



Digital Evidence Challenges in Cybercrime Enforcement under the 2023 Criminal Code

*Lonna Yohanes
Lengkong

Universitas Kristen Indonesia,
Indonesesia

Hendri Jayadi

Universitas Kristen Indonesia,
Indonesia

***Corresponding author:**

Lonna Yohanes Lengkong, Universitas
Kristen Indonesia,
Indonesesia. ✉yohanes.lengkong@uki.ac.id

Article Info:

Article history:

Received: June 29, 2026

Revised: August 26, 2026

Accepted: September 10, 2026

Available Online: September 29,
2026

Keywords:

Cybercrime; Chain of Custody;
Digital Evidence; Criminal Code
2023; Exclusionary Rule



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Politeknik Siber Cerdika International

Abstract

Background: The enactment of the new Criminal Code (Law No. 1 of 2023) represents a significant transformation in Indonesia's criminal law system, particularly through the integration of cybercrime offenses into the substantive criminal law framework.

Objective: This study aims to analyze the dogmatic construction of cybercrime offenses under the 2023 Criminal Code and identify challenges in the management of digital evidence within criminal justice practices following the implementation of the 2025 Criminal Procedure Code (Law No. 20 of 2025).

Methods: This research employs a normative-empirical legal method using statutory, conceptual, and comparative approaches.

Results: The study reveals an imbalance within Indonesia's criminal law system based on Lawrence M. Friedman's legal system theory. While the substantive dimension has developed through modern cybercrime regulations, the structural and cultural dimensions remain limited due to inadequate forensic capacity and digital literacy among legal practitioners. Challenges include the volatility of digital evidence, cross-border retrieval of cloud-stored data, and the application of exclusionary rules when chain-of-custody procedures are defective. Supreme Court Decision No. 1089 K/Pid.Sus/2018 illustrates these systemic challenges. Comparative analysis with *Wet computercriminaliteit III* in the Netherlands highlights the need for integrated legal reform.

Conclusion: Harmonization between substantive and procedural reforms is required through the development of electronic evidence guidelines, standardization of digital forensic procedures, accelerated Mutual Legal Assistance (MLA) mechanisms for cross-border data preservation, and modernization of legal education curricula.

To cite this article: Lengkong, L. Y., & Jayadi, H. (2026). Digital evidence challenges in cybercrime enforcement under the 2023 criminal code. *Journal of Law & Social Politics*, 4(4), 819-830. <https://doi.org/10.59261/jlsp.v4i4.160>

INTRODUCTION

The enactment of Law Number 1 of 2023 concerning the Criminal Code (hereinafter referred to as the 2023 Criminal Code) represents a historic milestone in the reform of national criminal law. As a codification that replaces the *Wetboek van Strafrecht* (WvS), which had been in effect for more than a century, the 2023 Criminal Code responds to an inevitable criminological reality: the *locus delicti* of crime has massively migrated from physical space to cyberspace. The speed of this migration consistently surpasses the adaptability of law enforcement institutions and regulatory frameworks. Clough (2010) argues that the unique characteristics of cyberspace,

including its borderlessness, instantaneous communication, and technical complexity, create fundamental challenges for criminal law systems grounded in territorial sovereignty and principles of physical causation.

The urgency of this study is supported by empirical data demonstrating a significant escalation of threats. The National Cyber and Crypto Agency (BSSN) recorded no fewer than 5.5 billion anomalous traffic events or cyberattacks throughout 2025, a figure that this article retains as a figure attributed to BSSN projections as reported by the media (BSSN, 2024). On the law enforcement side, the Indonesian National Police (Polri) uncovered 4,210 cybercrime cases throughout 2023, a figure that decreased to 3,331 cases in 2024, while case resolution showed a significant increase. Despite this positive trend, the case-resolution ratio remains below 65% of the total cases uncovered, indicating that structural obstacles in handling cybercrime cases have not been addressed systematically.

The paralysis of the National Data Center (PDN) due to a ransomware attack in mid-2024, which disrupted more than 200 essential public services, provides clear evidence of the vulnerability of national digital infrastructure to asymmetric attacks. This incident not only highlighted weaknesses in the security system but also exposed the jurisdictional impasse encountered when law enforcement officers attempt to track perpetrators operating from outside Indonesia's sovereign territory. Cloud-based evidence presents unique forensic challenges, including multitenancy, data volatility, and complex jurisdictional arrangements that undermine conventional chain-of-custody protocols. This incident was not merely a technical failure; it exposed the absence of formal procedural instruments capable of securing cross-border evidence in real time, a normative gap that forms the analytical focus of this article.

Cyber threats do not exclusively target public infrastructure; in a more complex dimension, modern cybercrime also infiltrates financial systems through the exploitation of virtual assets and decentralized financial networks, extending investigative challenges into the realm of transnational money laundering.

Contemporary cybercrime is often intertwined with money laundering (*TPPU*) through the use of virtual assets, cryptocurrencies, and decentralized finance (DeFi). The pseudonymous, decentralized, and cross-border characteristics of crypto assets allow criminals to obscure transaction trails, making the investigative process extremely complex, even for experienced law enforcement officers (Nelson et al., 2024). Brenner (2012) further notes that the transnational dimension of cybercrime fundamentally challenges the Westphalian concept of state jurisdiction, as acts committed in one jurisdiction may produce harm in another, often simultaneously across multiple legal systems.

