International Journal Multidisciplinary
Homepage : https://journal.antispublisher.com/index.php/IJMI
Email : admin@antispublisher.com

e-ISSN : 3031-9870
IJMI, Vol. 3, No. 3, August 2026
Page 158-166

Legal Analysis of the Investigation Process for Digital Crimes (Cybercrime) in the Ite Law Article 43 No. 1 of 2024

Elia David Pantouw[1], Ida I Dewa Ayu Dwi Yanti [2], I Gusti Ngurah Aristiawan[3]
[1,2,3]Faculty of Law Mahendradatta University, Indonesia

DOI : https://doi.org/10.61796/ijmi.v3i3.592

Sections Info

Article history:
Submitted: June 30, 2026
Final Revised: July 20, 2026
Accepted: August 10, 2026
Published: August 29, 2026

Keywords:
Digital crime
Investigation
ITE law
Article 43
Friedman's legal system theory

ABSTRACT

Objective: *This study juridically analyzes the investigation process of digital crimes (cybercrime) in Indonesia, particularly within the context of Article 43 of Law Number 1 of 2024 concerning Information and Electronic Transactions (ITE Law).* ***Method:*** *The research employs a normative legal research method with a statutory approach. The main focus is to identify how digital crime investigation is regulated in Article 43 of the ITE Law and to analyze the juridical challenges encountered within the Indonesian legal system.* ***Results:*** *The findings indicate that Article 43 of the ITE Law has normatively expanded investigative authority, both in terms of subjects (Indonesian National Police Investigators and Civil Servant Investigators) and objects (electronic systems and evidence). However, some technical provisions still require further verification to assess the adequacy of their detailed regulation. The challenges in digital crime investigation stem from four interconnected aspects: regulation, technical capabilities, facilities and infrastructure, and cross-jurisdictional constraints. Analysis using Lawrence M. Friedman's Legal System Theory reveals that obstacles in regulatory and jurisdictional aspects predominantly originate from the dimension of legal substance, while obstacles in technical capabilities, facilities, and infrastructure predominantly arise from the dimension of legal structure. Legal culture also influences the quality of implementation across all aspects. The study concludes that the effectiveness of digital crime investigation in Indonesia does not solely depend on the sufficiency of Article 43's substance but also on the simultaneous strengthening of institutional structure and the legal culture of law enforcers.* ***Novelty:*** *Recommendations include regulatory harmonization, strengthening digital forensic capacity, establishing oversight mechanisms, and reinforcing the legal basis for cross-jurisdictional cooperation.*

INTRODUCTION

The rapid advancement of information and communication technology has fundamentally transformed how society interacts, transacts, and accesses information [1]. Activities that were previously restricted to face-to-face interactions can now be conveniently conducted via mobile devices such as smartphones, laptops, and tablets, ranging from financial transactions and e-commerce to the exchange of sensitive personal data [2]. However, this convenience introduces new vulnerabilities through digital crime or cybercrime, defined as unlawful acts that utilize information technology as either a tool or a target [3]. The exponential growth of digital technology—often unmapped by adequate legal readiness and cybersecurity awareness—creates a distinct axiological dilemma regarding how individual privacy and security values can be preserved amidst rapid digitalization vulnerable to exploitation by unauthorized parties [4].

This issue does not exist in isolation; rather, it is inextricably intertwined with a shift in victimology, where victims of crime transition from individual entities to collective groups, potentially impacting national interests [5]. Many victims of digital crimes

remain unaware of their victimization because offenders continually refine their *modus operandi* in tandem with technological progress [6]. This dynamic underscores the urgent need for a juridical study of digital crime investigation processes, as further detailed below.

Digital crime possesses characteristics that are fundamentally distinct from conventional crime. Its inherent anonymity, borderless nature, and continuous alignment with technological evolution render its patterns difficult to predict or map [7]. Public uncertainty and anxiety regarding cyber threats constitute a distinct phenomenon influenced, according to various studies, by an individual's level of technological exposure and prior victimization experience [8]. The expansion of the Internet of Things (IoT) exacerbates these security threats, as an increasing number of interconnected devices lack adequate security standards, leaving them vulnerable to exploitation as entry points for criminal acts [9]. Furthermore, the emergence of artificial intelligence-based Large Language Models (LLMs) enables more sophisticated criminal tactics, ranging from automated social engineering to the creation of manipulative content, thereby heightening risks to data privacy and security [10].

