

ISSN 2809-672X (Online)
IUS POSITUM: Journal of Law Theory and Law Enforcement
https://journal.jfpublisher.com/index.php/jlte
Vol. 5 Issue 1, January 2026
doi.org/10.56943/jlte.v5i1.1111

Normative Recognition and Procedural Reality: The Legality of Digital Data in *Polri* Investigations

Stanny Rolanda Elias[1]*, M. Sholehuddin[2]
[1]stannyelias@gmail.com, [2]sholehuddin@ubhara.ac.id
[1]Polda Sulawesi Utara, [2]Universitas Bhayangkara Surabaya

*Corresponding Author: Stanny Rolanda Elias
Email: stannyelias@gmail.com

ABSTRACT

The rapid development of information technology has shifted criminal activities into digital environments, making digital data a crucial source of evidence for the Indonesian National Police (Polri). This study aims to analyze the legality of digital data as evidence in criminal investigations under Law Number 20 of 2025, the Electronic Information and Transactions Law, and modern evidence law. It addresses the juridical challenges regarding privacy protection, due process, and legal certainty during digital investigations. This research employs a normative legal method with statutory, conceptual, and analytical approaches. The findings indicate that the explicit recognition of electronic evidence under the 2025 Criminal Procedure Code provides greater legal certainty than the previous framework. However, its implementation still faces significant challenges, namely formal and substantive legality, chain of custody standards, digital forensic procedures, privacy protection, and judicial oversight. The novelty of this study lies in its systematic effort to connect the normative recognition of electronic evidence, the legality of digital investigative measures, and the protection of privacy within a single analytical framework. Therefore, improving implementing regulations, strengthening investigators' digital forensic capacity, and establishing effective oversight mechanisms are essential to ensure that digital evidence supports legal certainty, justice, and the protection of human rights.

Keywords: *Criminal Investigation, Digital Evidence, Digital Forensics, Due Process, Electronic Evidence*

INTRODUCTION

The rapid development of information and communication technology has fundamentally transformed patterns of social interaction, economic activity, and criminal conduct. Criminal activities that were traditionally committed through physical means have increasingly migrated into digital environments, giving rise to various forms of cybercrime that rely on computer systems, electronic communications, digital platforms, and networked technologies. This transformation has altered the nature of criminal investigation and evidence gathering, requiring law enforcement agencies, including the Indonesian National Police (*Kepolisian Negara Republik Indonesia* or *Polri*), to develop investigative methods capable of addressing the distinctive characteristics of digitally mediated crime. Electronic traces may reveal communications, financial transactions, user activities, and connections between suspects and criminal events, so digital information has become an increasingly important source of evidence.[1]

In the Indonesian criminal justice system, evidence is a fundamental element for establishing the occurrence of a criminal offence and the criminal responsibility of the accused. The former Criminal Procedure Code (*Kitab Undang-Undang Hukum Acara Pidana* or *KUHAP*), namely Law Number 8 of 1981, recognised five categories of lawful evidence under Article 184 paragraph (1), that is, witness testimony, expert testimony, documentary evidence, indications, and the defendan's statement. This evidentiary framework was formulated before the widespread emergence of digital technology and did not expressly establish digital data as an independent category of evidence. The subsequent development of electronic transactions and cybercrime exposed limitations in an evidentiary framework primarily designed around conventional forms of proof.[2]

The enactment of Law Number 20 of 2025 concerning the Criminal Procedure Code has introduced a new dimension to this issue. The new *KUHAP* explicitly recognises electronic evidence as a lawful means of evidence, and this recognition provides greater normative certainty than the previous framework, which relied substantially on the Electronic Information and Transactions Law and judicial interpretation.[3] Nevertheless, formal recognition does not resolve the procedural difficulties associated with acquiring, preserving, authenticating, and presenting digital evidence. Digital data may be volatile, easily altered, reproduced

[1] Appe Hutauruk, Fendi Maruba Parlindungan Hutahaean, and Adalin Ali, "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure," *Politica: Jurnal Hukum Tata Negara Dan Politik Islam* 13, no. 2 (September 22, 2026): 618–59, https://doi.org/10.32505/politica.v13i2.16111.
[2] Dewa Gede Giri Santosa and Karell Mawla Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia," *Jurnal Hukum Dan Peradilan* 11, no. 2 (July 31, 2022): 195, https://doi.org/10.25216/jhp.11.2.2022.195-218.
[3] Ambron Ritonga Wildan and Fanitia Aditia, "Pembaruan Sistem Pembuktian Pidana Indonesia Berdasarkan KUHAP 2025," *Delicti : Jurnal Hukum Pidana Dan Kriminologi* 4, no. 1 (October 22, 2026): 163–75, https://doi.org/10.25077/DELICTI.V.4.I.1.P.163-175.2026.