A comparison with countries rooted in civil law traditions, such as the Netherlands, provides a valuable critical perspective. Through the enactment of *Wet computercriminaliteit III* (effective March 1, 2019), the Netherlands simultaneously and synergistically reformed both substantive and procedural law. Dutch law enforcement officers are now equipped with modern investigative instruments such as *hackbevoegdheid* (the legal authority to hack with judicial authorization) and *netwerkzoeking* (network searches of external servers) (Van Roomen, 2025). Politou (2019) observes that the Dutch legislative approach reflects a conscious policy choice to ensure that procedural instruments evolve in tandem with substantive offense definitions, thereby preventing the emergence of the enforcement gap that currently afflicts Indonesia.

In contrast to Indonesia, the Netherlands has resolved the synchronization challenge that currently constitutes one of the most critical weaknesses of Indonesia's criminal law system—a disparity that illuminates how far Indonesia must travel to achieve comparable enforcement effectiveness.

This framework is selected because it enables an analysis of cybercrime enforcement not only from the perspective of substantive legal norms but also from the dimensions of institutional capacity and legal culture that determine the effectiveness of digital evidence implementation.

To map the novelty of this article, four of the most relevant previous studies were identified. Suseno et al. (2025) analyzed the dogmatic transformation of cybercrime from *lex specialis* (the Electronic Information and Transactions Law) to *lex generalis* (the 2023 Criminal Code) and mapped potential normative conflicts but neglected the practical implications of evidentiary mechanisms and the exclusionary-rule doctrine. Prasetyo (2025) evaluated the

effectiveness of cybercrime regulation from a legislative-policy perspective without delving into a micro-level analysis of dogmatic constructions. Yasir (2025) analyzed digital evidence within the evidentiary system of the Criminal Procedure Code before the 2025 KUHAP came into force, leaving a critical gap regarding the strict exclusionary implications of Article 235. Suseno et al. (2025) also illuminated normative and technical gaps in digital evidence implementation, including chain-of-custody issues and limited forensic capacity, but did not analyze the implications of the exclusionary-rule doctrine under the 2025 Criminal Procedure Code.

The research gap is thus clear: no comprehensive study has simultaneously analyzed the interaction between the dogmatic construction of cybercrime offenses in the 2023 Criminal Code and the new evidentiary regime of the 2025 Criminal Procedure Code. The novelty of this study lies in the simultaneous integration of substantive legal analysis and procedural legal analysis, combined with a normative-empirical and comparative approach. Specifically, this article addresses three main questions: (1) How does the dogmatic construction of cybercrime offenses in the 2023 Criminal Code respond to the development of digital crime? (2) What are the legal and technical forensic challenges in proving digital evidence in court, particularly in the context of the 2025 Criminal Procedure Code? (3) What is the direction of criminal procedural law reform, and what institutional capacity is needed to bridge this asymmetry?

METHOD

This study employed a normative-empirical legal research design. The normative dimension rested on a systematic analysis of legislative substance, encompassing the construction of legal norms, principles, and doctrines, while the empirical dimension examined the extent to which these norms were implemented and the challenges they faced in law enforcement practice. This methodological combination was consistent with the legal research paradigm that emphasizes understanding law not merely as a dead text but within its dynamic socio-practical context (Mahmud Marzuki, 2017).

Three approaches were applied synergistically. First, a statutory approach analyzed the 2023 Criminal Code (Law No. 1 of 2023), particularly Articles 258, 332, and 333–335, and the 2025 Criminal Procedure Code (Law No. 20 of 2025), particularly Article 235, along with the Electronic Information and Transactions Law (Law No. 19 of 2016 *jo.* Law No. 11 of 2008). Second, a conceptual approach analyzed the doctrines of *mens rea*, *actus reus*, chain of custody, the exclusionary rule, and the fruit-of-the-poisonous-tree doctrine in the digital context. Third, a comparative approach compared the Indonesian legal framework with the Dutch *Wet computercriminaliteit III* and Criminal Code, given the shared civil law tradition adopted by both countries.

The primary legal materials analyzed included Law No. 1 of 2023, Law No. 20 of 2025, the ITE Law, Supreme Court Decision No. 1089 K/Pid.Sus/2018, Supreme Court Decision No. 661 K/Pid.Sus/2019, Supreme Court Decision No. 5084 K/Pid.Sus/2022, and the Budapest Convention on Cybercrime. Secondary legal materials included Scopus- and Sinta-indexed scientific journals, criminal law textbooks, and official reports from BSSN and the Indonesian National Police. Data were analyzed qualitatively using legal interpretation techniques, including grammatical, systematic, historical, and teleological interpretation. The empirical findings of this study were illustrative in nature and served to strengthen the normative arguments rather than constitute definitive statistical generalizations, given the still-limited access to comprehensive published cybercrime verdict databases. This study did not involve human or animal participants and therefore did not require ethical approval; all data were collected in accordance with applicable institutional ethical standards. *Pasal 235 ayat (1) UU No. 20 Tahun 2025 sebagaimana dimuat dalam Lembaran Negara Republik Indonesia Tahun 2025*, was confirmed through Hukumonline.

