Law Synergy Conference (LSC)
E-ISSN: 3048-3530
Volume I; Number I; Month 6, Year 2024; Pages 179-185
Him :-
Website: https://sinergilp.com

Effectiveness of Law Enforcement against Cybercrime in Indonesia Study on Hacking Crimes and the Role of the ITE Law

Wildan Fahriza[1],Muhammad Arif Sahlepi[2].Rahmayanti[3].
wildanfahriza111@gmail.com arifsahlepi@gmail.com rahmayanti@dosen.pancabudi.ac.id
[123]Panca Budi Development University

Abstract

This study aims to analyze the effectiveness of law enforcement against hacking crimes in Indonesia, focusing on the role of the Electronic Information and Transactions Law (UU ITE). Cybercrime, especially hacking, has grown rapidly along with technological advances, but law enforcement against this crime still faces various challenges. Through a normative legal approach, this study evaluates the implementation of the ITE Law in handling hacking cases, and identifies major obstacles such as limited technical competence of law enforcement officers, jurisdictional limitations, and lack of international cooperation. The results of the study indicate that although the ITE Law provides a sufficient legal basis, regulatory updates are still needed to be more responsive to technological developments. In addition, increasing the capacity of law enforcement officers and strengthening international cooperation are considered important to deal with cross-border hacking crimes. This study recommends strategic steps, including technical training, regulatory revisions, and increased protection of personal data, to improve the effectiveness of law enforcement in Indonesia.

Keywords:*Hacking crime, ITE Law, cyber crime*

INTRODUCTION

In the era of globalization and the development of information technology, cybercrime has become a significant threat throughout the world, including in Indonesia. The advancement of digital technology has enabled various conveniences, but on the other hand, it has also provided a wide space for criminal acts in cyberspace. One of the most prominent forms of cybercrime is the crime of hacking, which involves illegal access to a computer system or network for various purposes, ranging from data theft to destruction of digital infrastructure.

Indonesia, as one of the countries with an increasing internet adoption rate, faces an increasing risk of hacking threats. Based on data from the National Cyber and Crypto Agency (BSSN), cyber attacks in Indonesia have increased every year. In 2020, there were more than 423 million cyber attacks detected, many of which involved hacking crimes. This shows that Indonesia is one of the main targets for cybercriminals, both domestic and foreign.(Trisnawati and Hanifah 2024)

One of the biggest challenges in handling cybercrime, especially hacking, is how the law can effectively address and enforce sanctions against perpetrators of this crime. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was later amended by Law Number 19 of 2016, is the main legal instrument that regulates cybercrime in Indonesia. The ITE Law provides a legal basis for law enforcement against various forms of cybercrime, including hacking, but its effectiveness is still often questioned.(Rianto, Zarzani, and Saragih 2024)

The main problems faced in enforcing the law against hacking crimes in Indonesia are related to several factors:

1. Lack of technical understanding in law enforcement: Law enforcement in Indonesia often faces difficulties in understanding the technical aspects of cybercrime. Hacking involves very complex

techniques, so it requires a deep understanding of information technology to be able to collect evidence, identify perpetrators, and process cases in court.

2. Jurisdictional boundaries: Hacking crimes often involve perpetrators from other countries, making law enforcement efforts more difficult. Indonesia has limited legal jurisdiction to prosecute criminals operating from abroad. This makes the legal process against hackers based abroad more difficult and complex.
3. Weaknesses in legal and technological infrastructure: Although the ITE Law provides a legal framework to combat cybercrime, Indonesia's legal and technological infrastructure is still inadequate to deal with the increasing scale of cyber threats. This is evident from the limitations in terms of expertise, security technology, and international cooperation in dealing with transnational cybercrime.
4. Unclear definition and scope of ITE Law: Several articles in ITE Law, especially those regulating hacking, are still considered too general and do not provide a clear definition of actions that can be categorized as hacking crimes. This ambiguity often causes problems in the prosecution and evidence process in court.(Medaline, Zarzani, and Sari 2020)

This research is very important considering the rapid development of cybercrime in Indonesia, which is often not balanced with effective law enforcement capabilities. When cybercrime such as hacking cannot be handled properly, it not only endangers the security of individual and corporate data, but also has an impact on national stability and Indonesia's digital economy. Therefore, a critical evaluation of the effectiveness of the ITE Law in dealing with hacking crimes is needed, with the aim of providing recommendations to improve the legal framework and law enforcement in Indonesia.