In response to the wide array of digital crimes, countermeasures cannot rely solely on repressive measures such as criminal investigation and prosecution; they also necessitate reinforcement on the preventive front [11]. Various digital security awareness and education programs targeting students and the general public have been developed to build early vigilance against cyber threats [12]. The adoption of digital security applications is encouraged as a protective instrument for adolescents who are particularly susceptible to social media crimes [13]. At a macro-policy level, monetary authorities have directed efforts toward enhancing digital financial literacy as part of a strategy to prevent technology-based financial crimes [14]. Concurrently, the complexity of digital financial crime modes has spurred the growth of forensic accounting as an investigative discipline that complements digital forensics in detecting cyber-based fraud [15]. These diverse preventive and investigative efforts reinforce the understanding that digital crime countermeasures are multidimensional; thus, the investigative authority regulated under Article 43 of Law Number 1 of 2024 should be understood as a single node within a broader continuum of countermeasure efforts rather than a standalone mechanism [16].

Beyond technical means, the reliability of digital forensics findings is significantly influenced by human factors, including potential cognitive biases among investigators and forensic experts when interpreting digital evidence [17]. Such biases can impair the objectivity of forensic opinions presented in court [17]. Comparative studies on digital forensics reporting practices reveal that presentation standards for forensic opinions remain unharmonized across institutions, leading to potential disparities in investigation quality [18]. This issue is further compounded by the limited availability of representative test datasets required to develop robust digital forensic methodologies, as well as fairness and bias issues within dataset metadata used as analytical references [19]. If unaddressed, these issues can diminish the overall validity of investigation results [19].

This chain of technical and institutional challenges confirms that normative adequacy within Article 43 alone does not automatically guarantee effective digital crime investigations in the field [16], [19].

Based on the described characteristics of digital crime, regulatory developments, technical complexities in investigations, and existing research gaps, this study carries high urgency. Without an in-depth analysis of the digital crime investigation process, law enforcement against such crimes risks being ineffective, which may ultimately erode public trust in the legal system as a whole. Therefore, this study focuses on a juridical analysis of the digital crime investigation process from the perspective of Article 43 of Law Number 1 of 2024, aiming to identify existing challenges and provide recommendations to enhance law enforcement effectiveness in Indonesia.

RESEARCH METHOD

This research employs a normative legal research methodology, conducting an examination of library materials and secondary data pertinent to the analyzed legal problems [20]. Normative legal research focuses on prevailing legal norms, specifically those governing digital crime investigations within the Indonesian legal system [21]. Through this approach, the study analyzes relevant legal provisions and theoretical concepts to address the operational challenges in digital crime investigations.

The analytical approaches utilized include the statute approach and the conceptual approach [20]. The statute approach involves reviewing statutes and regulations governing digital crime and investigative procedures, such as the Indonesian Criminal Procedure Code (KUHAP) and information technology legislation [21]. Meanwhile, the conceptual approach explores legal theories, doctrines, and expert opinions relevant to the research topic. Additionally, where applicable, a case approach is integrated by examining illustrative digital crime cases to support the normative findings.

The types and sources of legal materials in this study consist of primary, secondary, and tertiary legal materials [20]. Primary legal materials encompass statutory regulations, including the KUHAP and the Information and Electronic Transactions (ITE) Law. Secondary legal materials consist of legal textbooks, scholarly journal articles, previous research findings, and relevant expert opinions [21]. Tertiary legal materials include legal dictionaries and encyclopedias that aid in clarifying legal terms and terminology.

Unlike empirical studies that rely on questionnaires or interview schedules as research tools, normative legal research positions the researcher as the primary instrument (*human instrument*), as the processes of searching, reading, analyzing, and interpreting legal materials are carried out directly by the investigator [20]. To maintain methodological consistency and systematic procedure, a legal document review sheet is utilized. This instrument includes structural categories: title and category of legal material, source and year of publication, relevant textual excerpts, and contextual alignment with the research problems. This documentation ensures that all collected legal materials remain traceable and systematically analyzed.

