Southeast Asian Journal of Global Legal Horizon

Lifescifi Akademia Utama

Southeast Asian Journal of Global Legal Horizon

Volume: 3
Issue: 1
Year: 2026
Page: 29-36

Citation:
Saputro, M. S., & Pratiwi, G. F. (2026). Cybercrime Regulation and Criminal Law Strategies for Prevention and Countermeasures in Indonesia. *Southeast Asian Journal of Global Legal Horizon*, *4*(1), 29-36.

Article History:
Received: January 20, 2026
Revised: June 3, 2026
Accepted: June 18, 2026
Online since: June 30, 2026

Cybercrime Regulation and Criminal Law Strategies for Prevention and Countermeasures in Indonesia

Mansyur Bayu Saputro[1*], Girang Fitria Pratiwi[2]

[1] Universitas Janabadra, Yogyakarta, Indonesia
[2] Universitas Terbuka, Bengkulu, Indonesia

Abstract:

The development of information technology has created new opportunities for cybercrime and generated challenges for Indonesia's criminal justice system. This study aims to analyze the regulation of cybercrime within the Indonesian criminal law system and examine criminal law strategies for its prevention and countermeasures. This research employs a normative-empirical method with a qualitative approach by examining legislation, legal documents, and relevant academic literature. The analysis focuses on the Criminal Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Telecommunications Law. The findings indicate that Indonesia has established a broad legal framework for addressing cybercrime, particularly through Law Number 1 of 2024 as the Second Amendment to the Electronic Information and Transactions Law. However, law enforcement continues to face challenges concerning jurisdiction, offender identification, technological developments, institutional capacity, and electronic evidence. Therefore, effective cybercrime countermeasures require an integrated approach combining penal and non-penal policies, digital literacy, electronic evidence management, institutional capacity building, personal data protection, and international cooperation. Strengthening regulatory harmonization and adaptive law enforcement is essential to ensure effective legal protection in the digital environment.

Keywords:

Cybercrime; Criminal Law; Electronic Evidence; Law Enforcement; Prevention.

Copyright: © 2026 by the authors.
This work is licensed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).

1. Introduction

The development of information and communication technology has changed the pattern of people's interactions in various fields, including trade, public services, communication, and information exchange. Dependence on the digital space also creates opportunities for the emergence of various forms of cybercrime that are increasingly diverse and complex. Cybercrime is not only related to attacks on computer systems, but also includes the misuse of electronic transactions, theft or misuse of data, digital fraud, and other actions that utilize information technology as a means and targets of crime (Suhaemin & Muslih, 2021; Ariyaningsih et al., 2023). The acceleration of digitalization thus needs to be followed by the ability of the law to provide adequate protection, certainty, and law enforcement mechanisms.

The characteristics of cybercrime pose its own problems for the criminal law system because acts can be carried out through electronic networks, use identities that are difficult to trace, and involve data and systems in different jurisdictions. This condition causes conventional criminal law approaches to face challenges in determining jurisdiction, identifying perpetrators, obtaining evidence, and ensuring criminal accountability. Wijaya and Arifin (2020) show that the cross-border character of cybercrime requires legal instruments and cooperation that are able to bridge jurisdictional differences. In line with that, Anwary (2022) emphasized that the effectiveness of cybercrime prevention does not only depend on the existence of regulations, but also on institutional capacity and law enforcement.

In the Indonesian legal system, cybercrime regulation has developed through several legal instruments. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended through Law Number 19 of 2016 and finally through Law Number 1 of 2024, is one of the main bases in regulating acts related to information and electronic transactions. The latest amendment is directed to provide legal certainty and protect the public interest from misuse of information, documents, technology, and electronic transactions. In addition, Law Number 27 of 2022 concerning Personal Data Protection provides a special legal framework for personal data protection which is increasingly relevant in dealing with digital crime.

These regulations need to be placed within a broader criminal law framework. Law Number 1 of 2023 concerning the Criminal Code (KUHP) is an important part of the reform of the national criminal law, while Law Number 36 of 1999 concerning Telecommunications provides the basis for regulating the implementation of telecommunications related to the use of networks and communication technology. Suryani and Azhari (2020) and Melani et al. (2020) show that the development of digital criminal law needs to consider aspects of protecting rights, privacy, and non-conventional character from technology-based crimes.