RESULTS AND DISCUSSION

Result

Dogmatic Construction of Cybercrime Offenses in the 2023 Criminal Code

The codification of cybercrime offenses in Law No. 1 of 2023 represents a fundamental dogmatic transformation of the national criminal law system. Systematically, the 2023 Criminal

Code places cybercrime offenses within Chapter VIII, *Criminal Acts Endangering Public Security*, specifically Part Five, concerning *Criminal Acts against Informatics and Electronics*. This placement reflects a clear dogmatic choice: criminal law no longer limits its protection solely to tangible property but also recognizes information, electronic systems, and related digital interests as objects of legal protection deserving of state protection. From the perspective of normative hierarchy, the cybercrime provisions of the ITE Law, particularly Articles 30 and 46 concerning illegal access and Articles 31 and 47 concerning illegal interception, were explicitly repealed and recodified through the 2023 Criminal Code. The applicable principles include *lex posterior derogat legi priori* and, where appropriate, *lex specialis derogat legi generali*: the ITE Law remains operative with respect to provisions not incorporated into the 2023 Criminal Code, including provisions governing certain forms of electronic information and electronic transactions, while Articles 332 and 258 of the 2023 Criminal Code now provide the principal normative framework for the corresponding cybercrime offenses.

This protection rests on the global information-security paradigm known as the CIA triad: Confidentiality, Integrity, and Availability. The principal provisions of the 2023 Criminal Code relevant to cybercrime encompass several distinct clusters. The first concerns Illegal Access (Article 332), which criminalizes unauthorized access to computers and/or electronic systems, including access involving the circumvention, penetration, exceeding, or defeat of security mechanisms—conduct broadly corresponding to computer intrusion or hacking in international terminology. the statutory concept of unauthorized access must be carefully constructed to distinguish genuine intrusion from permitted network exploration, a nuance that the 2023 Criminal Code addresses through the formulations “without right” and “unlawfully” (*tanpa hak* or *melawan hukum*). The second cluster comprises Articles 333–335, which regulate specific forms of unauthorized use of or access to computers and electronic systems, particularly conduct affecting national defense information, government systems, protected systems, financial institutions, and protected government information. These provisions therefore should not be characterized simply as a general category of “data and system interference”; rather, they establish specialized offenses involving unauthorized access and use directed at particularly protected systems and information. The third cluster concerns Illegal Interception under Article 258, which prohibits the unlawful interception, recording, diversion, alteration, obstruction, and/or monitoring of transmissions of non-public Electronic Information and/or Electronic Documents and constitutes the recodified successor to the relevant interception provisions of the ITE Law, while being placed in Chapter VIII of the 2023 Criminal Code (Suseno et al., 2025).

The most prominent distinguishing characteristic of these cybercrime offenses lies in the construction of the elements of fault (*mens rea*) and the physical elements of the offenses (*actus reus*). Article 332 expressly requires intentional conduct and the absence of legal authorization or the presence of unlawfulness, reflected in the statutory formulations “without right” and “unlawfully.” In the digital dimension, intent cannot ordinarily be observed directly; it must instead be reconstructed from the surrounding circumstances and, where relevant, from digital traces, including malicious scripts, code injection, access logs, command histories, or other technical artifacts. Likewise, unlawful access is not established merely by demonstrating that a connection to a computer or electronic system occurred; the prosecution must establish the legally relevant circumstances surrounding the access, including whether it was unauthorized and whether the statutory requirements of the particular offense were satisfied. In this sense, digital conduct challenges conventional conceptions of physical evidence because the relevant evidentiary traces may exist as volatile data, metadata, logs, or other information that has no immediately perceptible physical form (Casey, 2011).

A particularly critical interpretive challenge within the dogmatic construction of Article 332 concerns the boundaries of the element “without right” (*tanpa hak*) in scenarios involving insider threats—perpetrators who possess legitimate access credentials but exceed their authorized scope of use. Unlike conventional criminal law, where the *wederrechtelijk* element is typically established through the absence of a legal entitlement, digital systems frequently grant technical access to authorized users whose subsequent actions may transgress organizational boundaries without necessarily constituting a clear-cut intrusion. Supreme Court Decision No. 5084 K/Pid.Sus/2022 illustrates this normative boundary precisely: the Court held that an

employee who transferred company data to a personal email account for legitimate work purposes did not fulfill the *wederrechtelijk* element under Article 32(2) of the ITE Law, as the act lacked the requisite criminal intent (*mens rea*). Transposed to the 2023 Criminal Code framework, this ruling highlights an urgent need for legislative and judicial clarity regarding Article 332: Indonesian courts will increasingly face cases in which the line between authorized access and criminal intrusion is determined not solely by the technical act itself but also by the actor's authorization, purpose, and circumstances, a standard that demands substantially greater evidentiary sophistication than conventional criminal prosecution.

A strong structural correspondence exists between the cybercrime architecture of the 2023 Criminal Code and the Dutch Cybercrime Code. Article 332 of the 2023 Criminal Code corresponds broadly to *computervredebreek* (Article 138ab WvS), while Articles 333–335 correspond to specialized offenses concerning unauthorized use of or access to computers and electronic systems under the Dutch framework, including provisions historically associated with *vernietiging van computergegevens* (Article 350a WvS). This normative convergence is influenced by the Budapest Convention on Cybercrime, which Indonesia has not yet ratified but may use as a comparative and normative reference. Although Indonesia has not ratified the Budapest Convention, the instrument may function as a form of soft-law reference in the development and interpretation of domestic cybercrime norms, as evidenced by structural similarities between Articles 332 and 258 of the 2023 Criminal Code and Articles 2–6 of the Budapest Convention on Cybercrime. Clough (2010) documents that countries adopting Budapest Convention standards consistently demonstrate greater evidentiary success in cross-border cybercrime prosecutions than those relying solely on domestic frameworks.