without apparent degradation, distributed across multiple systems, and stored in locations beyond the immediate physical control of investigators. Its evidentiary value therefore depends on formal admissibility and on the legality, integrity, and reliability of the process through which it is obtained and preserved.[4]

These difficulties are particularly relevant to criminal investigations conducted by *Polri*. Investigators may encounter digital evidence in various forms, including server logs, electronic communications, metadata, social media content, digital financial records, cryptocurrency transactions, and information stored on mobile devices or cloud-based systems. Investigative measures such as digital forensic acquisition, seizure of electronic devices, access to cloud storage, decryption of protected information, and interception of electronic communications may interfere directly with individual privacy and other fundamental rights. The acquisition of digital evidence without adequate procedural safeguards may therefore create tension between the state's legitimate interest in investigating crime and the individual's right to protection against arbitrary interference.[5]

Several studies have examined the evidentiary treatment of electronic information in Indonesian legal proceedings. Hakki and Sadjijono analyse the evidential system for non-physical sexual harassment and demonstrate how digital conversations and recordings are treated as evidence in legal proceedings.[6] Suarsika et al. examine the legal policy on exhibitionism through video-call-based social media and highlight the position of electronic information under the Information and Electronic Transactions Law, while also acknowledging the growing importance of electronic evidence in legal disputes.[7] These studies confirm the journal's engagement with digital evidence, yet they focus primarily on substantive offences and do not examine the procedural legality of digital investigative measures conducted by *Polri* after the enactment of Law Number 20 of 2025.

In addition, Santosa and Kamali analyse the acquisition and presentation of digital evidence in Indonesian criminal trials and emphasise the need for a more coherent authentication framework.[8] Hutauruk et al. examine smartphone data extraction as a form of digital search and argue that the 2025 *KUHAP* does not yet provide adequate normative limits between the seizure of a physical device and

[4] Hutauruk, Hutahaean, and Ali, "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure."
[5] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."
[6] Abdillah Hakki and Sadjijono Sadjijono, "The Evidential System for The Non-Physical Offense of Sexual Harrasment," *Ius Positum: Journal of Law Theory and Law Enforcement* 3, no. 2 (June 28, 2024): 1–10, https://doi.org/10.56943/jlte.v3i2.547.
[7] I Komang Suarsika, Ni Ketut Wiratny, and Erikson Sihotang, "Legal Policy on Exhibitionism Through Video Call-Based Social Media Reviewed from The Information and Electric Transacstions (IET) Law," *Ius Positum: Journal of Law Theory and Law Enforcement* 3, no. 2 (August 9, 2024): 48–61, https://doi.org/10.56943/jlte.v3i2.576.
[8] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."

access to its digital contents, particularly in relation to pretrial review.[9] These studies address procedural and forensic dimensions of digital evidence, but they do not comprehensively connect the legality of investigative measures with privacy protection and judicial oversight in the specific context of *Polri* investigations under the new *KUHAP*.Against this background, the objective of this study is to examine the legal validity of digital evidence in criminal investigations conducted by *Polri*. It specifically analyzes the development of the evidentiary framework from Law No. 8/1981 to Law No. 20/2025, the relationship between the Criminal Procedure Code and legislation concerning electronic information and transactions, and the legal requirements governing the acquisition and use of digital evidence. The study further examines whether the current framework provides adequate checks and balances to protect privacy and other fundamental rights during digital investigations. This study is expected to contribute to the development of Indonesian criminal procedural law by formulating a more coherent approach to digital evidence that accommodates the needs of effective law enforcement while maintaining legality, proportionality, accountability, and protection of individual rights.

The novelty of this study lies in its systematic effort to connect three dimensions that are often discussed separately in the existing literature, namely, the normative recognition of electronic evidence under the 2025 *KUHAP*, the legality of digital investigative measures conducted by *Polri*, and the protection of privacy and due process of law. This study does not stop at the question of whether digital data may be admitted as evidence. It examines how formal and substantive legality requirements are translated into procedures for acquiring, preserving, authenticating, and presenting digital evidence. In this way, the study offers an analytical framework that integrates legal certainty, forensic accountability, and judicial oversight within a single construction.

