Implementation of Law Enforcement Against Cybercrime in Indonesia.

Peter Valentino Munthe, Suci Ramadani, Ismaidar

Abstract

The development of information and communication technology has provided various conveniences in people's lives, but at the same time it has also given rise to various new forms of crime that utilize cyberspace or known as *cybercrime*. This research aims to analyze the implementation of law enforcement against *cybercrime* crimes in Indonesia and identify various obstacles faced by law enforcement officials in the process of handling them. The research method used is a normative legal research method with a statutory approach and a conceptual approach. Data was obtained through literature studies of laws and regulations, books, scientific journals, and various relevant legal documents. The results of the study show that law enforcement against *cybercrime* in Indonesia has a legal basis through the Criminal Code, the Law on Information and Electronic Transactions and its amendments, as well as a number of other related regulations. However, in its implementation, there are still various obstacles, including the very rapid development of crime modes, the limitation of human resources who have competence in the field of information technology and digital forensics, difficulties in obtaining and securing electronic evidence, and the characteristics of *cybercrime* that can exceed the boundaries of the country's jurisdiction. Therefore, it is necessary to strengthen the capacity of law enforcement officials, improve technological facilities and infrastructure, improve regulations, and strengthen national and international cooperation so that law enforcement against *cybercrime* can be carried out effectively and be able to provide certainty and legal protection for the community.

***Keywords**: Cybercrime, Law Enforcement, Crime, Cybercrime, Indonesia.*

Peter Valentino Munthe[1]
Department, Affiliation, Country
E-mail: pmunthe1@gmail.com[1]

Suci Ramadani[2], Ismaidar[3]
e-mail: suciramadani@dosen.pancabudi.ac.id[2], ismaidarisma@gmail.comg[3]
3rd International Conference Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Cross-Sector and Cross-Disciplinary Strategies for Achieving the SDGS
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

The development of information and communication technology has brought significant changes to various aspects of people's lives. The use of the internet, social media, digital financial services, electronic commerce, and various technology-based systems has made it easier to conduct communication and transactions without being limited by time and space. However, these developments have also been followed by the emergence of various forms of criminal acts that use information technology as a means or as a target for crime. This crime is known as *cybercrime* or cybercrime. *Cybercrime* is basically a form of crime that has different characteristics from conventional crime because it is carried out through electronic systems, can involve perpetrators and victims in different regions, and leave behind evidence, which is mostly in digital form (Arifin, 2023).

The forms of *cybercrime* in Indonesia are increasingly diverse, ranging from illegal access to electronic systems, theft and misuse of data, online fraud, electronic information manipulation, hacking, dissemination of unlawful content, to various other criminal acts that use digital technology as a means of implementation. This condition poses its own challenges to the law enforcement system in Indonesia. Cybercrime not only requires legal provisions that are able to accommodate technological developments, but also requires law enforcement officials who have the ability to conduct investigations, investigations, collection of electronic evidence, and digital forensic analysis. In practice, police officers still face various institutional, technical, and regulatory obstacles in handling cybercrime (Tjahyono, Nurhasim, & Cahyono, 2025).

Juridically, Indonesia already has a legal basis for law enforcement against criminal acts that occur through electronic systems. One of the important legal bases is Law Number 11 of 2008 concerning Information and Electronic Transactions which has undergone changes 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 Information and Electronic Transactions. These changes were made, among other things, because a number of previous provisions still caused multiple interpretations and controversies, so it is necessary to strengthen legal certainty and a sense of justice in society (Republic of Indonesia, 2024). This provision also regulates the authority of investigators in conducting investigations into criminal acts in the field of information technology and electronic transactions, including examinations of electronic systems, searches, seizures, and cooperation with investigators of other countries in order to obtain information and evidence.