In this study, we will explore two main issues: How effective is law enforcement against hacking crimes in Indonesia based on the ITE Law? What are the main challenges faced by law enforcement in dealing with hacking crimes, and how can regulations be improved to address these issues? Through this study, it is expected to produce an in-depth analysis of the effectiveness of the ITE Law in dealing with cybercrime, as well as provide solutions to the various challenges faced in law enforcement.

METHOD

This research uses a normative legal approach(Indra Utama Tanjung 2024)with analytical descriptive method. The focus of this study is on the analysis of laws and regulations relevant to the crime of hacking, especially the ITE Law. The data sources used are primary legal materials, such as related laws and regulations, as well as secondary legal materials, such as journals, legal articles, and research reports. The data will be analyzed qualitatively to evaluate the effectiveness of law enforcement and identify the challenges faced in the practice of law enforcement against the crime of hacking in Indonesia.

RESULTS AND DISCUSSION

Effectiveness of Law Enforcement against Hacking Crimes in Indonesia Based on the ITE Law

Law enforcement against hacking crimes in Indonesia is specifically regulated by Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments. The ITE Law is the main instrument in dealing with cybercrime, which covers various crimes, including hacking. Article 30 of the ITE Law regulates the act of illegally accessing electronic systems that is carried out intentionally and without rights, which is the basis for action against hackers.(Rhamadhani, Rahman, and Badaru 2022)

Article 30 of the ITE Law is divided into several verses that regulate hacking categories:

Article (1) regulates the act of accessing a computer or electronic system without permission.

Article (2) emphasizes the act of accessing an electronic system with the intention of obtaining information that does not belong to him.

Article (3) concerns acts of illegal access that cause disruption to electronic systems.

However, the effectiveness of law enforcement against hacking crimes based on the ITE Law still raises a number of questions. From the perspective of the theory of legal efficacy put forward by Soerjono Soekanto, the law can be said to be effective if it meets several elements, namely legal substance, law enforcement officers, facilities and infrastructure, and public legal awareness. Based on this theory, we can assess the effectiveness of hacking law enforcement in Indonesia.

Substantially, Article 30 of the ITE Law has indeed provided a fairly clear legal basis for prosecuting hacking. However, there are still some weaknesses in its implementation. One of the main problems is the lack of a specific definition related to the forms of hacking. The ITE Law does not provide a detailed definition of various hacking methods such as phishing, brute force, or ransomware. This ambiguity makes the interpretation of the law very dependent on the technical understanding of law enforcement officers, which is not always adequate.(Yudhisthira and Ramadani 2023)

In addition, not all hacking acts can be clearly regulated in the ITE Law, especially new types of crimes that emerge along with the development of information technology. Some more sophisticated hacking techniques, such as attacks via the Internet of Things (IoT) or attacks using Artificial Intelligence (AI), are not specifically covered in this regulation. Therefore, the substance of the ITE Law needs to be updated to be more responsive to increasingly complex technological developments. Law enforcement against hacking crimes is highly dependent on the competence of law enforcement officers, especially in terms of understanding and handling technical cases. Law enforcers in Indonesia, both at the investigator, prosecutor, and judge levels, often face challenges in understanding how cyber attacks work in detail.

Law Enforcement Theory according to Lawrence M. Friedman states that the success of law enforcement is influenced by three elements, namely legal structure, legal substance, and legal culture. In Indonesia, although the legal structure already exists, law enforcement officers often have difficulty in handling hacking cases that require technical knowledge. The large number of hacking cases that are not resolved properly raises questions about the competence of law enforcement officers in identifying perpetrators and understanding digital evidence. Although various efforts have been made to improve the capabilities of law enforcement officers through technical training, the results are still not optimal. Many hacking cases ultimately cannot be resolved due to lack of evidence or errors in the procedures for handling electronic evidence. Therefore, improving the competence of law enforcement officers is an urgent need so that law enforcement against hacking can run more effectively.(Trisnawati and Hanifah 2024)