Position of Digital Evidence in the 2025 Criminal Procedure Code

Prior to the enactment of the 2025 Criminal Procedure Code, criminal law enforcement faced the reality that the previous Criminal Procedure Code (Law No. 8 of 1981) did not expressly accommodate digital evidence within its evidentiary framework. Judicial and law-enforcement practice sought to bridge this gap by expanding the evidentiary significance of electronic information through Article 5 of the ITE Law, an ad hoc solution that nevertheless generated continuing questions concerning evidentiary status, authenticity, and procedural safeguards.

The 2025 Criminal Procedure Code (Law No. 20 of 2025) addresses this lacuna directly. Through Article 235(1), *bukti elektronik* (electronic evidence) is expressly recognized as an independent category of admissible evidence alongside witness testimony, expert testimony, documentary evidence, the defendant's statement, physical evidence, judicial observation, and other material capable of being used for evidentiary purposes, provided that it is obtained lawfully. Article 235 further requires that evidence be capable of authentication and be obtained lawfully, while authorizing judges to assess authentication and the legality of its acquisition. This represents a significant normative development. Critically, however, although Article 235 expressly establishes an exclusionary mechanism for evidence that is unauthenticated or unlawfully obtained, the *fruit of the poisonous tree* doctrine is not expressly elaborated as an independent doctrine within the provision itself.

Ali Murtadho (2025) assert that the application of the exclusionary rule in Indonesia had previously been sporadic due to a normative vacuum. The 2025 Criminal Procedure Code provides a more solid foundation for protecting suspects' human rights but simultaneously demands standardization of law-enforcement procedures that are not yet widely available. Pollitt (2020) emphasizes that any evidentiary regime that formally incorporates digital evidence must be accompanied by mandatory forensic handling standards; without such standards, the exclusionary rule may function as a mechanism that inadvertently privileges technically sophisticated defendants over effective prosecution.

Digital evidence has inherently volatile characteristics: it may be modified, duplicated without alteration of the original, or destroyed remotely within seconds through techniques such as remote wiping. Its evidentiary value is therefore highly dependent on the integrity of the retrieval, preservation, examination, and storage processes, specifically the unbroken maintenance of the chain of custody. Casey (2011) defines the chain of custody as the documented and unbroken sequence of possession, transfer, analysis, and disposition of evidence,

encompassing continuous documentation from identification and preservation through forensic acquisition, laboratory analysis, and court presentation. Even minor investigative actions may unexpectedly alter digital evidence, including situations in which Internet-connected devices initiate automatic system processes after seizure (Quick and Choo, 2018).

A comparative doctrinal question of considerable significance is whether Article 235(1) of the 2025 Criminal Procedure Code establishes a sufficient threshold of scientific reliability for the admission of digital evidence, or whether Indonesia continues to operate under a system of judicial evaluation in which judges retain substantial discretion to assess electronic evidence without detailed statutory reliability criteria. In the United States common-law tradition, the Daubert standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 1993) imposes a gatekeeping obligation on judges to evaluate whether scientific evidence is based on sufficient facts, reliable methodology, and reliable application, effectively constituting a judicially enforced scientific-reliability threshold. Article 235(1) of the 2025 Criminal Procedure Code, while recognizing electronic evidence as a valid independent category and requiring authentication and lawful acquisition, does not expressly codify a reliability framework equivalent to Daubert. This represents a significant normative gap: although the new provision establishes statutory requirements of authentication and lawful acquisition, the assessment of scientific reliability in digital-forensic evidence remains substantially dependent on judicial competence, expert testimony, and the development of consistent interpretive standards.

Empirical Illustration: Supreme Court Decision No. 1089 K/Pid.Sus/2018

Supreme Court Decision No. 1089 K/Pid.Sus/2018 provides a concrete illustration of this systemic problem. In that case, the defendant was charged under Article 28(2) *jo.* Article 45A(2) of the ITE Law (Law No. 19 of 2016) for allegedly disseminating hate speech through a Facebook account. The panel of justices at the cassation level rejected the prosecutor's Facebook screenshot evidence because the prosecutor failed to establish the authenticity of the account through adequate digital-forensic examination. The absence of sufficiently reliable digital-forensic verification of the evidence and its chain of custody rendered the electronically obtained evidence procedurally deficient, despite its substantive relevance to the case.

This decision exemplifies a pattern increasingly documented in Indonesian cybercrime adjudication: technically relevant digital evidence may be excluded or accorded diminished evidentiary weight not necessarily because its substantive content is unreliable, but because deficiencies exist in the process by which the evidence was acquired, authenticated, preserved, or presented. The panel's approach may be understood, in effect, as reflecting an emerging exclusionary-rule framework that anticipated the more explicit codification of evidentiary legality in the 2025 Criminal Procedure Code. This demonstrates that even before formal codification, Indonesian courts had begun applying procedural-integrity standards to digital evidence, creating a *de facto* enforcement gap for investigators without adequate forensic training.

The disparity in digital literacy among law-enforcement officials often makes it difficult for judges to assess complex technical claims. In the courtroom, a battle of experts is becoming increasingly commonplace: defense counsel may dispute the validity of investigators' extraction methods—for example, by alleging changes in hash values indicating possible data modification after seizure, or by highlighting inconsistencies with international standards such as ISO/IEC 27037. If judges doubt the integrity of the chain of custody, then, based on the principle of *in dubio pro reo*, digital evidence may be disregarded or accorded insufficient evidentiary weight to support a finding of guilt.