Although legal tools are available, the effectiveness of law enforcement against *cybercrime* is not only determined by the existence of laws and regulations. The rapidly changing character of cybercrime, the use of technology to disguise the identity of perpetrators, the existence of electronic evidence that is easily changed or eliminated, and the possibility of cross-border network involvement are problems that must be faced by law enforcement officials. Research on the handling of cybercrime also shows that there is a gap between legal provisions and investigation practices in the field, including coordination and procedural issues in obtaining data needed for investigation purposes (Tjahyono, Nurhasim, & Cahyono, 2025). Therefore, the ability of law enforcement institutions to adapt to technological developments is an important part of increasing the effectiveness of cybercrime handling.

Law enforcement efforts against digital crime also require synergy between the National Police of the Republic of Indonesia, ministries in charge of communication and digital, related institutions, electronic system operators, and the public. The government and the National Police continue to encourage the strengthening of integrated enforcement against various forms of digital crime through cross-agency collaboration (Ministry of Communication and Digital, 2026). Based on these conditions, a study of the implementation of law enforcement against cybercrime crimes in Indonesia is important to know how legal provisions are applied in practice, identify obstacles faced by law enforcement officials, and analyze efforts that can be

made to increase the effectiveness of law enforcement so as to be able to provide legal certainty and protection for the public in dealing with the development of crime in the digital space.

Literature Review

3.1 Law Enforcement Concept

Law enforcement is one of the important elements in realizing order, certainty, and justice in people's lives. Basically, law enforcement is a process to implement normative legal provisions into real life. Law enforcement is not only related to the actions of the authorities in sanctioning violations of the law, but also includes the entire process to ensure that the values, norms, and provisions that have been established in laws and regulations can run as they should. Thus, law enforcement is a process that connects the law as written in the regulations with the law as applied in society.

Soekanto explained that the effectiveness of law enforcement is influenced by five main factors, namely legal factors or laws and regulations, law enforcement officials, facilities or facilities that support law enforcement, community factors, and cultural factors (Soekanto, 2022). These five factors have a relationship that affects each other. Good regulations will not be able to provide optimal results if they are not supported by professional law enforcement officials and adequate facilities. On the other hand, the ability of law enforcement officials will also experience obstacles if the legal substance used is unclear or unable to keep up with community developments.

In the context of *cybercrime*, the theory of law enforcement has strong relevance. Legal factors are related to the ability of laws and regulations to regulate various forms of crime committed using information technology. Law enforcement factors are related to the ability of the police, prosecutors, judges, and related parties to understand the characteristics of cybercrime. Meanwhile, facilities and facilities are related to the availability of digital forensic laboratories, technological devices, and the ability to identify and trace electronic evidence. Community factors and legal culture also have an effect because the level of public awareness about digital security and compliance with the law will determine the effectiveness of preventing and handling cybercrimes.

Thus, law enforcement against *cybercrime* cannot be assessed solely based on the number of cases that have been successfully processed. The effectiveness of law enforcement must be seen comprehensively from the readiness of legal substance, the quality of law enforcement officials, the availability of facilities and infrastructure, public awareness, and a developing legal culture. This approach is an important basis for analyzing the implementation of law enforcement against *cybercrime crimes* in Indonesia.

3.2 The Concept of Cybercrime

Cybercrime is a term used to describe various forms of unlawful acts related to the use of computers, internet networks, electronic systems, and information technology. The development of the internet has created a new interaction space known as *cyberspace*. In this space, people can carry out various communication activities and transactions without having to be in the same location. However, the characteristics of cyberspace also provide opportunities for the emergence of new forms of crime that are different from conventional crimes.

Abidin explained that *cybercrime* is a form of crime that arises due to the use of internet technology. *Cybercrime* can be in the form of unlawful acts by using computer networks as a means to commit crimes or making computers and electronic systems the object of crime so that they can cause losses to other parties (Abidin, 2017). In this sense, information technology can have two positions at once, namely as a tool to commit crimes and as a target of criminal acts.