The research gap is normative and procedural. Existing literature has documented the recognition of electronic evidence and the technical challenges of digital forensics, but it has not adequately answered how substantive and formal legality standards should be operationalised in *Polri* investigations after the 2025 *KUHAP*. More specifically, no study has simultaneously examined (i) the boundary between device seizure and data extraction, (ii) the lawfulness of obtaining data from service providers and cloud systems, (iii) chain-of-custody and cryptographic verification standards as conditions for evidentiary validity, and (iv) oversight and legal remedies available to individuals whose personal data are affected by digital investigative measures. The absence of a framework that unites these dimensions produces uncertainty about how police investigators should act and how courts should assess the legality of digital evidence.

[9] Hutauruk, Hutahaean, and Ali, "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure."

Against this background, this study aims to analyse the legality of using digital data as evidence in criminal investigations conducted by *Polri* under Law Number 20 of 2025 concerning the Criminal Procedure Code, the Electronic Information and Transactions Law, and the principles of modern criminal evidence law. More specifically, the study aims (i) to explain the development of the digital evidentiary framework from Law Number 8 of 1981 to Law Number 20 of 2025, (ii) to analyse the formal and substantive legality requirements binding on investigators in obtaining and using digital evidence, and (iii) to assess the adequacy of procedural safeguards for privacy protection and due process of law in digital investigations conducted by *Polri*.

LITERATURE REVIEW

Studies on digital evidence in criminal procedure have developed alongside the expansion of information technology and cybercrime. Digital evidence differs from conventional evidence because it can be copied, altered, deleted, encrypted, and stored across multiple systems. Its evidentiary value therefore depends on both formal admissibility and the reliability of the process by which it is obtained, preserved, and presented. In Indonesia, this debate begins with the former Criminal Procedure Code, namely Law No. 8/1981, Article 184(1) of which recognized five categories of lawful evidence: witness testimony, expert testimony, documentary evidence, indications, and the defendant's statement.[10] The provision did not expressly recognize electronic information or digital data as an independent category of evidence. The Electronic Information and Transactions Law later recognized electronic information and electronic documents as lawful evidence, but formal recognition alone did not resolve procedural questions concerning authentication, integrity, and chain of custody.[11]

Indonesian legal scholarship has examined digital evidence from several perspectives. Santosa and Kamali analyzed the acquisition and presentation of digital evidence in Indonesian criminal trials. They argue that digital evidence requires specific methods of acquisition and presentation, and that courts must consider how such evidence was obtained when evaluating its validity.[12] Their study confirms that formal recognition is insufficient without reliable forensic procedures and documented chain of custody. Digital forensics therefore occupies a central position in transforming raw digital data into evidence that can withstand

[10] "Undang-Undang (UU) Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana" (1981), https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981.
[11] "Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik" (2016), https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016.
[12] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."

judicial scrutiny. Expert testimony may assist judges in understanding technical matters, but it cannot replace a lawful and transparent evidentiary procedure.

The role of digital forensics becomes particularly critical in specific types of cybercrime. International literature, such as Casey's work on digital evidence, emphasizes that forensic soundness requires verifiable methods, expert testimony, and strict documentation.[13] In the Indonesian context, various studies have applied these principles to cases involving social media, online fraud, and personal data theft. For instance, forensic analysis of digital devices has been used in cases involving online pornography and hate speech, where electronic traces and user-generated content become central evidentiary material.[14] Similarly, law enforcement against phishing and personal data theft highlights the growing need to protect personal information during digital investigations.[15]These cases illustrate that digital evidence is no longer peripheral in Indonesian criminal proceedings. They also reveal persistent challenges concerning electronic platform regulation, personal data protection, and the reliability of digitally stored information.

Another strand of literature concerns privacy and due process. Digital searches and device seizures may expose large amounts of personal information, including data unrelated to the alleged offence. The Constitutional Court of the Republic of Indonesia, through Decision No. 21/PUU-XII/2014, strengthened judicial review over coercive measures in criminal investigations.[16] This decision reinforces the principle that investigative actions affecting individual rights must remain subject to legal scrutiny. The Personal Data Protection Law further reinforces the need to limit access, use, disclosure, and retention of personal information during criminal investigations.[17] In this context, the principles of legality, necessity, proportionality, and accountability become essential safeguards. They ensure that digital evidence is obtained through lawful procedures and that the rights of suspects and third parties are protected.