Another problem lies in proof. The digital nature of cybercrime causes electronic evidence to have a strategic position in the law enforcement process. Hardinanto et al. (2023) emphasized the importance of computer forensics in obtaining and analyzing electronic documents as evidence, while Wiarti (2023) and Mantik et al. (2022) discussed the position and legality of digital evidence in cybercrime cases. Thus, the effectiveness of cybercrime prevention is not enough only through criminalization, but also requires a mechanism for proof and law enforcement that is able to adapt to technological developments.

Previous studies have discussed the characteristics of cybercrime, regulatory developments, criminal law policies, and the position of electronic evidence (Nugroho & Chandrawulan, 2022; Anwary, 2023; Nadriana & Sukmana, 2022; Kasim, 2024; Fairuzzen et al., 2024). However, there is still a need for a discussion that integrates aspects of cybercrime regulation in the Indonesian criminal law system with enforcement challenges and its prevention and countermeasures in a

comprehensive manner. Therefore, this study aims to analyze cybercrime regulation in the Indonesian criminal law system and evaluate legal approaches that can be used to improve the effectiveness of prevention and countermeasures.

Based on this description, this study formulated two research questions: (1) How is cybercrime regulated in the Indonesian criminal law system based on the development of relevant laws and regulations? (2) What are the criminal law strategies that can be applied to improve the prevention and control of cybercrime in Indonesia?

2. Methods

This study uses a normative-empirical legal research method with a qualitative approach. The normative approach is used to analyze the legal provisions that govern cybercrimes in the Indonesian criminal law system, while the empirical approach is used to understand the application of these provisions in efforts to prevent and counter cybercrime. The research is carried out through the study of laws and regulations, legal documents, scientific literature, and various information related to the development and enforcement of cybercrime in Indonesia. The analysis is carried out in a descriptive-analytical manner by linking the applicable legal provisions with legal problems that arise due to the development of information technology.

The primary legal materials in this study include the Constitution of the Republic of Indonesia in 1945, Law Number 1 of 2023 concerning the Criminal Code, Law Number 11 of 2008 concerning Information and Electronic Transactions as amended through Law Number 19 of 2016 and finally through Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 36 of 1999 concerning Telecommunications. The ITE Law is the main instrument in the research because it regulates various acts related to the misuse of information, documents, systems, and electronic transactions, including provisions regarding electronic evidence. Law Number 1 of 2024 is also an important concern because it updates a number of provisions in the ITE Law and adjusts them to the needs of the development of the digital space.

Secondary legal materials consist of scientific journal articles, books, research results, and academic publications relevant to cybercrime, criminal law policy, digital law enforcement, electronic evidence, and personal data protection. These materials are used to strengthen analysis of the legal problems being studied. Meanwhile, supporting materials are used to gain an understanding of technological developments and the characteristics of cybercrime.

The collection of materials was carried out through literature studies and searches of relevant legal documents. All materials obtained were then classified based on the themes of cybercrime regulation, law enforcement, electronic proof, and prevention and countermeasures strategies. Furthermore, data and legal materials were analyzed qualitatively by interpreting legal provisions, comparing them with the development of cybercrime problems, and drawing the relationship between legal norms and law enforcement needs. The results of the analysis were used to answer two research questions regarding cybercrime regulation in the Indonesian criminal law system as well as criminal law strategies that can be applied to improve cybercrime prevention and countermeasures. Law Number 27 of 2022 is also used as an important basis for analyzing personal data protection related to cybercrime.

3. Results and Discussion

3.1 Regulation of Cybercrime in the Indonesian Criminal Law System

Cybercrime is a form of crime that has different characteristics from conventional crimes because it utilizes information technology and electronic networks as means and objects of crime. This character causes the boundaries of space and time to become increasingly unclear so that an act can be carried out without the physical presence of the perpetrator at the place where the consequences occur. Suhaemin and Muslih (2021) explained that cybercrime has a virtual character, perpetrators can hide their identities, and technological developments create forms of crime that are difficult to reach by conventional legal mechanisms. The development of digitalization is also related to the increasing chances of technology-based crime, so a legal system that is able to keep up with these changes is needed (Ariyaningsih et al., 2023).

In the Indonesian legal system, the regulation of cybercrime does not only rely on one regulation, but is spread across several legal instruments. Law Number 11 of 2008 concerning Information and Electronic Transactions is an important basis for regulating criminal acts committed through electronic systems. These provisions were then amended through Law Number 19 of 2016 and finally through Law Number 1 of 2024. The development of these regulations shows that the law needs to be adapted to changes in technology and the needs of the digital society. Melani et al. (2020) placed criminal law policy in the field of electronic transactions in response to the emergence of non-conventional criminal acts in the digital space.