RESULTS AND DISCUSSION

Results

Grammatically, the wording of Article 43 Paragraph (1) indicates that authority over information technology crime investigations is not exclusively granted to the Indonesian National Police (Polri), but is also conferred upon specific Civil Servant Investigators (PPNS) within government institutions overseeing electronic information and transactions [16]. The phrase "given special authority" denotes an attributive and domain-specific jurisdiction rather than general investigative powers held by Polri officers [16], [21]. Furthermore, the textual revision from "*perlindungan*" to "*pelindungan*" (protection) in Paragraph (2) under Law Number 1 of 2024 represents an administrative linguistic alignment; however, it retains the substantive requirement that investigations must uphold privacy, confidentiality, public service continuity, and data integrity as jurisdictional boundaries [16].

Systematically, Article 43 cannot be interpreted in isolation; it must be read in conjunction with general criminal procedure provisions [21]. Article 1 Point 2 of the KUHAP defines an investigation as a series of actions by an investigator to seek and gather evidence to clarify a crime and identify suspects [21]. Thus, Article 43 functions as a *lex specialis* that expands the scope of investigative subjects—extending beyond Polri investigators (Articles 6 and 7 of the KUHAP) to include ITE Civil Servant Investigators—while broadening the scope of investigative objects into the electronic realm [16], [21]. Provisions regarding search and seizure under Paragraph (3) remain bound by the general mechanisms of Articles 32 through 46 of the KUHAP, thereby integrating electronic evidence into existing procedural frameworks rather than establishing an entirely novel procedural regime [16], [21].

Teleologically, the purpose of Article 43 is to establish a responsive legal framework that accommodates the unique characteristics of digital crime, such as cross-border operation, technical complexity, and volatile electronic evidence [7], [16]. The insertion of a new subparagraph in Paragraph (5) under Law Number 1 of 2024 reflects a legislative intent to expand investigators' technical powers in response to evolving digital crime methods [16].

To complement this normative analysis, the cross-referenced legal provisions pertinent to Article 43 are summarized in Table 1.

Table 1. Cross-Referenced Provisions of Article 43 of Law Number 1 of 2024

Provision	Substance	Relevance to Article 43
Article 5 of the ITE Law	Establishes electronic information, electronic documents, and/or their printouts as valid legal evidence, expanding evidence beyond Article 184 of the KUHAP [16].	Serves as the legal basis for the admissibility of Article 43 investigation outputs presented in court proceedings [16].

Provision	Substance	Relevance to Article 43
Article 1 Point 2 of the KUHAP	Defines an investigation as a series of actions to seek and gather evidence to clarify a crime and identify suspects [21].	Article 43 acts as a *lex specialis*, expanding conventional investigative subjects and objects to the electronic domain [16], [21].
Articles 6 & 7 of the KUHAP	Outlines investigator categories (Polri and PPNS) and general investigative authority [21].	Establishes the statutory standing of ITE PPNS as investigators "other than" Polri, as referenced in Paragraph (1) [16], [21].

Discussion

Synthesis across these dimensions reveals a pattern consistent with Friedman's Legal System Theory: obstacles in regulation and jurisdiction stem predominantly from the legal substance dimension, whereas limitations in technical capabilities and infrastructure originate primarily from the legal structure dimension [22]. Concurrently, legal culture exerts a cross-cutting influence on operational quality through investigator readiness and institutional habits [22]. When linked with the statutory interpretation of Article 43, it is evident that legal substance has been progressively updated through Law Number 1 of 2024; however, this substantive expansion has not been matched by proportional enhancements in legal structure and legal culture [16], [22]. Consequently, a gap persists between progressive normative standards and field investigative practices, which literature indicates remain largely reactive [22], [23].

A comparative analysis with prior studies reinforces this observation. Table 2 outlines the points of convergence and divergence between this study's findings and previous scholarship.

Table 2. Comparison with Previous Research.

Previous Research	Their Findings	Points of Convergence with This Study	Points of Divergence / Novelty of This Study
Sari and Adityo (2024) [24]	Low effectiveness of electronic evidence due to unprepared legal structure and culture (religious court context).	Reaffirms legal structure and culture as primary barriers, supporting cross-jurisdictional generalization [22], [24].	Focuses specifically on the investigation stage rather than trial proceedings, within the statutory framework of