Despite this growing body of scholarship, a gap remains. Many studies focus on admissibility, forensic examination, or substantive criminal offences. Fewer studies systematically examine the legality of police investigative measures in obtaining digital evidence under Law No. 20/2025 on the Criminal Procedure Code. The new *KUHAP* expands the categories of lawful evidence to include electronic

---

[13] Nan Xiao et al., "A Novel Blockchain-Based Digital Forensics Framework for Preserving Evidence and Enabling Investigation in Industrial Internet of Things," *Alexandria Engineering Journal* 86 (January 2024): 631–43, https://doi.org/10.1016/j.aej.2023.12.021.

[14] Casey Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet,* 3rd ed. (Academic Press, 2011), https://www.researchgate.net/publication/220691491_Digital_Evidence_and_Computer_Crime_-_Forensic_Science_Computers_and_the_Internet_3rd_Edition.

[15] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003).

[16] "Constitutional Court of the Republic of Indonesia, Decision No. 21/PUU-XII/2014." (2014), https://www.mkri.id/public/content/persidangan/putusan/21_PUU-XII_2014.pdf.

[17] "Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi" (2022), https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

evidence, which provides greater legal certainty than the previous framework.[18] However, its implementation still depends on implementing regulations, uniform technical standards, forensic capacity, and effective oversight. This study addresses that gap by integrating formal legality, substantive reliability, privacy protection, and judicial oversight in criminal investigations conducted by the Indonesian National Police. In doing so, it positions digital evidence not merely as a technical issue but as a constitutional and procedural issue that requires a coherent legal framework.

RESEARCH METHODOLOGY

This study employs a normative legal research method, which treats law as a system of norms and examines primary, secondary, and tertiary legal materials to address the legal issues under investigation.[19] The normative approach is appropriate because the central problems of this study concern the construction of legality, evidentiary requirements, and procedural safeguards in digital investigations, rather than empirical patterns of social behaviour.[20] The approaches used consist of the statutory approach, the conceptual approach, and the analytical approach. The statutory approach examines the applicable legal framework governing digital evidence, namely Law Number 20 of 2025 concerning the Criminal Procedure Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and relevant regulations concerning digital forensics and electronic evidence.[21] The conceptual approach is used to assess the legal principles, doctrines, and concepts arising from the use of digital evidence, including legality, necessity, proportionality, chain of custody, and due process of law.[22] The analytical approach is employed to evaluate the coherence and adequacy of the existing framework in regulating the acquisition, preservation, authentication, and presentation of digital evidence in criminal investigations conducted by the Indonesian National Police.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation, judicial decisions, and official legal documents with binding authority, particularly Law

[18] "Undang-Undang (UU) Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Acara Pidana" (2025), https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025.
[19] Marzuki Peter Mahmud, *Penelitian Hukum*, 19th ed. (Jakarta: Kencana, 2019), https://opac.perpusnas.go.id/DetailOpac.aspx?id=1409842.
[20] Putri Wulandari, "Normative Legal Research Methodology from the Experts' Perspective: A Comparative Analysis of Concepts and Approaches," *Archipel: Journal of Indonesian Interdisciplinary Studies* 1, no. 6 (February 28, 2026): 12–25, https://doi.org/10.65739/archipel.v1i6.34.
[21] Undang-undang (UU) Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, 2025; Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[22] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."

Number 20 of 2025, Law Number 8 of 1981, the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, the Criminal Code, and Constitutional Court Decision Number 21/PUU-XII/2014. Secondary legal materials comprise books, peer-reviewed journal articles, legal doctrines on criminal evidence, theories of digital evidence, and relevant court decisions. Tertiary legal materials include legal dictionaries and encyclopedias that provide explanations of legal terms used in the study. Legal materials are collected through library research, which involves identifying, inventorying, and classifying relevant sources according to the research questions.[23] The selection of materials is guided by their relevance to the legality of digital evidence and the procedural framework governing police investigations, with priority given to sources published between 2021 and 2026 to ensure contemporary relevance.