The regulation of cybercrime must also be placed within the framework of the national criminal law as a whole. Law Number 1 of 2023 concerning the Criminal Code is part of the national criminal law reform, while the ITE Law functions as one of the special instruments that regulates acts related to information and electronic transactions. Suryani and Azhari (2020) show that the reform of criminal law policies in dealing with digital crime must pay attention to technological developments as well as ethical aspects and privacy protection. Thus, cybercrime regulation needs to create a balance between the interests of law enforcement and the protection of people's rights.

In addition to the ITE Law and the Criminal Code, Law Number 27 of 2022 concerning Personal Data Protection has increasing relevance in the cybercrime legal system. The misuse of personal data can be part of a series of digital crimes so that data protection cannot be separated from cybercrime prevention policies. The legal framework was then strengthened by Law Number 36 of 1999 concerning Telecommunications which provides the basis for regulating the implementation of telecommunications. Thus, there is a relationship between the regulation of digital crimes, data protection, and the implementation of communication networks.

Another problem in regulating cybercrime is jurisdiction. The cross-border nature of cyberspace can cause perpetrators, victims, devices, and data to be in different legal locations. Wijaya and Arifin (2020) emphasized the importance of international legal instruments and cooperation between countries in dealing with transnational cybercrime. These jurisdictional issues are also related to the need for harmonization and the development of legal approaches that can effectively reach digital crimes (Nadriana et al., 2022).

Based on the results of the analysis, cybercrime regulation in Indonesia has formed a relatively broad legal framework through the Criminal Code, ITE Law, PDP Law, and telecommunications regulations. However, the existence of various legal instruments does not automatically guarantee the effectiveness of countermeasures. Nugroho and Chandrawulan (2023) show that the development of cybercrime still poses challenges even though various countries have developed cybersecurity regulations and systems. Therefore, cybercrime regulation must be understood as a system that continues to develop and requires harmonization

between criminal law, information technology law, data protection, and cross-jurisdictional cooperation mechanisms.

3.2 Criminal Law Strategy in Cybercrime Prevention and Countermeasures in Indonesia

Cybercrime countermeasures cannot only be carried out through the establishment of criminal provisions, but require a legal strategy that includes prevention, enforcement, proof, and institutional capacity building. The dynamic character of cybercrime means that criminal law must be able to respond to changes in modes and technologies used by perpetrators. Kasim (2024) assesses that criminal law policy is an important part of dealing with cybercrime because the development of digital crime takes place faster than regulatory changes. Countermeasures strategies thus need to be carried out in an adaptive and sustainable manner.

The first approach is penal policy through criminalization and law enforcement. The ITE Law, as last amended through Law Number 1 of 2024, provides a legal basis for various acts related to the misuse of information and electronic systems. The existence of these criminal provisions needs to be supported by consistent legal application so that the norms that have been formed can provide the effect of legal protection and certainty. Melani et al. (2020) explained that criminal law policies in electronic transactions are needed in response to changes in the form of crime due to technological developments. Meanwhile, Anwary (2022) shows that the effectiveness of cybercrime eradication is related to the quality of the legal framework and the ability of public institutions to implement it.

The law enforcement aspect also depends heavily on the ability of the authorities to handle the characteristics of digital crime. Cybercrime often leaves a trail in the form of electronic data that requires special methods to obtain, maintain, and analyze it. Hardinanto et al. (2023) explained that computer forensics has an important role in ensuring the authenticity of information or electronic documents so that they can be used in the proof process. In line with that, Wiarti (2024) emphasized that the legality of electronic evidence is not only related to its existence, but also to the fulfillment of material and formal requirements as well as the support of digital forensics and expert testimony.

The position of digital evidence is also a challenge because electronic information can be altered, deleted, or manipulated. Mantik et al. (2022) point out the importance of proper procedures in the use of digital evidence and the need to ensure the authenticity and integrity of evidence in legal proceedings. Therefore, improving the ability of investigators, public prosecutors, judges, and experts to understand digital technology is an important part of cybercrime countermeasures strategies.

In addition to penal policies, a non-penal approach needs to be developed through increasing digital literacy, information security awareness, strengthening network security systems, and protecting personal data. Nugroho and Chandrawulan (2023) emphasized the importance of increasing user awareness and security strategies to create a safer digital environment. These efforts are in line with the needs of the implementation of Law Number 27 of 2022 concerning Personal Data Protection, especially in encouraging responsible data management and reducing the risk of data misuse.

