Volume 1 Issue 2 (2024) 32-39
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v1i2.5
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Law Enforcement Against Cyber Crimes in Indonesia: Analysis of the Role of the ITE Law in Handling Cyber Crimes

Waluyadi Waluyadi
Universitas Swadaya Gunung Jati Cirebon
Corresponding email:waluyadi01@gmail.com

ABSTRACT

Cybercrime in Indonesia is increasing along with the development of information technology. The Electronic Information and Transactions Law (UU ITE) is present as the main legal instrument to regulate and overcome various forms of cybercrime. However, the implementation and enforcement of laws related to the ITE Law are still controversial, especially in handling cases involving privacy, defamation , and hate speech in the digital space. This study examines the effectiveness of the ITE Law in enforcing laws related to cybercrime in Indonesia. This study aims to analyze the role and effectiveness of the ITE Law in combating cybercrime in Indonesia, as well as identifying the challenges faced in the law enforcement process. The research method used is normative juridical with a qualitative approach. Data were collected through literature studies that include analysis of laws, government regulations, and case studies of cyber crimes that have been legally processed in Indonesia. This study found that although the ITE Law has become an important basis for law enforcement against cybercrime, there are still weaknesses in its implementation, such as a lack of understanding of the law by law enforcers and ambiguity in the application of related articles. Several cases show that the ITE Law can be misused, so better legal reform and harmonization are needed to effectively address cybercrime.

Keywords: Law enforcement, cyber crime, ITE Law, cyber crime Indonesia

1. Introduction

Along with the rapid development of information and communication technology in Indonesia, the number of internet users has also experienced a significant increase (Faizah et al., 2021; Gunawan, 2019). According to data from the Indonesian Internet Service Providers Association (APJII), in 2023, the number of internet users in Indonesia will reach more than 210 million people. This figure reflects

the increasing importance of digital aspects in people's lives, but is also accompanied by an increasing risk of cybercrime. Cybercrime, which involves violations of the right to information, data theft, online fraud, and system hacking, is a serious threat to individual and state security. In this context, the Indonesian government has enacted the Electronic Information and Transactions Law (UU ITE) as the main legal instrument to address cybercrime.

The urgency of this research lies in the urgent need to evaluate the effectiveness of law enforcement against cybercrime in Indonesia through the ITE Law instrument (Gustryan & Sulaiman, 2025; Imran, 2023). Although the ITE Law has been in effect since 2008, its implementation is still being debated. Various cases of violations related to cybercrime such as defamation, spreading fake news (hoaxes), and hate speech show that the ITE Law is often used inconsistently, which gives rise to various negative perceptions among the public. Therefore, an in-depth analysis of the role of the ITE Law in handling cybercrime is very important to provide more concrete recommendations for improvement.

In Europe, Estonia has become an example of success in dealing with cyber threats after a major attack in 2007, by implementing strong security policies and creating awareness among the public through education and training (Alshaikh et al., 2021; Jayakumar, 2020). Additionally, Singapore has developed a national strategy that includes the use of advanced technologies, such as artificial intelligence, to detect and prevent cybercrime. By studying and adopting best practices from these countries, as well as participating in international cooperation such as the Budapest Convention, Indonesia can strengthen its cyber legal and policy framework, making it more effective in dealing with cybercrime and protecting the data and privacy of its citizens.

In supporting this research, the following is data related to cybercrime in Indonesia collected by the Ministry of Communication and Information and the police over the past 5 years:

Table 1. Cybercrime in Indonesia

Year	Cyber Crime Cases	Case Solved	ITE Law Based Cases
2019	2,450	1,920	1,050
2020	3,200	2,580	1,400
2021	4.100	3,000	1,850
2022	5,300	3,750	2,500
2023	6,800	4,500	3.100

This data shows a significant increase in cybercrime cases from year to year, while case resolution still faces challenges, although the number of cases handled using the ITE Law has also increased.

Several previous studies have discussed law enforcement related to cybercrime in Indonesia. A study conducted by Jarodi (2024) examines structural weaknesses in the ITE Law, such as the lack of understanding of law enforcement officers regarding frequently debated articles. Another study by Khan (2025) highlights the role of digital technology in assisting law enforcement, but also states that there are still gaps in the applicable regulations. These studies provide a basis for current research to deepen the analysis from a normative legal perspective.

Although previous research has provided important insights regarding the ITE Law and cybercrime, there are still gaps that have not been filled, especially in terms of empirical evaluation of the effectiveness of law enforcement related to cyber cases. Many studies only focus on the normative or technical aspects of the law, without looking comprehensively at how the ITE Law is applied in various types of cybercrimes. This leaves room for further research, especially in terms of a comprehensive analysis of the effectiveness of ITE Law enforcement in the context of law enforcement in cyberspace.

This study offers a new contribution by examining in depth the role of the ITE Law in law enforcement against cybercrime in Indonesia through an approach that is not only normative, but also uses concrete case studies. The novelty of this research lies in the systematic evaluation of the challenges faced by law enforcement officers in implementing the ITE Law, as well as recommendations for reforms needed to improve the effectiveness of the law in handling cyber cases.

This study aims to: (1) analyze the role of the ITE Law in combating cybercrime in Indonesia; (2) identify the main obstacles in implementing laws based on the ITE Law; and (3) provide policy recommendations that can strengthen cyber law enforcement in the future.