Based on its characteristics, *cybercrime* can include various acts such as illegal access to electronic systems, data theft, system destruction, manipulation of electronic information, fraud through digital media, identity abuse, and various other forms of crime committed by utilizing

computer networks and the internet. Technological developments also cause the mode of cybercrime to continue to change so that the law is required to be able to adapt to these developments. Idris, Nurlani, and Aprita explained that *cybercrime* is a crime committed by utilizing information technology through the internet so that the legal regulation requires harmonization between provisions regarding information technology and national criminal law (Idris, Nurlani, & Aprita, 2024).

One of the important characteristics of *cybercrime* is the absence of strict territorial boundaries as in conventional crimes. Perpetrators can commit criminal acts from a different area from where the victim is located or with the location of the targeted electronic system. This condition raises problems regarding jurisdiction, evidence collection, perpetrator identification, and cooperation between institutions and between countries. In addition, evidence in cybercrime is generally in the form of information and electronic documents. The character of electronic evidence is different from physical evidence because it can be easily copied, moved, modified, or deleted. Therefore, handling *cybercrime* requires technical capabilities and special procedures in maintaining the integrity of digital evidence. An understanding of these characteristics is very necessary in analyzing how the process of investigation, investigation, proof, and the imposition of sanctions against *cybercrime* perpetrators is carried out.

3.3 Law Enforcement against Cybercrime in Indonesia

Law enforcement against *cybercrime* in Indonesia is part of the state's efforts to provide legal protection to the public in the use of information technology and electronic transactions. Technological developments have caused forms of crime to become more complex, so the provisions of conventional criminal law need to be supported by special regulations that are able to reach various acts carried out through electronic systems.

Indonesia already has special arrangements through Law Number 11 of 2008 concerning Information and Electronic Transactions which then underwent changes through Law Number 19 of 2016 and finally with Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. This regulation is one of the main legal bases in handling various criminal acts carried out through electronic systems. In addition to the ITE Law, the application of the law to cyber crimes can also be related to other criminal law provisions according to the characteristics of the acts committed.

In practice, the existence of these regulations has not automatically made law enforcement against cybercrime run without obstacles. Suryawin et al. explained that law enforcement against *cybercrime* in Indonesia still faces a number of problems, such as the limitation of human resource competence in understanding the technical aspects of information technology, the complexity of digital forensic proof, cross-border jurisdictional issues, and infrastructure and budget limitations (Suryawin et al., 2026).

The same problem is also seen in research on the effectiveness of handling cybercrime at the police level. Law enforcement against *Cybercrime* can run in accordance with applicable legal procedures, but does not necessarily achieve the optimal level of effectiveness. Limited facilities, technical capabilities of law enforcement officials, and uneven special units that handle cybercrimes can be inhibiting factors in the law enforcement process (Caesar, 2021).

Sitanggang, Darmawan, and Saputra also stated that cyber law enforcement in Indonesia still faces challenges in the form of limited resources and technical skills even though various regulations have been developed to deal with crime in the digital space (Sitanggang, Darmawan, & Saputra, 2024). This shows that the success of law enforcement against *cybercrime* is not only determined by the availability of regulations, but also the ability of law enforcement institutions to implement these regulations.

Therefore, law enforcement against *cybercrime* requires a comprehensive approach. Strengthening regulations needs to be followed by increasing the competence of the apparatus, developing digital forensic facilities, increasing coordination between the police, prosecutor's office, courts and related agencies, and international cooperation in dealing with cross-border

crimes. With the fulfillment of these various aspects, the implementation of law enforcement against *cybercrime* is expected to provide legal certainty, protection for victims, as well as create a preventive effect on the development of crime in the digital space.

Research Methodology

This research uses normative *juridical research* methods. Normative legal research is research conducted by examining legal norms, legal principles, laws and regulations, doctrines, and various literature related to the legal issues being studied. This method is used because the research focuses on analyzing the implementation of law enforcement against *cybercrime* crimes in Indonesia based on applicable legal provisions.

The approach used in this study consists of a statute *approach* and a *conceptual approach*. The legislative approach is carried out by examining various regulations related to *cybercrime*, especially Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, including Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, the Criminal Code, and other relevant regulations. Meanwhile, a conceptual approach is used to analyze the concepts of law enforcement, criminal acts, *cybercrime*, electronic evidence, and other legal aspects related to cybercrime.