The next strategy is to strengthen cooperation between agencies and between countries. The nature of cybercrime that can go beyond the boundaries of jurisdiction makes national law enforcement sometimes require information exchange, mutual legal assistance, and international cooperation mechanisms. Wijaya and Arifin (2020) place international cooperation as an important part of dealing with cybercrime that has a cross-border dimension. Nadriana et al. (2022) also show that the character of cyberspace poses challenges to the application of legal principles and requires the development of an approach that is in accordance with the character of digital crime.

Thus, cybercrime countermeasures in Indonesia need to use an integrated approach that combines penal and non-penal policies. Penal policies provide the basis for criminalization and law enforcement, while non-penal policies function to reduce the chances of crime through education, technological security, data protection, and increasing public awareness. Fairuzzen et al. (2024) emphasized that legal developments must go hand in hand with the development of cybercrime so that regulations are not left behind from technological changes. This integrated approach is an important basis for building a cybercrime countermeasures system that is more adaptive, effective, and oriented towards community protection.

4. Conclusion

This study shows that cybercrime is a form of crime that has dynamic, cross-border characteristics, and is highly dependent on the development of information technology so that it requires an adaptive criminal law system. The regulation of cybercrime in Indonesia has been supported by several legal instruments, especially Law Number 1 of 2023 concerning the Criminal Code, Law Number 11 of 2008 concerning Information and Electronic Transactions and the latest amendments through Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 36 of 1999 concerning Telecommunications. The existence of these various regulations shows that there are efforts to build a legal framework that is able to provide a basis for criminalization, community protection, and law enforcement against crime in the digital space.

However, the existence of regulations does not fully guarantee the effectiveness of cybercrime countermeasures. Challenges still lie in determining jurisdiction, identifying perpetrators, developing crime modes, the capacity of law enforcement officials, and the collection and proof of electronic evidence. Therefore, cybercrime countermeasures strategies need to be carried out in an integrated manner through penal and non-penal policies. Penal policies need to be strengthened through law enforcement, capacity building of apparatus, and optimization of digital evidence, while non-penal policies can be carried out through digital literacy, increasing cybersecurity awareness, protecting personal data, and strengthening cooperation between agencies and between countries. This approach is needed to build a cybercrime countercrime system that is effective, adaptive, and able to provide legal protection amid the development of digital technology.

References

Anwary, I. (2022). The role of public administration in combating cybercrime: An analysis of the legal framework in Indonesia. *International Journal of Cyber Criminology, 16*(2), 216-227.

Anwary, I. (2023). Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach. *International Journal of Cyber Criminology, 17*(1), 12-22.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi kejahatan siber dengan percepatan digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum, 1*(1), 1-11.

Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, 2*(1), 139-153.

Hardinanto, A., Arief, B. N., & Setiyono, J. (2023). The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law. *Jurnal Cakrawala Hukum, 14*(2), 155-166.

Kasim, Z. (2024). Kebijakan hukum pidana untuk penanggulangan cyber-crime di Indonesia. *Indragiri Law Review, 2*(1), 18-24.

Mantik, V., Watulingas, R. R., & Muaja, H. S. (2022). Tinjauan yuridis tentang kedudukan alat bukti digital dalam tindak pidana kejahatan mayantara (cyber crime). *Lex Privatum*, *10*(5), 112-124.

Melani, M., Disemadi, H. S., & Jaya, N. S. P. (2020). Kebijakan Hukum Pidana Dibidang Transaksi Elektronik Sebagai Tindak Pidana Non-Konvensional. *Pandecta Research Law Journal*, *15*(1), 111-120.

Nadriana, L., & Sukmana, P. (2022). Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges. *International Journal of Cyber Criminology*, *16*(2), 192-204.

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1.

Suhaemin, A., & Muslih, M. (2021). Karakteristik Cybercrime di Indonesia. *EduLaw: Journal of Islamic Law and Yurisprudance*, *2*(1), 15-26.

Suryani, D. E., & Azhari, A. (2020). Digital Criminal Law Policy: Ethical and Privacy Challenges In the Enforcement of The New Indonesian Criminal Code (Kuhp) On Cybercrime. *AT-TAFAHUM: Journal of Islamic Law*, *4*(1), 14-23.

Wiarti, J. (2023). Legality of electronic evidence in cyber crime cases. *Ahmad Dahlan Indonesian Law Journal*, *1*(2), 11-19.

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63-74.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.