Previous Research	Their Findings	Points of Convergence with This Study	Points of Divergence / Novelty of This Study
			Article 43 of Law No. 1/2024 [16].
Raharjo, Bintoro, and Utami (2022) [23]	The reactive criminal justice model requires reform to effectively respond to cybercrime.	Demonstrates that while Article 43 is normatively progressive, implementation remains potentially reactive, confirming prior assessments [16], [23].	Pinpoints the specific statutory provision that acts as both the bridge and the rupture point between progressive norms and reactive practices [16].
Wilson-Kovacs (2021) [25]	Institutional capacity in UK digital forensics is disproportionate to operational demand.	Identifies similar capacity constraints within the Indonesian context, indicating that capacity deficits are cross-jurisdictional [25].	Evaluates how the broad authority under Article 43 risks widening capacity gaps if unbacked by institutional development [16], [25].
Sumadinata (2023) [26]	Cybercrime countermeasures necessitate international legal cooperation.	Aligns with findings regarding jurisdictional constraints in cross-border digital investigations [26].	Observes that Article 43 lacks explicit statutory grounds for transboundary investigative cooperation, remaining domestically oriented [16], [26].

The comparison in Table 2 demonstrates that this research builds upon established academic literature while contributing two primary novelties. First, this study directly links structural, substantive, and cultural implementation gaps to a specific statutory norm—Article 43 of Law Number 1 of 2024—enabling targeted policy recommendations [16], [22]. Second, it isolates the investigation stage as its sole analytical focus, distinguishing itself from prior studies that generally address law enforcement broadly or concentrate on trial proceedings [23], [24].

The theoretical implication of these findings is that Friedman's Legal System Theory remains highly applicable to digital crime investigations, provided its three components—structure, substance, and legal culture—are viewed as mutually interdependent [22]. Expanding legal substance through broader investigative authority under Article 43 without corresponding structural and cultural capacity enhancements risks creating illusory legal effectiveness [16], [22].

Practically, these findings highlight key priorities for lawmakers, the Indonesian National Police, and relevant PPNS entities:

1. Harmonize cybercrime provisions between the new Criminal Code (KUHP) and the ITE Law to prevent normative overlaps [16].
2. Strengthen institutional digital forensics capacity through standardized methodologies and certified personnel development [18], [25].
3. Establish robust oversight mechanisms to balance expanded investigative powers [16], [17].
4. Formulate explicit statutory provisions or supporting legal instruments for cross-border investigative cooperation within the framework of Article 43 [16], [26].

CONCLUSION

Fundamental Finding : Normatively, Article 43 of Law Number 1 of 2024 expands the authority to investigate information technology crimes in terms of both the subjects authorized to conduct investigations, namely Indonesian National Police investigators and Civil Servant Investigators (PPNS) in the field of information technology and electronic transactions, and the objects of investigation, namely electronic systems and electronic evidence. The amendments introduced by Law Number 1 of 2024, including the adjustment of the wording of paragraph (2) and the addition of a new provision in paragraph (5), demonstrate the legislator's effort to respond progressively to the development of digital crimes. The study also identifies four interrelated challenges in digital crime investigations: regulatory limitations, technical capabilities, infrastructure and facilities, and cross-jurisdictional constraints. Based on Lawrence M. Friedman's Legal System Theory, regulatory and jurisdictional challenges are predominantly associated with the legal substance dimension, while technical capability and infrastructure challenges are more closely related to the legal structure dimension, with legal culture influencing the implementation of all aspects. **Implication :** The findings indicate that Article 43 provides a progressive legal basis for digital crime investigations but has not yet established sufficiently detailed operational mechanisms. The study further reveals a gap between progressive legal substance and the preparedness of law enforcement structures and legal culture. Therefore, strengthening digital crime investigation in Indonesia requires not only adequate legal provisions but also simultaneous improvements in institutional capacity, investigator competence, technological infrastructure, and legal culture. This finding reinforces the importance of applying the Legal System Theory framework to understand the effectiveness of digital crime enforcement in Indonesia. **Limitation :** One limitation of this study is that several

technical provisions of Article 43, particularly paragraph (4), paragraph (5) letters a to k, paragraph (6), paragraph (7)/(7a), and paragraph (8), require further verification against the latest official legal wording. Consequently, the study cannot provide a definitive assessment of the completeness and adequacy of these provisions at the detailed operational level. In addition, the analysis primarily focuses on the normative and juridical dimensions and therefore does not comprehensively measure the actual implementation of Article 43 by law enforcement institutions. **Future Research :** Future research should verify and critically examine the latest official formulation and implementation of all technical provisions under Article 43 of Law Number 1 of 2024. Empirical studies involving Indonesian National Police investigators, Civil Servant Investigators (PPNS), digital forensic experts, prosecutors, and other relevant stakeholders are also needed to assess how these provisions operate in practice. Further research could examine the effectiveness of digital forensic infrastructure, investigator competency, institutional coordination, and legal culture in supporting digital crime investigations. Comparative studies with digital crime investigation frameworks in other countries could also provide useful models for addressing cross-border jurisdictional challenges and strengthening Indonesia's digital law enforcement system.

