerning transnational cybercrime, technological adaptation, and evolving cyber threats. This demonstrates that digital evidence regulation requires continuous legal development in response to rapid technological change.

From the perspective of Lawrence M. Friedman's legal system theory, the effectiveness of digital evidence regulation depends on the interaction between legal substance, legal structure, and legal culture.[18] Indonesia has improved its legal substance through legislative reform, particularly by recognizing electronic evidence under KUHAP 2025 and the amended ITE Law. However, structural factors such as institutional readiness, technological infrastructure, and law enforcement capacity remain relatively underdeveloped.

Legal culture also plays an essential role in determining the effectiveness of evidentiary reform. Public trust in digital investigation mechanisms and judicial institutions significantly influences the legitimacy of criminal proceedings involving electronic evidence. Furthermore, evidentiary law theory emphasizes that digital evidence requires stricter standards of proof compared to conventional evidence because of its susceptibility to

[16] Republic of the Philippines, Republic Act No. 10175 concerning Cybercrime Prevention Act of 2012.
[17] Supreme Court of the Philippines, Jurisprudence on Electronic Evidence and Cybercrime Prosecution (2021–2024).
[18] Lawrence M. Friedman, Law and Society: An Introduction, New York: Oxford University Press, 2021, p. 102.

manipulation. Therefore, forensic validation and expert testimony become indispensable elements in establishing evidentiary reliability.

Comprehensive Reform of Digital Evidence Regulation in Indonesia: Procedural Standards, Judicial Development, and Institutional Challenges

The rapid development of cybercrime demonstrates that legal reform concerning digital evidence can no longer be postponed. Indonesia must immediately establish comprehensive implementing regulations governing digital forensic procedures, authentication standards, electronic seizure mechanisms, and chain of custody requirements. In addition, institutional strengthening is equally important. Legal reform should include investment in forensic laboratories, technological infrastructure, and specialized training programs for judges, prosecutors, investigators, and forensic experts.

Comparative analysis with the Philippines indicates that procedural clarity and institutional readiness are essential factors in ensuring effective cybercrime enforcement. Without adequate procedural safeguards and institutional capacity, formal recognition of digital evidence will remain ineffective in practice. Therefore, the modernization of criminal procedure law should not merely focus on legislative amendments but also emphasize institutional reform, professional competence, and technological adaptation within the broader criminal justice system.

Digital evidence has fundamentally altered the traditional evidentiary system in criminal law. Unlike conventional evidence, it exists in intangible form, is easily duplicated, and is highly vulnerable to manipulation. These characteristics require stricter procedural safeguards to maintain its evidentiary value. According to modern evidentiary theory, digital evidence must fulfill three essential criteria: authenticity, integrity, and reliability.[19]

Authenticity ensures that evidence originates from a legitimate source, integrity guarantees that data remains unchanged, and reliability ensures its trustworthiness in judicial proceedings. Additionally, the principle of chain of custody plays a crucial role in maintaining evidentiary validity. Any break in this chain may result in inadmissibility.[20]

The enactment of Law No. 20 of 2025 represents a major reform in Indonesian criminal procedure law. Unlike the previous Criminal Procedure Code, the new KUHAP explicitly recognizes digital evidence as an independent form of legal proof.[21]

This reform reflects Indonesia's adaptation to technological developments and aligns with global legal trends. To be admissible, digital evidence must meet requirements of authenticity, integrity, and reliability.[22]

---

[19] Mahrus Ali, "Digital Evidence dalam Sistem Peradilan Pidana Indonesia," Jurnal RechtsVinding: Media Pembinaan Hukum Nasional, Vol. 11, No. 1 (2022), p. 12.

[20] International Criminal Police Organization (INTERPOL), Global Guidelines for Digital Forensics Laboratories and Cybercrime Investigations (Lyon: INTERPOL, 2022), p. 40.

[21] Law No. 20 of 2025 on KUHAP.