In terms of facilities and infrastructure, law enforcement against hacking crimes also still faces obstacles. The support system for handling cybercrime in Indonesia is still not optimal, especially in terms of the technology used by law enforcement officers. Many police stations and law enforcement agencies are not yet equipped with adequate technology to comprehensively track and analyze hacking activities. One important technology in handling cybercrime is digital forensics, which allows the collection and analysis of digital evidence from computers or networks. However, in Indonesia, digital forensics is still not fully developed. In some cases, the collection of digital evidence is carried out in a manner that is not in accordance with standards, so that the evidence obtained cannot be used in court. This shows that the supporting facilities used by law enforcement officers in handling hacking crimes need to be significantly improved.

Public legal awareness is also a determining factor in the effectiveness of law enforcement. In the context of cybercrime, many hacking victims do not report their cases because they do not understand their rights or because they feel that the legal system will not provide adequate solutions. In addition, many internet users in Indonesia do not fully understand the threat of hacking crimes, so they often do not take sufficient precautions. This lack of awareness is a major problem in efforts to prevent hacking crimes. According to the Legal Compliance Norm theory put forward by Tom R. Tyler, compliance with the law depends not only on legal sanctions, but also on the public's understanding and acceptance of these legal norms. Therefore, there needs to be a more systematic effort to increase public awareness of cybercrime and the importance of reporting every hacking crime that occurs.(Nurdin1 et al., nd)

Challenges in Enforcing Hacking Crimes

One of the biggest challenges in law enforcement against hacking crimes is jurisdictional limitations. Cybercrimes such as hacking are often committed by perpetrators outside of Indonesia, making law enforcement difficult. Although the ITE Law has provided a legal basis for handling cybercrimes, this law has

limitations in terms of taking action against perpetrators operating outside of Indonesia's jurisdiction.(Dhadha et al. 2021)

Based on the principle of territoriality in criminal law, law enforcement jurisdiction is usually limited by the borders of a country. However, cybercrime often involves perpetrators operating from various countries using networks that are difficult to trace. This causes law enforcement officers in Indonesia to have difficulty in identifying and arresting perpetrators based abroad.

International cooperation is very important in handling transnational cybercrime. Indonesia needs to increase collaboration with other countries through extradition agreements and international law enforcement cooperation, such as the Budapest Convention on Cybercrime, which is the main international instrument in dealing with transnational cybercrime. Although Indonesia has not ratified this convention, steps towards international cooperation need to be increased to ensure that perpetrators of hacking crimes can be brought to justice.(Mighty and Pakpahan 2023)

As a cross-border crime, hacking requires multilateral cooperation between countries and international bodies. At the global level, international conventions such as the Budapest Convention provide a framework for countries to jointly address cybercrime. However, Indonesia has not yet become a full member of this convention, so law enforcement efforts against hacking crimes involving perpetrators from abroad often encounter obstacles.

In addition, several countries that are the center of hacking activities do not have extradition cooperation with Indonesia, which causes many cybercrime cases to not be processed properly. Although the ITE Law provides a legal basis for handling cybercrime, law enforcement against perpetrators based abroad is often hampered by diplomatic and international relations constraints.

On the other hand, the challenges in enforcing the law against hacking crimes also include aspects of data security and privacy. In hacking cases, the data that is often stolen or manipulated is the personal data of internet users or companies. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has been passed to provide better protection for personal data, but its enforcement still needs to be strengthened.(Ninggeding, Bayuaji, and Indriastuty 2023)Personal data stolen or hacked in hacking attacks is often used for other criminal purposes such as fraud or money laundering. Therefore, the PDP Law and the ITE Law need to be more closely integrated in law enforcement efforts against hacking crimes, so that protection of personal data can be optimized.