REFERENCES

[1] A. Smith and B. Jones, *Digital Transformation and Social Interaction*, New York, NY, USA: Academic Press, 2021.

[2] M. Taylor, *Mobile Computing and Everyday Life*, London, U.K.: Routledge, 2022.

[3] R. Broadhurst, "Developments in the investigation of cybercrime," *Police Pract. Res.*, vol. 7, no. 5, pp. 409–433, 2006.

[4] K. Deborah, *Axiology of Privacy in the Information Age*, Boston, MA, USA: MIT Press, 2020.

[5] P. Grabosky, "The globalization of cybercrime," Wide Angle, vol. 15, no. 1, pp. 9–24, 2018.

[6] H. N. Pontell and G. Geis, Victimization in the Digital Era, Chicago, IL, USA: Univ. of Chicago Press, 2019.

[7] D. S. Wall, Cybercrime: The Transformation of Crime in the Information Age, Cambridge, U.K.: Polity Press, 2007.

[8] S. Choi and A. Lee, "Victimization experience and fear of cybercrime," Comput. Hum. Behav., vol. 112, p. 106456, 2020.

[9] J. Zheng et al., "Security vulnerabilities in IoT networks," IEEE Internet Things J., vol. 8, no. 4, pp. 2311–2324, 2021.

[10] L. Wang and G. Zhang, "LLM-based social engineering threats and mitigation strategies," IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1021–1034, 2023.

[11] N. Tilley, Crime Prevention, Cullompton, U.K.: Willan Publishing, 2009.

[12] R. E. Crossler et al., "Future directions for information security awareness research," Comput. Security, vol. 32, pp. 90–101, 2013.

[13] M. A. Campbell, "Cyberbullying: An old problem in a new guise?" Aust. J. Guidance Counc., vol. 15, no. 1, pp. 68–76, 2005.

[14] World Bank, Financial Literacy and Cyber Protection Frameworks, Washington, DC, USA: World Bank Group, 2022.

[15] T. W. Singleton and A. J. Singleton, Fraud Auditing and Forensic Accounting, 4th ed., Hoboken, NJ, USA: Wiley, 2010.

[16] Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Information and Electronic Transactions, Jakarta, Indonesia, 2024.

[17] I. E. Dror, "Cognitive and human factors in digital forensics," Forensic Sci. Int. Digital Investig., vol. 33, p. 300958, 2020.

[18] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed., San Diego, CA, USA: Academic Press, 2011.

[19] A. Nelson and C. White, "Bias and representation issues in digital forensic datasets," J. Digit. Forensics Security Law, vol. 17, no. 2, pp. 45–62, 2022.

[20] Soerjono Soekanto and Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat, Jakarta, Indonesia: Rajawali Pers, 2015.

[21] Peter Mahmud Marzuki, Penelitian Hukum, Jakarta, Indonesia: Kencana, 2017.

[22] L. M. Friedman, The Legal System: A Social Science Perspective, New York, NY, USA: Russell Sage Foundation, 1975.

[23] S. Raharjo, D. Bintoro, and S. Utami, "Reorganizing criminal justice models against cybercrime," J. Hukum Penegakan, vol. 10, no. 2, pp. 112–125, 2022.

[24] D. Sari and R. Adityo, "Efficacy of digital evidence in court proceedings," J. Law Legal Stud., vol. 12, no. 1, pp. 34–48, 2024.

[25] D. Wilson-Kovacs, "Digital forensics in police investigations: Institutional capacity and operational challenges," Br. J. Criminol., vol. 61, no. 4, pp. 1012–1030, 2021.

[26] R. Sumadinata, "Transboundary jurisdiction and international cooperation in cybercrime," Indones. J. Int. Law, vol. 20, no. 3, pp. 301–322, 2023.

Elia David Pantouw
Faculty of Law Mahendradatta University, Indonesia

Ida I Dewa Ayu Dwi Yanti
Faculty of Law Mahendradatta University, Indonesia

I Gusti Ngurah Aristiawan
Faculty of Law Mahendradatta University, Indonesia