The analysis of legal materials is conducted qualitatively using a descriptive-analytical method. The analytical process begins with the interpretation of relevant legal norms, particularly the provisions of Law Number 20 of 2025 governing electronic evidence, the authority of investigators, and coercive measures involving digital data. The analysis proceeds by examining the relationship between formal legality and substantive reliability, assessing whether the existing framework provides adequate safeguards for privacy and due process, and identifying gaps between normative recognition and procedural implementation. Legal materials are analysed using deductive and inductive reasoning, that is, by applying general legal principles to specific provisions and by drawing generalisations from specific cases and doctrines to formulate a coherent construction of legality in digital investigations. The results of the analysis are presented in the form of a prescriptive account explaining how digital evidence should be lawfully acquired, preserved, authenticated, and presented in criminal investigations conducted by the Indonesian National Police.

RESULT AND DISCUSSION

Formal Recognition and Procedural Deficit

The enactment of Law Number 20 of 2025 marks a decisive shift in the normative status of digital evidence. Article 235 paragraph (1) letter (h) recognises electronic evidence as an independent and lawful means of proof, and Article 235 paragraph (3) conditions its admissibility on authentication and lawful acquisition.[24] This formal recognition responds to the long-standing critique that the former *KUHAP* left digital information in a normative vacuum, forcing courts to rely on the Electronic Information and Transactions Law and ad hoc judicial

[23] Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, 21st ed. (CV. Rajawali, 2022), https://jdih.dprd.sukoharjokab.go.id/koleksi-buku/791.
[24] "Undang-Undang (UU) Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Acara Pidana" (2025), https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025.

interpretation. The new framework therefore supplies the legal certainty that earlier scholarship identified as missing, including Santosa and Kamali's finding that formal admissibility without procedural standards generates persistent uncertainty.[25]

Formal recognition, however, does not automatically produce operational certainty. Article 235 paragraph (5) authorises judges to exclude evidence that is inauthentic or unlawfully obtained, yet the Code does not establish mandatory technical standards for authentication, nor does it prescribe a uniform chain-of-custody protocol. Pratama and Juhana demonstrate that digital forensic procedures remain discretionary and that the absence of a mandatory chain-of-custody standard creates what they term "authentication asymmetry," particularly in relation to synthetic or AI-generated evidence.[26] This finding qualifies the optimism surrounding Article 235 and supports the earlier warning of Hutauruk et al. that the 2025 *KUHAP* leaves the boundary between physical seizure and digital extraction undefined.[27] The result is a framework that is normatively progressive but procedurally incomplete.

Chain of Custody and Forensic Reliability

The second dimension of legality concerns the integrity of the evidentiary process. Digital data is volatile, replicable, and vulnerable to undetected alteration, so its probative value depends on a demonstrable continuity of custody from acquisition to presentation. Indonesian practice has begun to recognise this requirement, and courts have accepted digital forensic evidence where metadata and integrity records are properly documented.[28] Yet the 2025 *KUHAP* does not itself codify a chain-of-custody standard. Article 56 paragraph (1) letter (e) permits investigators to seek digital forensic assistance, but it does not prescribe certification requirements for forensic personnel, validated tools, or hash-based verification.[29]

This gap is significant because the reliability of digital evidence cannot be secured by formal admissibility alone. Anggraeniko et al. argues that the absence of explicit exclusionary rules and chain-of-custody requirements risks allowing unlawfully obtained or contaminated digital evidence to enter the trial process,

[25] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."
[26] Reggy Indra Pratama and Ujuh Juhana, "Defisit Kepastian Autentikasi Alat Bukti Elektronik Dalam Penyidikan Delik Digital Pasca-Harmonisasi UU ITE Dan KUHAP 2025," *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi* 3, no. 3 (July 22, 2026): 136–46, https://doi.org/10.62383/konstitusi.v3i3.1905.
[27] Hutauruk, Hutahaean, and Ali, "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure."
[28] Irvan Saputra and Andi Maysarah, "Implementasi Digital Forensics Dalam Pembuktian Tindak Pidana Cyber Crime Di Pengadilan Negeri Medan," *Warta Dharmawangsa* 20, no. 1 (January 25, 2026): 416–30, https://doi.org/10.46576/wdw.v20i1.8264.
[29] Undang-undang (UU) Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, 2025.

thereby undermining due process and the presumption of innocence.[30] The argument reinforces Santosa and Kamali's earlier position that courts must assess not only what digital evidence shows but also how it was obtained and preserved.[31] In this respect, the new *KUHAP* creates the normative foundation for forensic accountability but leaves its operational realisation to implementing regulations that have not yet been issued.