Comparative Analysis: Wet computercriminaliteit III (Netherlands) vs. Indonesian Framework

The systemic failure illustrated by Supreme Court Decision No. 1089 K/Pid.Sus/2018 is not without comparative precedent. The Netherlands, having confronted analogous enforcement challenges, offers an instructive model of legislative solutions that Indonesia would do well to study.

The Netherlands provides the most relevant comparative reference within the civil-law tradition. Through *Wet computercriminaliteit III*, which entered into force on March 1, 2019,

Dutch criminal procedure law introduced highly specific and adaptive digital-investigation instruments. Politou (2019) identifies four key innovations of this legislation.

First, *netwerkzoekende* (network search): law-enforcement officers may, subject to statutory conditions and the requisite authorization, search not only seized devices but also remotely connected computers and systems. This power directly addresses the cross-border and cloud-computing problems that Indonesian investigators face in cases involving geographically dispersed digital infrastructure, including cases such as the 2024 PDN ransomware incident.

Second, *hackbevoegdheid* (legal hacking authority): Dutch police may, under strictly defined statutory conditions and judicial oversight, covertly and remotely access a suspect's device or computer system to gather evidence, install investigative software, or perform other authorized investigative actions. The power is subject to proportionality and other procedural safeguards and provides law enforcement with a technically sophisticated investigative capability for confronting equally sophisticated cybercrime.

Third, decryption obligations: suspects may, under certain legally defined conditions, be required to cooperate in decrypting data or communications, subject to applicable *nemo tenetur* protections. This provision creates a legally regulated mechanism for addressing encryption barriers that might otherwise render relevant cybercrime evidence inaccessible.

Fourth, data-retention obligations: service providers may be subject to statutory obligations concerning the preservation or retention of specified categories of traffic and subscriber data for defined periods, enabling law enforcement to seek lawful access before relevant information is deleted or becomes unavailable.

Van Roomen (2025) demonstrated that synchronization between substantive and procedural legal reforms is the main key to success in combating cross-border cybercrime. Indonesia currently lacks equivalent instruments to several of these Dutch investigative mechanisms. The absence of such instruments may render sophisticated provisions of the 2023 Criminal Code difficult to operationalize when confronting organized cybercrime syndicates operating across multiple jurisdictions.

The most complex technical and forensic obstacles are rooted in cloud computing and transnational jurisdiction. In ransomware cases—as evidenced by the 2024 PDN incident—perpetrators may store activity logs, credentials, encryption keys, and other operational data on overseas infrastructure, potentially protected by end-to-end encryption (E2EE). Osula (2015) showed that conventional Mutual Legal Assistance (MLA) procedures often take months, while volatile digital data may disappear, be deleted, or be overwritten before international access authorization is issued. Arnel (2023) further argue that the territorial and transnational architecture of cybercrime prosecution creates a sovereignty dilemma in which enforcement authority remains bounded by state borders while digital conduct and evidentiary traces move across jurisdictions instantaneously. further observe that bilateral data-sharing agreements between states remain among the most pragmatically effective mechanisms for bridging jurisdictional gaps in cross-border digital investigations.

Discussion

The Paradox of Legal Asymmetry: A Friedman Systems Analysis

The central paradox identified in this study, that advanced substantive criminal law may fail in the face of inadequate formal procedural instruments, is best analyzed through the tripartite framework of Lawrence M. Friedman's Legal System Theory (Friedman, 1975). While Friedman's framework was developed in the context of the American legal system in the 1970s, its analytical utility extends beyond its original sociological context. Indonesian legal scholars, including Rahardjo (1979) and Wignjosoebroto (2002), have similarly observed that Indonesian law is characterized by a persistent gap between formally enacted norms and actual law-enforcement practice, precisely the structural-cultural dynamic that Friedman's framework was designed to diagnose. The application of Friedman's tripartite model to the Indonesian cybercrime context is therefore not a naïve theoretical transplant but an analytically appropriate deployment of a framework whose diagnostic power has been applied across pluralistic legal systems. Friedman posits that a legal system comprises three interdependent components: substantive law (the rules and norms), legal structure (the institutional machinery), and legal culture (the values, attitudes,

and behaviors of legal actors). Effective legal reform requires coherence across all three dimensions; asymmetric reform, which advances one dimension while neglecting others, systematically generates implementation failures.

Applied to the Indonesian cybercrime context, the 2023 Criminal Code represents a genuine and commendable advancement of the substantive dimension. The CIA triad's incorporation into the analytical framework, the explicit protection of digital information and electronic systems, and the detailed construction of offenses in Articles 332–335 all demonstrate sophisticated legislative drafting. Yet the structural dimension (the institutional machinery for enforcement) remains severely underdeveloped. Forensic laboratory capacity is disproportionately concentrated in Jakarta; Regional Police (*Polda*) and Resort Police (*Polres*) levels lack sufficient numbers of certified digital-forensic experts; and judicial education concerning the technical assessment of digital evidence remains limited.