The type of data used in this study is secondary data consisting of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations related to *cybercrime* and law enforcement in Indonesia. Secondary legal materials include books, scientific journals, research results, academic articles, and expert opinions relevant to research problems. The tertiary legal materials are in the form of legal dictionaries, encyclopedias, and other sources that provide explanations of primary and secondary legal materials.

The data collection technique is carried out through library *research* by identifying, inventorying, reading, and analyzing various relevant legal sources and literature. The data obtained is then selected based on its relationship with research problems, especially regarding the legal basis, the implementation of law enforcement, obstacles faced by law enforcement officials, and efforts that can be made in dealing with *cybercrime*.

Furthermore, the data was analyzed using a descriptive qualitative analysis method. The analysis was carried out by describing the applicable legal provisions, connecting them with the theory and concept of law enforcement, and then assessing their implementation in the context of handling *cybercrime* in Indonesia. The results of the analysis were then systematically compiled to obtain an overview of the implementation of law enforcement, the various obstacles faced, and the efforts needed to increase the effectiveness of law enforcement against *cybercrime* crimes in Indonesia.

Results

Implementation of law enforcement against criminal acts *Cybercrime* in Indonesia is an important part of providing certainty and legal protection to the public amid the increasing use of information technology. Cybercrime has different characteristics from conventional crimes because it is carried out by utilizing computers, internet networks, and electronic systems and can occur without being limited by geographical area. This condition causes the law enforcement process to require legal instruments and technical capabilities that are able to keep up with technological developments. Indonesia already has a legal basis through Law Number 11 of 2008 concerning Information and Electronic Transactions which has undergone changes through Law Number 19 of 2016 and Law Number 1 of 2024. The latest changes were made, among others, to overcome provisions that in their implementation still cause multiple

interpretations and strengthen legal certainty and a sense of justice in society (Republic of Indonesia, 2024).

In the law enforcement process, one of the important aspects in handling *cybercrime* is proof. Article 5 of the Electronic Information and Transaction Law emphasizes that electronic information, electronic documents, and/or printed results are legal evidence and an extension of evidence in accordance with the procedural law applicable in Indonesia (Republic of Indonesia, 2024). This provision provides a basis for law enforcement officials to use digital evidence in the process of investigation, investigation, prosecution, and examination in court. In addition to the ITE Law, Law Number 27 of 2022 concerning Personal Data Protection is also related to the handling of digital crime because it regulates prohibitions on the use of personal data and criminal provisions related to the protection of personal data (Republic of Indonesia, 2022).

Despite the support of laws and regulations, the implementation of law enforcement against *cybercrime* still faces various obstacles. The rapid development of digital crime modes causes law enforcement officials to continue to improve their knowledge and abilities in the field of information technology. Research by Suryawin et al. shows that the implementation of law enforcement against cybercrime still faces obstacles in the form of limited human resources, the complexity of digital forensic proof, cross-border jurisdictional issues, and limited infrastructure and budgets (Suryawin et al., 2026). This condition shows that there is a gap between the development of technology-based crime and the available law enforcement capacity.

The issue of jurisdiction becomes increasingly important because the perpetrator of the crime can be in a different country from the victim or the location of the electronic system being attacked. Handling cases like this requires inter-agency coordination and international cooperation in obtaining information, tracking perpetrators, and obtaining electronic evidence. Studies on *transnational cybercrime* show that Indonesia already has a number of legal instruments and institutions that support the handling of cybercrime, but still faces obstacles in the form of jurisdictional limitations, harmonization of rules between countries, technology, and human resources (Martono, Akbar, & Rahmatiar, 2025).