Challenges and Solutions in Law Enforcement of Hacking Crimes in Indonesia

Having discussed the effectiveness of law enforcement against hacking crimes in Indonesia, it is important to further explore the main challenges faced in the law enforcement process and how existing regulations can be improved to address these challenges. In this context, three key aspects that need to be analyzed are the lack of technical understanding among law enforcement officers, regulations that are not yet fully adaptive to technological developments, and the need for better international cooperation.(Ersya 2017)

One of the main challenges in law enforcement against hacking crimes is the lack of technical understanding of law enforcement officers, including police, prosecutors, and judges. Hacking is a highly technical crime, requiring a deep understanding of information technology, networks, encryption, and computer security systems. Law enforcement officers who do not have adequate technical backgrounds often have difficulty in collecting evidence, analyzing attack patterns, and understanding the methods used by the perpetrators.(AR Hakim and Tanjung 2024)

In criminal law theory, the law enforcement theory by Lawrence M. Friedman explains that the success of law enforcement is highly dependent on three elements: legal substance, legal structure, and legal culture. In the context of handling hacking, challenges arise in the aspect of legal structure, which includes the quality and competence of law enforcement officers themselves. Lack of technical knowledge makes law enforcement sometimes unable to understand the scale and impact of hacking attacks, leading to low success rates in law enforcement against hackers.

To address this issue, capacity building is needed through continuous and specialized training for law enforcement officers. This training should cover technical aspects of digital forensics, how to trace cyber attacks, and methods for handling electronic evidence. Countries such as the United States and the United Kingdom have developed special units to handle cybercrime, such as the FBI Cyber Division and the National

Cyber Security Center in the United Kingdom, which are equipped with human resources with high technical capabilities. Indonesia can learn from this approach by strengthening cyber units in the police and improving the technical capabilities of personnel handling cybercrime cases.(Dewantoro and Dian Alan Setiawan SH 2023)

Hacking crimes continue to develop along with the development of information technology. Hacking methods used by perpetrators also continue to change and become more sophisticated, ranging from the use of ransomware, distributed denial of service (DDoS) attacks, to Internet of Things (IoT)-based attacks. However, existing regulations, including Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), are still limited in dealing with new types of cybercrime.

The ITE Law has indeed been revised in 2016, but the revision regulates more aspects such as online insults and defamation, rather than expanding the scope of the law to handle more complex cybercrimes. Hacking crimes, especially those involving advanced technologies such as AI or blockchain, are still not specifically regulated in the ITE Law. As a result, many hacking cases using new technologies are difficult to prosecute effectively in court.

The legal responsiveness theory by Philip Selznick proposes that the law must be adaptive and able to respond to ever-changing social and technological developments. In this case, the ITE Law and related regulations must be updated regularly to face the increasingly complex challenges of cybercrime. One example of a more responsive regulation is the General Data Protection Regulation (GDPR) in the European Union, which includes strict rules on data security and the obligations of companies to protect users' personal information from cyber attacks. Indonesia can learn from this approach and expand the scope of more specific regulations related to hacking, for example by including provisions on the responsibilities of digital platforms or internet service providers in protecting systems from cyber attacks.(Badaru 2021)

Cybercrimes such as hacking often involve actors operating across borders, creating jurisdictional challenges. Many hackers operate from overseas, exploiting weaknesses in national regulations and using their remote physical locations to evade law enforcement. In this regard, law enforcement against hacking requires strong international cooperation.

International agreements on combating cybercrime are crucial in addressing these challenges. One of the most prominent international frameworks is the Budapest Convention on Cybercrime, adopted by European and other countries as the main international legal instrument to combat cross-border cybercrime. The convention provides guidance for member states to strengthen cooperation in law enforcement against cybercrime, including hacking. Countries that have ratified the convention are required to assist each other in the investigation, collection of evidence, and extradition of cybercriminals.(Setiawan 2021)

Unfortunately, until now Indonesia has not become a full member of the Budapest Convention. This makes Indonesia have less access to international law enforcement mechanisms that can facilitate the handling of cross-border hacking cases. To overcome this, the Indonesian government needs to consider ratifying the Budapest Convention or increasing bilateral and multilateral cooperation with other countries in terms of information exchange, joint investigations, and extradition of cybercriminals.(Handoyo, Husamuddin, and Rahma 2024)

In addition, Interpol and other international organizations have played an important role in supporting their member countries to deal with cybercrime. Through the Cybercrime Operations Desk program, Interpol assists member countries in investigating hacking cases involving perpetrators from various countries. Indonesia can utilize these cooperation platforms to more effectively handle hacking cases involving international perpetrators.