The cultural dimension presents perhaps the deepest challenge. Digital literacy among prosecutors, defense counsel, and judges varies enormously. Without a baseline level of technical competence, the adversarial system, designed to arrive at truth through the presentation and testing of informed arguments, may become a site where procedural technicalities, rather than substantive reliability, determine outcomes. Supreme Court Decision No. 1089 K/Pid.Sus/2018 illustrates this precisely: Facebook screenshot evidence that was substantively relevant was rejected or given insufficient evidentiary weight because the prosecutor failed to establish account authenticity and chain of custody through credible digital-forensic verification. Casey (2011) describes this as the competence gap, the distance between what forensic science can establish and what legal actors can effectively utilize in adversarial proceedings.

This analysis reinforces the conclusion that Indonesia's path to effective cybercrime law enforcement is not primarily a legislative challenge. The 2023 Criminal Code has substantially addressed the imperative of substantive reform. The primary challenge is structural and cultural: building the institutional capacity and legal culture necessary to operationalize sophisticated substantive norms in forensic and judicial practice. If the structural-cultural gap is the root cause, the codification of the exclusionary rule in the 2025 Criminal Procedure Code, far from resolving it, risks deepening the paradox by elevating procedural standards beyond what current forensic infrastructure can reliably satisfy.

The Exclusionary Rule Paradox and Due Process of Law

The explicit statutory recognition of the exclusionary rule through Article 235 of the 2025 Criminal Procedure Code creates what this study terms the exclusionary paradox: the very procedural protection designed to safeguard suspects' legal rights simultaneously functions as a mechanism that may render the 2023 Criminal Code's advanced substantive provisions less effective in practice. This paradox is not a flaw in constitutional design but rather the potential consequence of formal procedural advancement that outpaces institutional forensic capacity. The term exclusionary paradox, as employed in this article, is advanced as a new analytical concept to describe the phenomenon in which progressive procedural codification may paradoxically undermine the effectiveness of advanced substantive criminal law, a paradox that has not previously been documented systematically in the Indonesian criminal-procedure literature.

The due process of law principle embedded in Article 1(1) of the *KUHAP* and reinforced by the 2025 Criminal Procedure Code demands that state power in criminal proceedings be exercised according to established rules and with respect for individual rights. This is a fundamental constitutional commitment. Ali Murtadho (2025) argue that Indonesian courts have previously applied the exclusionary rule inconsistently due to the absence of clear statutory authorization, resulting in unpredictable evidentiary outcomes. The 2025 *KUHAP* brings welcome clarity but simultaneously raises the evidentiary standard that investigators must meet.

The practical consequence is significant. Electronic evidence obtained through otherwise valid investigative methods but accompanied by serious procedural deficiencies—a missing signature in a chain-of-custody log, an inadequately documented extraction procedure, or a forensic process whose reliability cannot be adequately demonstrated—may be rendered inadmissible or deprived of evidentiary force under Article 235. Sophisticated defense counsel can therefore challenge evidence not only by demonstrating substantive unreliability but also by

identifying defects in the legality, authentication, or documentation of its acquisition. Brenner (2012) describes this as the procedural asymmetry problem in cybercrime prosecution: defendants with qualified counsel may benefit disproportionately from procedural technicalities in digital-evidence exclusion compared with defendants in conventional criminal cases.

The resolution of this paradox requires not the abandonment of the exclusionary rule, which would be constitutionally and normatively regressive, but rather the systematic elevation of forensic collection standards so that admissible evidence routinely meets the applicable legal threshold. This requires adherence to internationally recognized standards such as ISO/IEC 27037:2012 (Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence) and the ACPO Good Practice Guide for Digital Evidence, as well as sufficient judicial and prosecutorial capacity to assess compliance with such standards credibly (Pollitt, 2020).

This position is reinforced by Supreme Court Decision No. 661 K/Pid.Sus/2019 (in a case involving the evidentiary assessment of electronically mediated criminal conduct), in which the justices affirmed that digital evidence must be authenticated through appropriate evidentiary support, including expert testimony where technical examination is necessary; absent adequate verification, digital evidence may carry only limited evidentiary weight.

Digital Sovereignty and Cross-Border Jurisdictional Challenges

The 2024 PDN ransomware attack exposed a fundamental tension in the digital-sovereignty framework: Indonesia's legitimate interest in prosecuting cybercriminals whose actions damage its critical infrastructure conflicts with the technical reality that evidence of those crimes may reside on servers located in foreign jurisdictions subject to different legal regimes. This tension represents what Arnel (2023) identify as the sovereignty dilemma of cybercrime enforcement, the conflict between the state's territorial jurisdiction and the borderless architecture of the Internet.

Existing MLA frameworks were designed largely around cases involving discrete evidence located in a known jurisdiction. Cloud computing fundamentally disrupts this assumption: data may be fragmented across multiple server locations, dynamically migrated between jurisdictions, or subject to contractual arrangements that complicate straightforward government access requests. Identify cloud forensics as a distinct and emerging subdiscipline of digital forensics, requiring specialized tools and legal frameworks beyond those applicable to conventional device forensics.

The Netherlands' approach through *netwerkzoeking* and the Budapest Convention's Article 32(b), which permits law enforcement to access publicly available computer data and data to which the lawful controller consents, provides a partial model. Bilateral cloud-data-sharing arrangements between states and cloud-service providers, in addition to state-to-state agreements, represent an effective complementary pathway for accessing cross-border digital evidence within timeframes that preserve forensic value.

Indonesia's accession to the Budapest Convention would represent a significant step toward harmonizing its cybercrime framework with international standards. The Council of Europe's Second Additional Protocol to the Budapest Convention (2022) specifically addresses challenges involving cloud computing and emergency requests for stored computer data, providing mechanisms that Indonesian investigators currently lack (Council of Europe, 2021). Without participation in such frameworks or the development of equivalent bilateral and multilateral mechanisms, Indonesian law enforcement will continue to face substantial evidentiary barriers in cases involving cross-border digital evidence.