[22] Organisation for Economic Co-operation and Development (OECD), Cybercrime and Digital Evidence (Paris: OECD Publishing, 2023), p. 61

KUHAP 2025 introduces several key procedural principles:

a. Authentication: evidence must be verified through digital forensic processes;

b. Chain of custody: handling must be traceable from collection to trial;

c. Expert testimony: forensic experts are required to validate evidence.

Despite these developments, implementing regulations remain limited, creating challenges in practical enforcement.[23]

The amended ITE Law (Law No. 1 of 2024) reinforces the recognition of electronic information as valid legal evidence. The relationship between KUHAP 2025 and the ITE Law shows improved harmonization:

a. ITE Law → substantive recognition;

b. KUHAP → procedural regulation.

However, challenges persist due to lack of standardized forensic procedures, limited institutional capacity, and inconsistent judicial interpretation.[24]

The Constitutional Court has strengthened the legitimacy of digital evidence through its jurisprudence. In Decision No. 20/PUU-XIV/2016, the Court affirmed that electronic evidence is admissible if obtained lawfully and does not violate constitutional rights.[25] The Court emphasized the importance of balancing law enforcement interests with privacy protection and due process.

The Supreme Court has played a significant role in shaping the practical application of digital evidence, as seen in Decision No. 574 K/Pid.Sus/2021, the Court accepted digital evidence supported by forensic validation. Similarly, Decision No. 108 PK/Pid.Sus/2022 highlighted the importance of chain of custody and technical verification.[26] These rulings demonstrate a progressive judicial approach.

Despite recent reforms, several issues remain:

a. fragmented legal framework;

b. absence of national forensic standards;

c. institutional limitations.

These gaps indicate that legal reform must include both regulatory and institutional improvements.[27]

---

[23] National Institute of Standards and Technology (NIST), Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1 (Gaithersburg: U.S. Department of Commerce, 2022), p. 22.

[24] European Union Agency for Cybersecurity (ENISA), *Electronic Evidence and Digital Forensics: Challenges and Opportunities* (Athens: ENISA, 2023), p. 17.

[25] Constitutional Court Decision No. 20/PUU-XIV/2016.

[26] Supreme Court Decision No. 108 PK/Pid.Sus/2022.

[27] Rita Komalasari dan Cecep Mustafa, Electronic Evidence in Justice System, *Jurnal Hukum dan Peradilan*, Vol. 12, No. 3 (2023), p. 90.

According to Lawrence M. Friedman's theory, legal effectiveness depends on:

a. legal structure;

b. legal substance;

c. legal culture.

Indonesia has improved its legal substance, but structural and cultural aspects remain weak.[28]

To ensure effective implementation, Indonesia must:

a. develop implementing regulations;

b. establish forensic standards;

c. strengthen institutional capacity;

d. harmonize laws.[29]

Conclusion

The study concludes that digital transformation has significantly reshaped criminal evidentiary systems, particularly in cybercrime cases. Digital evidence has become a central element in modern criminal proceedings due to its ability to capture and represent electronic activities. However, its unique characteristics require advanced legal frameworks to ensure admissibility and reliability.

Indonesia has made substantial progress through the enactment of Law No. 1 of 2024 and Law No. 20 of 2025, which formally recognize digital evidence. Nevertheless, challenges remain due to a lack of implementing regulations, absence of standardized forensic procedures, and institutional limitations.[30] Comparatively, the Philippines demonstrates a more advanced procedural system, indicating that Indonesia is still in a transitional phase.

Recommendation

To ensure the effective implementation of digital evidence regulation in Indonesia, comprehensive regulatory strengthening is required. The Government should immediately establish implementing regulations under KUHAP 2025 that provide clear procedural guidance concerning digital evidence collection, examination, authentication, preservation, and presentation before the court. Furthermore, legal harmonization between the ITE Law and KUHAP must be strengthened to eliminate potential inconsistencies between substantive recognition and procedural application. The establishment of national digital forensic standards, including

[28] Lawrence M. Friedman, *Loc., Cit.*
[29] Council of Europe, Electronic Evidence and Criminal Justice: Updated Frameworks and Recommendations (Strasbourg: Council of Europe Publishing, 2023), p. 55.
[30] UNODC Report (2023), p. 66.

certification mechanisms, technical guidelines, and standardized operating procedures (SOPs), is also essential to ensure the authenticity, integrity, and reliability of digital evidence in criminal proceedings.