In addition to a repressive approach through the criminal process, *countering cybercrime* also requires a preventive approach. Prevention can be done through increasing digital literacy, protecting electronic systems, increasing public awareness of data security, and stronger coordination between the government, police, electronic system operators, and the public. This collaboration is increasingly important because the pattern of digital crime continues to develop, ranging from online fraud to crimes targeting vulnerable groups. In 2026, the Ministry of Communication and Digital together with the National Police also emphasized strengthening integrated enforcement and cross-agency collaboration in dealing with digital crime (Ministry of Communication and Digital, 2026).

Thus, the implementation of law enforcement against criminal acts *Cybercrime* Indonesia already has a fairly developed legal basis, but the effectiveness of its implementation still needs to be improved. Strengthening the capacity of law enforcement officials, digital forensic facilities, inter-agency coordination, international cooperation, and regulatory updates that are adaptive to technological developments are important steps so that law enforcement is able to provide legal certainty, protect victims, and prevent the development of crime in the digital space.

The implementation of law enforcement against *cybercrime* in Indonesia is a form of state response to the development of information technology that has consequences for the emergence of various new forms of crime. Cybercrime has a different character from conventional crime because it can be carried out without physical contact between the perpetrator and the victim, uses a digital identity that is difficult to trace, and is not limited by geographical area. In the context of national law, law enforcement against *cybercrime* aims to

provide protection for the interests of the community while creating legal certainty in the use of information technology. Soekanto explained that the success of law enforcement is influenced by legal regulatory factors, law enforcement officials, facilities and facilities, society, and legal culture (Soekanto, 2022). The concept shows that the success of *cybercrime eradication* does not only depend on the existence of regulations, but also the readiness of all law enforcement components.

Normatively, Indonesia already has a number of regulations that are the basis for handling cybercrimes. One of the main regulations is Law Number 11 of 2008 concerning Information and Electronic Transactions which was later amended through Law Number 19 of 2016 and finally through Law Number 1 of 2024. The second amendment to the ITE Law was carried out because a number of previous provisions in its implementation still caused multiple interpretations and controversies, so improvements are needed to provide legal certainty and a sense of justice to the public (Republic of Indonesia, 2024). Law Number 1 of 2024 takes effect from January 2, 2024 and changes a number of provisions in the previous regulation. In addition to the ITE Law, the handling of crimes related to the misuse of personal data is also strengthened through Law Number 27 of 2022 concerning Personal Data Protection which regulates the rights of data subjects, the obligations of data controllers and processors, the prohibition of the use of personal data, and criminal provisions (Republic of Indonesia, 2022).

One of the important aspects of law enforcement against *cybercrime* is the evidentiary process. Crimes that occur through electronic systems generally produce electronic information and documents that must be found, secured, examined, and maintained for the sake of the legal process. This condition causes law enforcement officials to not only understand criminal law and criminal procedure law, but also require skills in the field of information technology and digital forensics. Suryawin et al. found that law enforcement against *cybercrime* in Indonesia still faces limited human resource competencies in understanding the technical aspects of information technology, the complexity of digital forensic proof, cross-border jurisdictional issues, and infrastructure and budget limitations (Suryawin et al., 2026). Therefore, improving the competence of investigators and developing digital forensic facilities is an important part of increasing the success of case disclosure.

Another problem faced is the nature of *cybercrime* that can go beyond the boundaries of a country's jurisdiction. Perpetrators can carry out actions from outside Indonesian territory, use electronic systems located in other countries, or store data on cross-border digital services. This situation causes the process of identifying perpetrators and collecting evidence to be not always completed using domestic law enforcement mechanisms. Thus, it is necessary to strengthen international coordination and cooperation, especially in information exchange, digital evidence security, perpetrator identification, and legal processes against transnational cybercrimes. This approach is important because technological developments allow criminal acts to be carried out quickly while the law enforcement process must still pay attention to applicable legal procedures and jurisdictions.