Directions for Legal Reform and Institutional Capacity Building

Unraveling the deadlock in the application of cybercrime offenses under the 2023 Criminal Code amidst the stringent evidentiary regime of the 2025 Criminal Procedure Code requires comprehensive and synergistic intervention across all three dimensions of Friedman's legal system. This study formulates four concrete recommendations, each grounded in the foregoing analysis.

First, the urgent issuance of a Supreme Court Regulation (PERMA) on Electronic Evidence Procedures. This PERMA should codify: (a) technical standards for handling and preserving digital

evidence from the crime scene; (b) requirements for the validity and reliability of forensic data extraction, including specifications and validation requirements for forensic software and hardware; (c) parameters for judges' assessment of scientific evidence and forensic expert testimony; and (d) specific procedures for the search and seizure of digital devices and electronically stored information. Although PERMA No. 4 Tahun 2020 concerning *Administrasi dan Persidangan Perkara Pidana di Pengadilan secara Elektronik* represents an important initiative, it focuses primarily on electronic trial administration and does not comprehensively address operational digital-forensic standards, requiring further substantive development (MA RI, 2020). The Dutch experience demonstrates that explicit procedural regulation of digital-evidence handling, rather than leaving standards primarily to judicial discretion, can produce more consistent and predictable outcomes.

Second, the standardization and certification of digital-forensic competencies. The Indonesian National Police (Polri) and the Attorney General's Office need to establish an internal certification program adhering to the ISO/IEC 27037 standard and extending appropriate competency development to the Polda and Polres levels. Pollitt (2020) argues that standardized forensic certification at the investigative level is the single most impactful intervention available to criminal justice systems seeking to improve digital-evidence admissibility rates. The Supreme Court should also provide intensive continuing education for judges to ensure sufficient digital literacy for the credible assessment of parties' technical claims in court.

Third, the acceleration and modernization of the Mutual Legal Assistance (MLA) regime for the digital age. The Indonesian government should proactively negotiate Fast-Track Data Preservation Protocols through bilateral and multilateral agreements with countries hosting global cloud-service providers, particularly the United States, Singapore, and European Union member states. Such protocols could allow law enforcement authorities to request the rapid preservation or temporary freezing of relevant cross-border data while formal legal processes are completed. Such mechanisms are increasingly important in international cybercrime cooperation and can reduce the risk that volatile digital evidence will be deleted or overwritten before lawful access is obtained (Council of Europe, 2021).

Fourth, beyond short- to medium-term institutional reforms, the most fundamental long-term transformation lies in investing in the next generation of legal practitioners through a comprehensive modernization of the Indonesian legal-education curriculum. Integrating courses on substantive digital criminal law, procedural rules governing electronic evidence, and computational forensics into the standard curriculum of Indonesian Faculties of Law is an urgent structural reform. This addresses the cultural dimension of Friedman's framework: a new generation of prosecutors, defense counsel, and judges equipped with baseline digital literacy will substantially reduce the competence gap that currently undermines the adversarial assessment of digital evidence. Casey (2011) notes that digital-forensics literacy is no longer a specialized competency; it is a foundational requirement for any legal professional operating in the contemporary criminal-justice system.

The international relevance of these recommendations extends beyond Indonesia. Across ASEAN and the broader Global South, nations are simultaneously modernizing their substantive cybercrime laws while confronting similar structural and cultural challenges in enforcement. Indonesia's experience offers valuable lessons for other developing nations navigating the transition from ITE-law-style *lex specialis* regimes to KUHP-style codification. Brenner's (2012) observation that the fundamental challenge of cybercrime governance is not the absence of norms but the incapacity to enforce them applies with particular force to the Indonesian context.

The limitations of this study must be acknowledged. First, the empirical base relies primarily on two illustrative Supreme Court decisions (No. 1089 K/Pid.Sus/2018 and No. 661 K/Pid.Sus/2019), given the current limited access to a comprehensive published cybercrime-verdict database in Indonesia. Second, the comparative analysis focuses on the Netherlands, reflecting shared civil-law traditions; a broader ASEAN comparative analysis would enrich the findings. Third, the 2025 Criminal Procedure Code is recent, and its judicial application is still emerging; longitudinal empirical study will be required to assess the actual impact of Article 235 and the codification of the exclusionary rule on digital-evidence admissibility in practice.

CONCLUSION

This study has demonstrated that the 2023 Criminal Code successfully modernizes Indonesia's substantive criminal law by recognizing digital information and electronic systems as legally protected interests and defining cybercrime offenses with greater technical precision through provisions including Articles 258 and 332–335. The 2025 Criminal Procedure Code further advances formal criminal law by explicitly recognizing electronic evidence through Article 235 and establishing statutory requirements concerning authentication and the lawful acquisition of evidence, thereby providing a clearer foundation for the exclusion of unlawfully obtained or unauthenticated evidence.

However, as this article has demonstrated, these normative advances harbor a fundamental paradox that cannot be resolved through regulatory refinement alone.