In addition to regulatory reform, institutional and judicial strengthening must become a central priority. Law enforcement institutions should be supported through improved technological infrastructure, specialized training programs, and enhanced professional competence for investigators, prosecutors, judges, and forensic experts. The Supreme Court should develop judicial guidelines to promote consistent interpretation and application of digital evidence standards across courts. Moreover, comparative experiences from the Philippines demonstrate the importance of procedural clarity, forensic validation, and institutional preparedness; therefore, relevant best practices should be adapted to Indonesia's legal system while considering its constitutional framework and criminal justice structure. Through these measures, digital evidence regulation can develop into a more reliable, effective, and rights-based component of Indonesia's criminal justice system.

References

Benny Sumardiana et al., Evaluation of Electronic Evidence in Criminal Justice, *Indonesian Journal of Criminal Law Studies* Vol. 9 No. 2 (2024).

Constitutional Court of the Republic of Indonesia, decisions on electronic evidence admissibility and privacy rights (compiled jurisprudence, 2021–2024).

Constitutional Court Decision No. 20/PUU-XIV/2016.

Dyah Ochtorina Susanti & A'an Efendi, *Penelitian Hukum (Legal Research)* (Jakarta: Sinar Grafika, 2022).

Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2021).

European Union Agency for Cybersecurity (ENISA), Electronic Evidence and Digital Forensics: Challenges and Opportunities (ENISA, 2023).

----------. Lorraine V. Aragon, "Digital Evidence and Standards of Proof in Cybercrime Cases". *International Journal of Law and Information Technology*. (2021).

INTERPOL, Global Guidelines for Digital Forensics Laboratories and Cybercrime Investigations (INTERPOL, 2022).

----------. Council of Europe, Electronic Evidence and Criminal Justice: Updated Frameworks (2021–2023 reports).

Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2022).

Jonathan Clough, *Principles of Cybercrime* (3rd ed., Cambridge University Press, updated discussions 2022); UNODC, Cybercrime in the Digital Age: Recent Developments and Emerging Threats (2023).

Law No. 20 of 2025 on the Criminal Procedure Code (KUHAP), provisions on electronic evidence.

Law No. 1 of 2024 concerning Amendments to the ITE Law.

Lawrence M. Friedman, Law and Society: An Introduction (New York: Oxford University Press, 2021).

Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2021).

Rita Komalasari & Cecep Mustafa, Electronic Evidence in Justice System, *Jurnal Hukum dan Peradilan* Vol. 12 No. 3 (2023).

Mahrus Ali, Digital Evidence dalam Sistem Peradilan Pidana Indonesia, *Jurnal RechtsVinding* Vol. 11 No. 1 (2022).

National Institute of Standards and Technology (NIST), Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Rev.1 (2022).

OECD, *Cybercrime and Digital Evidence* (Paris: OECD Publishing, 2023).

Republic of the Philippines, Republic Act No. 10175 (Cybercrime Prevention Act of 2012); Supreme Court of the Philippines, administrative circulars and e-court developments (2020–2024).

Supreme Court Decision No. 108 PK/Pid.Sus/2022.

----------. No. 574 K/Pid.Sus/2021.

----------. Decisions involving cybercrime and electronic evidence (jurisprudential trends, 2020–2024).

Supreme Court of the Philippines, jurisprudence on constitutional limits in cyberspace and digital surveillance (2021–2024).

----------. Decisions on electronic evidence and cybercrime prosecutions (2020–2024 jurisprudence).

United Nations Office on Drugs and Crime (UNODC), Digital Evidence and Cybercrime (Vienna: United Nations, 2024).

----------. Cybercrime in the Digital Age: Recent Developments and Emerging Threats (United Nations, 2023).

Widodo Ekatjahjana, *Hukum Pembuktian dalam Sistem Peradilan Pidana Indonesia* (Jakarta: Sinar Grafika, 2021).