Hacking crimes are often closely related to the theft or manipulation of personal data, which has serious implications for individual privacy and corporate security. In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has provided a legal framework to protect internet users' personal data from misuse, but its enforcement still needs to be strengthened.(R. Hakim 2023)

The PDP Law includes provisions regarding the obligations of companies or electronic system organizers to maintain the security of personal data, as well as giving individuals the right to sue in the event of data leaks or misuse. In the context of hacking, the PDP Law is very important because personal data is often the main target of hackers. Cases of large-scale data theft involving large companies in Indonesia show that data security violations still occur frequently.(Ali 2023)

Strengthening the PDP Law in enforcing the law against hacking must be done by integrating this regulation with the ITE Law, so that handling hacking crimes can be more comprehensive. In addition, technology companies also need to be more proactive in reporting security breaches and strengthening their cybersecurity infrastructure. The government also needs to provide stricter sanctions for companies that do not comply with data protection rules, including significant fines to provide a deterrent effect.

Law enforcement against hacking crimes in Indonesia still faces various challenges, ranging from the lack of technical understanding of law enforcement officers, regulations that are not fully responsive to technological developments, to limited international cooperation. Although Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) provides an important legal framework, the substance and implementation of this law still need improvement in order to be more effective in dealing with cybercrimes such as hacking.(Muliadi and Assaad 2024)Another challenge faced is the protection of personal data which is often the target of attacks in hacking crimes. The newly passed Personal Data Protection Law needs to be better integrated with the ITE Law, so that law enforcement against hacking can provide better protection for individual data and privacy.

Recommendations that can be taken from this study include improving the technical competence of law enforcement officers through training and capacity building, updating regulations to be more adaptive to technological developments, strengthening international cooperation in handling cross-border cybercrime, and ensuring that the Personal Data Protection Law is implemented properly to protect personal data from hacking attacks. With these efforts, law enforcement against hacking in Indonesia can be more effective, and the threat of cybercrime can be better handled.(Duarif and Saleh 2024)

CONCLUSION

The conclusion of this study shows that law enforcement against hacking crimes in Indonesia, although regulated in the Electronic Information and Transactions Law (UU ITE), still faces a number of significant challenges. Although the ITE Law provides a clear legal basis, implementation in the field has not been fully effective due to various factors, such as the lack of technical understanding of law enforcement officers and limitations in the technological infrastructure that supports digital forensics. This challenge is exacerbated by the cross-border nature of hacking crimes, where national legal jurisdiction is often insufficient to prosecute perpetrators operating abroad. Regulations that are not fully responsive to technological developments, such as the use of the Internet of Things (IoT) and blockchain, also add to the complexity of dealing with increasingly sophisticated cybercrimes. On the other hand, protection of personal data and privacy, although strengthened through the Personal Data Protection Law (UU PDP), still requires stricter enforcement and better integration with the ITE Law. In addition, international cooperation is an important aspect that must be strengthened so that Indonesia can participate more actively in dealing with transnational cybercrimes, such as through ratification of relevant international conventions. To improve the effectiveness of law enforcement, it is necessary to increase the technical capacity of law enforcement officers, update regulations that are adaptive to technological developments, and strengthen international cooperation in handling hacking cases. With these steps, it is hoped that Indonesia can better face the threat of cybercrime and provide stronger legal protection for society in the digital era.

BIBLIOGRAPHY

Ali, H Zainuddin. 2023. Sociology of Law. Sinar Grafika.

Badaru, Baharuddin. 2021. “Effectiveness of Investigations into Criminal Acts of Spreading Fake News Through Online Media.” Journal of Lex Generalis (JLS) 2 (5): 1692–1702.

Dewantoro, Naufal Mahira, and MH Dian Alan Setiawan SH. 2023. “Law Enforcement of Phishing-Based Cybercrime in the Form of Application Package Kit (APK) Based on the Electronic Information and Transactions Law.” In Bandung Conference Series: Law Studies, 3:892–900.

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, and Dora Kusumastuti. 2021. “The Effectiveness of the Role of the ITE Law in Protecting and Maintaining All Cyber Activities in Indonesia.” Legal Standing: Journal of Legal Studies 6 (1): 40–48.