The study's central finding is that this dual substantive and procedural advancement has generated an enforcement paradox, analyzed through Lawrence M. Friedman's Legal System Theory: while the substantive and normative dimensions of reform have advanced significantly, the structural dimension (institutional forensic capacity) and the cultural dimension (digital literacy among legal actors) remain critically underdeveloped. Supreme Court Decision No. 1089 K/Pid.Sus/2018 exemplifies this systemic failure: substantively relevant digital evidence was rejected or given insufficient evidentiary weight because account authenticity and chain of custody were not adequately verified through digital-forensic examination.

Comparative analysis of the Dutch *Wet computercriminaliteit III* confirms that effective cybercrime enforcement requires simultaneous reform of substantive norms, procedural instruments (*netwerkzoeking*, *hackbevoegdheid*, and other specialized investigative powers), and institutional capacity. Without implementing the four recommended interventions (PERMA on electronic evidence, digital-forensic standardization, fast-track MLA protocols, and legal-education curriculum reform) the 2023 Criminal Code risks remaining a sophisticated legal instrument on paper but a blunt instrument in practice. Future research should pursue empirical survey-based studies following the full implementation of the 2025 Criminal Procedure Code, broader ASEAN comparative analysis, and longitudinal evaluation of the 2023 Criminal Code's cybercrime provisions.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to Universitas Kristen Indonesia for providing academic support and research facilities during the preparation of this article. The authors also appreciate the contributions of colleagues, legal scholars, and practitioners who provided valuable discussions and insights related to cybercrime regulation, digital evidence, and criminal law reform in Indonesia. This research was conducted independently, and all opinions and analyses presented in this article are solely the responsibility of the authors.

AUTHOR CONTRIBUTION STATEMENT

Lonna Yohanes Lengkong contributed to the conceptualization of the research, development of the analytical framework, legal analysis, methodology design, data interpretation, and preparation of the initial manuscript draft. Hendri Jayadi contributed to the validation of legal arguments, refinement of theoretical perspectives, critical review, and improvement of the manuscript structure and academic presentation. Both authors actively participated in reviewing the final manuscript, discussing the research findings, and approving the final version for publication.

REFERENCES

- Ali Murtadho, N. (2025). Illegally obtained evidence in Indonesia's Draft Criminal Procedure Code (RUU KUHP): Exclusionary rules and the due process of law. *Jurnal Penelitian Hukum De Jure*, 25(3), 291–308. <https://doi.org/10.30641/dejure.2025.V25.291-308>
- Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime—why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37(1), 29–51. <https://doi.org/10.1080/13600869.2022.2061888>
- Badan Siber dan Sandi Negara. (2024). *Laporan tahunan keamanan siber Indonesia 2023*. BSSN.

- Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*.
- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
- Clough, J. (2010). *Principles of cybercrime* (Vol. 406). Cambridge: Cambridge University Press.
- Council of Europe. (2021). *Budapest convention on cybercrime (ETS No. 185)*. <https://rm.coe.int/1680081561>
- Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Kencana Prenada Media Group.
- Nelson, F. M., Propseriani, M. D., Ramadhan, C. R., & Andini, P. P. (2024). Cracking the code: Investigating the hunt for crypto assets in money laundering cases in Indonesia. *JILS*, 9, 89. <https://doi.org/10.15294/jils.vol9i1.4534>
- Osula, A. M. (2015). *Mutual legal assistance & other mechanisms for accessing extraterritorial data*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Research Paper.
- Peraturan Mahkamah Agung Nomor 4 Tahun 2020 tentang Administrasi dan Persidangan Perkara Pidana di Pengadilan secara Elektronik. (2020). <https://jdih.mahkamahagung.go.id>
- Politou, E., Alepis, E., & Patsakis, C. (2019). Profiling tax and financial behaviour with Big Data under the GDPR. *Computer law & security review*, 35(3), 306-329.
- Pollitt, M. (2020). Digital forensics: An analytical course of action. *Journal of Digital Forensics, Security and Law*, 15(1), 11-25.
- Prasetyo, D. I., Sholehuddin, M., & Karim. (2025). Ratio legis of cybercrime legislation policy in Indonesia. *International Journal of Cyber Criminology*, 18(2), 57-70.
- Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019. (2019). Direktori Putusan Mahkamah Agung. <https://putusan3.mahkamahagung.go.id>
- Putusan Mahkamah Agung Nomor 1089 K/Pid.Sus/2018. (2018). Direktori Putusan Mahkamah Agung. <https://putusan3.mahkamahagung.go.id>
- Putusan Mahkamah Agung Nomor 5084 K/Pid.Sus/2022. (2022). Direktori Putusan Mahkamah Agung. <https://putusan3.mahkamahagung.go.id>
- Quick, D., & Choo, K. K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix. *Future Generation Computer Systems*, 78, 558-567.
- Rahardjo, S. (1979). *Hukum dan perubahan sosial: suatu tinjauan teoretis serta pengalaman-pengalaman di Indonesia*. Genta Publishing.
- Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Nathania, B. A. T. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, 11(1). <https://doi.org/10.1080/23311886.2024.2439543>
- Van Roomen, T. (2025). Cross-border evidence gathering in criminal crypto investigations: A case study of the Netherlands. *Tilburg Law Review*, 30(1). <https://doi.org/10.5334/tilr.423>
- Wignjosoebroto, S. (2002). *Hukum: Paradigma, metode, dan dinamika masalahnya*. Elsam dan Huma.
- Yasir, M. (2025). The position of digital evidence in the KUHAP evidence system: Normative analysis and implementation challenges. *International Journal of Educational Review, Law and Social Sciences (IJERLAS)*, 5(3).