Privacy, Proportionality, and Judicial Oversight

The third dimension concerns the constitutional limits of digital investigation. Digital searches may expose vast quantities of personal information unrelated to the alleged offence, including communications, location history, financial records, and data belonging to third parties. Hutauruk et al. argue that the extraction of smartphone data must be treated as a distinct object of search requiring specific, relevant, and proportionate judicial authorisation, and that suspects currently lack adequate pretrial remedies when irrelevant personal data is extracted.[32] This position is consistent with the principle that investigative measures affecting fundamental rights must remain subject to judicial scrutiny.

The 2025 *KUHAP* partially accommodates this concern by empowering judges to assess the legality of evidence acquisition, but it does not establish a comprehensive authorisation regime for digital searches. Privacy protection therefore continues to depend on the discretion of investigators and the vigilance of judges. Pratama and Juhana recommend mandatory chain-of-custody standards and forensic certification as mechanisms for strengthening legal certainty while safeguarding suspects' rights.[33] The analysis suggests that judicial oversight must operate not only at trial but also at the stage of authorisation, particularly where extraction of data from devices or cloud systems may exceed the scope of the alleged offence. Without such oversight, the recognition of digital evidence may expand investigative power without a corresponding expansion of procedural safeguards.

CONCLUSION

The legal framework governing the use of digital data as evidence in criminal investigations conducted by the Indonesian National Police has undergone a

[30] Litya Surisdani Anggraeniko, Auliah Ambarwati, and Feby Reski Utami, "Admissibility of Digital Evidence in Indonesia: Criminal–Civil Implications for the Chain of Custody and Evidentiary Validity," *Priviet Social Sciences Journal* 6, no. 4 (April 22, 2026): 483–94, https://doi.org/10.55942/pssj.v6i4.1566.

[31] Giri Santosa and Ibnu Kamali, "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia."

[32] Hutauruk, Hutahaean, and Ali, "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure."

[33] Pratama and Juhana, "Defisit Kepastian Autentikasi Alat Bukti Elektronik Dalam Penyidikan Delik Digital Pasca-Harmonisasi UU ITE Dan KUHAP 2025."

significant transformation. The enactment of Law Number 20 of 2025 provides explicit normative recognition of electronic evidence, thereby offering greater legal certainty than the previous framework under Law Number 8 of 1981. However, this study finds that formal recognition is insufficient to guarantee substantive reliability. The legality of digital evidence depends on the integration of formal admissibility with substantive legality, including strict chain-of-custody procedures, verifiable forensic authentication, and adherence to privacy and due process principles. Without clear operational standards, the recognition of digital evidence risks expanding investigative powers without providing adequate safeguards for individual rights.

This study has several limitations. As a normative legal research, it relies primarily on statutory, conceptual, and analytical approaches rather than empirical data from the field. The analysis focuses on the normative construction of the 2025 *KUHAP* and its supporting regulations, but it does not measure the actual implementation of digital forensic procedures by Polri investigators. Furthermore, because Law Number 20 of 2025 is a recent enactment, many of its implementing regulations and technical guidelines have not yet been issued, limiting the ability to assess its full operational impact. Consequently, this study cannot evaluate how courts and investigators will resolve the interpretive ambiguities identified in the discussion.

Future studies should adopt empirical or socio-legal approaches to examine the practical implementation of digital evidence procedures by Polri after the issuance of the new *KUHAP*'s implementing regulations. Researchers could investigate how investigators navigate the boundary between device seizure and data extraction, how chain-of-custody standards are applied in police forensic laboratories, and how judges assess the authenticity of electronic evidence in actual court proceedings. Future research should also explore the effectiveness of pretrial review mechanisms for individuals whose personal data is affected by digital investigative measures. Building on the findings of this study, such research would contribute to the development of clearer technical standards, stronger judicial oversight, and more effective legal remedies that balance the needs of law enforcement with the protection of fundamental rights.

REFERENCES

Anggraeniko, Litya Surisdani, Auliah Ambarwati, and Feby Reski Utami. "Admissibility of Digital Evidence in Indonesia: Criminal–Civil Implications for the Chain of Custody and Evidentiary Validity." *Priviet Social Sciences Journal* 6, no. 4 (April 22, 2026): 483–94. https://doi.org/10.55942/pssj.v6i4.1566.