In addition to a repressive approach, *cybercrime must* also be carried out through a preventive approach. The government, police, electronic system operators, the private sector, educational institutions, and the community need to build prevention mechanisms through increasing digital literacy, system security, personal data protection, and ease of reporting digital crimes. By 2026, the Ministry of Communication and Digital and the National Police will strengthen coordination in handling digital crime, including through the integration of reporting systems and increased collaboration across agencies (Ministry of Communication and Digital, 2026). This shows that law enforcement against *cybercrime* requires an integrated approach that is not solely oriented towards punishing perpetrators.

Based on this description, it can be understood that the implementation of law enforcement against *cybercrime* in Indonesia has been supported by an increasingly growing legal apparatus. However, its effectiveness is still determined by the capabilities of the

apparatus, the availability of digital forensic technology, inter-institutional coordination, community participation, and international cooperation. Therefore, improving the quality of human resources, strengthening technological infrastructure, updating adaptive regulations, and increasing public awareness are strategic steps so that law enforcement against *cybercrime* can provide legal certainty, protection for victims, and create a safe digital space for the community.

Conclusion

Based on the results of the discussion, it can be concluded that the implementation of law enforcement against *cybercrime* in Indonesia has a fairly strong legal foundation through Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, especially Law Number 1 of 2024, and is supported by other regulations such as Law Number 27 of 2022 concerning Personal Data Protection. The existence of these regulations provides a basis for law enforcement officials to conduct investigations, investigations, evidence, and prosecutions of various forms of crimes committed through electronic systems.

However, the effectiveness of law enforcement against *cybercrime* still faces various obstacles. These obstacles include the rapid development of crime modes, limited human resources who have competence in the field of information technology and digital forensics, limited facilities and infrastructure, difficulties in maintaining and proving the validity of electronic evidence, and jurisdictional issues if the crime involves perpetrators, victims, or electronic systems located in different countries. These conditions show that the existence of laws and regulations alone is not enough to ensure the success of law enforcement.

Therefore, more comprehensive efforts are needed through improving the competence of law enforcement officials, strengthening digital forensic facilities, increasing inter-agency coordination, strengthening international cooperation, and updating regulations that are able to keep up with technological developments. In addition to repressive actions against perpetrators, preventive efforts through increasing digital literacy, personal data protection, and public awareness of cyber security also need to be strengthened. With the support of regulations, apparatus, technology, the community, and integrated cooperation, law enforcement against *cybercrime* crimes in Indonesia is expected to run more effectively and be able to provide legal certainty and protection for the public in the digital space.

References

[1] Abidin, D. Z. (2017). Crime in information and communication technology. *Journal of PROCESSOR, 10*(2), 509–516.

[2] Arifin, Z., & Handayani, E. P. (2023). *Cybercrime: Investigating Law Enforcement and Its Countermeasures*. Yogyakarta: Deepublish.

[3] Caesar, L., Angkasa, & Ningrum, D. H. R. (2021). The effectiveness of law enforcement against cybercrime by the Cybercrime Unit at the Banyumas Police. *Soedirman Law Review, 3*(1), 161–169. doi:10.20884/1.slr.2021.3.1.128.

[4] Idris, M., Nurlani, M., & Aprita, S. (2024). Regulation and enforcement of cyber *crime law*: Harmonization of the revision of the ITE Law and the Criminal Code. *Lex Lata: Scientific Journal of Law, 6*(3), 396–411. doi:10.28946/lexl.v6i3.4266.

[5] Gemilang, G., & Ismaidar, I. (2024). The politics of restorative justice law in criminal law reform in Indonesia. *Innovative: Journal of Social Science Research, 4*(1), 7370-7382.

[6] Syahranuddin, S. H., & Ramadani, S. S. (2023). Criminal Law Policies in Overcoming Cyber Crime in Indonesia. In *Proceedings of The International Conference on Multi-Disciplines Approaches for The Sustainable Development* (pp. 738-742).

[7] Telaumbanua, S. E., Ismaidar, I., & Ramadani, S. (2025). The Position of Customary Criminal Law in The Development of The Legal System in Indonesia Based on The

Criminal Code Number 1 Of 2023. *Journal of Research in Social Science and Humanities, 5*(2).