Duarif, Duarif, and Moh Saleh. 2024. “Prevention and Action against Cyber Crime by Teluk Bintuni Resort Police.” UNES Law Review 6 (4): 12110–19.

Ersya, Muhammad Prima. 2017. “Legal Issues in Tackling Cyber Crime in Indonesia.” Journal of Moral and Civic Education 1 (1): 50–62.

Hakim, Aulia Rahman, and Indra Utama Tanjung. 2024. "The Principle of the Reverse Burden of Proof of Corruption Crimes in the Legal System in Indonesia." In Law Synergy Conference Proceedings, 1:7–11.

Hakim, Rohman. 2023. “Law Enforcement of Criminal Acts of Drug Abuse by Children in the Perspective of Law Number 35 of 2009.” Journal of Legal Preferences 4 (2): 279–91.

Handoyo, Budi, MZ Husamuddin, and Ida Rahma. 2024. “Legal Review of Cyber Crime Law Enforcement Study of the Implementation of Law Number 11 of 2008.” MAQASIDI: Journal of Sharia and Law, 40–55.

Indra Utama Tanjung. 2024. BASICS OF LEGAL RESEARCH METHODS. Karanganyar: CV Pustaka Dikara). https://scholar.google.com/citations?view_op=view_citation&hl=id&user=rToGqjUAAAAJ&cstart=20&pagesize=80&citation_for_view=rToGqjUAAAAJ:Wp0gIr-vW9MC.

Medaline, Onny, T Riza Zarzani, and Ayumi Kartika Sari. 2020. "Revitalization of Complete Systematic Land Registration (PTSL) Program as a Form of Agrarian Reform in the Field of Socioeconomic Mapping of Society." International Journal of Research and Reviews 7 (10): 108–14.

Muliadi, Muliadi, and A Istiqlal Assaad. 2024. “The Effectiveness of Police Functions in Investigating Misuse of Information and Electronic Transactions.” Journal of Lex Philosophy (JLP) 5 (1): 237–54.

Ninggeding, Narto Yabu, Rihantoro Bayuaji, and Dwi Elok Indriastuty. 2023. “Law Enforcement Against Cyber Crime in the Banking Sector in Indonesia.” Wijaya Putra Journal of Legal Studies 1 (2): 215–24.

Nurdin1, Merry Kurniawati, Chika Aurel Rivaldi, Novia Rahmadani, Hilyah Az Zahra4, Andika Rayhan, and Putra Herang5. nd “THE ROLE OF TELEMATICS LAW IN SOLVING CYBERCRIME CASES.”

Perkasa, Anggada, and Kartina Pakpahan. 2023. “Law Enforcement Policy in Combating Gambling Crimes Through Electronic Media in Indonesia.” SIBATIK JOURNAL: Scientific Journal in the Fields of Social, Economic, Cultural, Technology, and Education 2 (7): 2067–84.

Rhamadhani, Ayuning Tyas, Sufirman Rahman, and Baharuddin Badaru. 2022. “Effectiveness of Cyber Crime Investigation Process: Case Study of Gowa Police.” Journal of Lex Theory (JLT) 3 (2): 49–64.

Rianto, Rianto, T Riza Zarzani, and Yasmirah Mandasari Saragih. 2024. “Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Criminal Acts.” JIIP-Journal of Scientific Education 7 (1): 393–98.

Setiawan, M Nanda. 2021. “Criticizing the ITE Law Article 27 Paragraph (3) Viewed from the Socio-Politics of Indonesian Criminal Law.” DATIN Law Journal 2 (1): 1–21.

Trisnawati, Trisnawati, and Shofia Hanifah. 2024. “DEVELOPMENT OF ELECTRONIC EVIDENCE RESULTING FROM HACKING AS EVIDENCE IN CRIMINAL ACTS.” Multidisciplinary Indonesian Center Journal (MICJO) 1 (3): 1344–49.

Yudistira, Muhammad, and Ramadani Ramadani. 2023. “Legal Review of the Effectiveness of Handling Cybercrime Related to Personal Data Theft According to Law No. 27 of 2022 by KOMINFO.” UNES Law Review 5 (4): 3917–29.