Constitutional Court of the Republic of Indonesia, Decision No. 21/PUU-XII/2014. (2014). https://www.mkri.id/public/content/persidangan/putusan/21_PUU-XII_2014.pdf.

Eoghan, Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet,*. 3rd ed. Academic Press, 2011. https://www.researchgate.net/publication/220691491_Digital_Evidence_and_Computer_Crime_-_Forensic_Science_Computers_and_the_Internet_3rd_Edition.

Giri Santosa, Dewa Gede, and Karell Mawla Ibnu Kamali. "Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia." *Jurnal Hukum Dan Peradilan* 11, no. 2 (July 31, 2022): 195. https://doi.org/10.25216/jhp.11.2.2022.195-218.

Hakki, Abdillah, and Sadjijono Sadjijono. "The Evidential System for The Non-Physical Offense of Sexual Harrasment." *Ius Positum: Journal of Law Theory and Law Enforcement* 3, no. 2 (June 28, 2024): 1–10. https://doi.org/10.56943/jlte.v3i2.547.

Hutauruk, Appe, Fendi Maruba Parlindungan Hutahaean, and Adalin Ali. "Smartphone Data Extraction as Digital Search: Rethinking the Limits of Pretrial Review under Indonesia's 2025 Code of Criminal Procedure." *Politica: Jurnal Hukum Tata Negara Dan Politik Islam* 13, no. 2 (September 22, 2026): 618–59. https://doi.org/10.32505/politica.v13i2.16111.

Makarim, Edmon. *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada, 2003.

Peter Mahmud, Marzuki. *Penelitian Hukum*. 19th ed. Jakarta: Kencana, 2019. https://opac.perpusnas.go.id/DetailOpac.aspx?id=1409842.

Pratama, Reggy Indra, and Ujuh Juhana. "Defisit Kepastian Autentikasi Alat Bukti Elektronik Dalam Penyidikan Delik Digital Pasca-Harmonisasi UU ITE Dan KUHAP 2025." *Konstitusi : Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi* 3, no. 3 (July 22, 2026): 136–46. https://doi.org/10.62383/konstitusi.v3i3.1905.

Saputra, Irvan, and Andi Maysarah. "Implementasi Digital Forensics Dalam Pembuktian Tindak Pidana Cyber Crime Di Pengadilan Negeri Medan." *Warta Dharmawangsa* 20, no. 1 (January 25, 2026): 416–30. https://doi.org/10.46576/wdw.v20i1.8264.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. 21st ed. CV. Rajawali, 2022. https://jdih.dprd.sukoharjokab.go.id/koleksi-buku/791.

Suarsika, I Komang, Ni Ketut Wiratny, and Erikson Sihotang. "Legal Policy on Exhibitionism Through Video Call-Based Social Media Reviewed from The Information and Electric Transacstions (IET) Law." *Ius Positum: Journal of Law Theory and Law Enforcement* 3, no. 2 (August 9, 2024): 48–61. https://doi.org/10.56943/jlte.v3i2.576.

Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2016). https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016.

Undang-undang (UU) Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (2025). https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025.

Undang-undang (UU) Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (2025). https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025.

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

Undang-undang (UU) Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (1981). https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981.

Wildan, Ambron Ritonga, and Fanitia Aditia. "Pembaruan Sistem Pembuktian Pidana Indonesia Berdasarkan KUHAP 2025." *Delicti : Jurnal Hukum Pidana Dan Kriminologi* 4, no. 1 (October 22, 2026): 163–75. https://doi.org/10.25077/DELICTI.V.4.I.1.P.163-175.2026.

Wulandari, Putri. "Normative Legal Research Methodology from the Experts' Perspective: A Comparative Analysis of Concepts and Approaches." *Archipel: Journal of Indonesian Interdisciplinary Studies* 1, no. 6 (February 28, 2026): 12–25. https://doi.org/10.65739/archipel.v1i6.34.

Xiao, Nan, Zhaoshun Wang, Xiaoxue Sun, and Junfeng Miao. "A Novel Blockchain-Based Digital Forensics Framework for Preserving Evidence and Enabling Investigation in Industrial Internet of Things." *Alexandria Engineering Journal* 86 (January 2024): 631–43. https://doi.org/10.1016/j.aej.2023.12.021.