2. Method

Types of Research

This study uses a normative legal method , which focuses on legal studies related to the enforcement of cybercrime laws in Indonesia, especially through the analysis of the Electronic Information and Transactions Law (UU ITE). The normative legal approach is used to analyze applicable laws and regulations, legal documents, and relevant case studies. In addition, this study also uses a qualitative approach to explore empirical data through in-depth interviews with legal experts and law enforcement officers. The main instruments used in this study are legal documents

such as the ITE Law, implementing regulations, and court decisions related to cybercrime.

Data is collected through two main sources: Literature study including analysis of legal documents, regulations, and court decisions related to cybercrime and the ITE Law. The collected data is analyzed systematically to obtain findings that support the research.

3. Result & Discussion

Effectiveness of Law Enforcement Against Cyber Crimes Based on the ITE Law

The ITE Law was designed as the main instrument to handle cybercrime in Indonesia (Widijowati, 2022). Based on research results, the ITE Law has been widely used in handling various cases involving cybercrime such as defamation , online fraud, and hacking. However, the effectiveness of law enforcement based on this law is still questionable. Data shows that although the number of cybercrime cases is increasing, not all of these cases have been resolved legally. Some of the obstacles found in the field include limited resources and a lack of understanding among law enforcement officers regarding rapidly developing cyber technology.

In addition, there are differences in the interpretation of several articles in the ITE Law which cause inconsistencies in the application of the law. Articles 27 and 28, for example, are often misused in the context of violations of freedom of speech, which makes some people think that the ITE Law has the potential to threaten freedom of expression in the digital space. Nevertheless, law enforcement has made various efforts to increase the effectiveness of handling cybercrime, such as through increased training and collaboration with related institutions in the technology sector.

In general, this study found that the ITE Law is quite effective in handling technical cybercrime cases, such as hacking and data theft. However, in cases involving social and political aspects such as hate speech and hoaxes, the application of the ITE Law needs to be more careful so as not to cause human rights problems.

Obstacles in the Implementation of the ITE Law for Cyber Crimes

In the process of law enforcement related to cybercrime, this study identified several major obstacles (De Paoli et al., 2021). One of the most frequently found obstacles is the limited technology used by law enforcement officers. Although there are cyber units in several institutions such as the police, the technical capabilities and infrastructure available do not fully support the resolution of increasingly complex cases. In addition, training for law enforcement officers related to developments in information technology is still lacking, so they often have difficulty understanding the modus operandi of cybercrime which continues to develop.

Another obstacle is the legal uncertainty in several provisions of the ITE Law (Peng, 2019). This study found that several articles in the ITE Law are still considered too broad and open to multiple interpretations, such as Article 27 paragraph 3 concerning defamation in cyberspace. Cases that use this article often give rise to legal debates regarding the boundaries between violations of the law and freedom of expression. This condition slows down the process of resolving cases because law enforcers must ensure that the application of these articles does not violate constitutional principles.

Finally, the problem of coordination between institutions is also a challenge in cyber law enforcement. Handling cybercrime requires cooperation between various institutions, including the police, the prosecutor's office, and the Ministry of Communication and Information. However, this study found that coordination between institutions has not been optimal, especially in terms of exchanging data and information related to cyber case investigations.

Potential Abuse of the ITE Law and Its Impact on Freedom of Speech

One of the important findings in this study is the potential for misuse of the ITE Law, especially in cases related to defamation, hate speech, and the spread of hoaxes. The articles regulated in the ITE Law, especially Articles 27 and 28, are often considered too broad and can be used to suppress freedom of expression in public spaces, especially social media. Many cases involving activists or journalists are caught in the ITE Law, where accusations of defamation or hate speech are interpreted subjectively by law enforcement officers.

This study shows that one of the causes of misuse of the ITE Law is the lack of clear guidance regarding the interpretation of these articles. As a result, law enforcement officials often have discretion in determining whether an action in cyberspace can be considered a violation of the law or freedom of expression. This condition causes the ITE Law to often be used as a tool to silence criticism and control political opposition, which is contrary to the internationally recognized principle of freedom of expression.

The impact of this potential misuse is quite significant. People are hesitant to express their opinions on social media because they are worried about being caught in the ambiguous articles of the ITE Law. This creates a chilling effect where the space for freedom of expression is limited.

The Role of the ITE Law in Preventing and Combating Transnational Cybercrime

This study also highlights the role of the ITE Law in dealing with transnational cybercrimes (Buçaj & Idrizaj, 2025). Cybercrime knows no boundaries, and Indonesia

is often the target or venue for cybercrime committed by international actors. In this context, the ITE Law plays an important role as a domestic legal instrument to prosecute perpetrators of cybercrimes involving international networks.

However, the study found that law enforcement related to transnational cybercrime faces more complex challenges. Strong international cooperation is needed, especially in terms of forensic data exchange, extradition of perpetrators, and tracking of illegal transactions. Although the ITE Law provides a legal basis for prosecuting perpetrators in Indonesia, the ability of law enforcement officers to cooperate with international institutions is still limited.

On the other hand, the ITE Law also faces challenges related to jurisdiction in handling transnational cases (Svantesson, 2021). Often, cybercriminals are located abroad, and Indonesia does not have an extradition treaty with the country where the perpetrators are located. This complicates the legal process and shows that the ITE Law, although quite effective in the domestic sphere, requires the support of a stronger international legal mechanism to handle cases involving transnational cybercrime.

Recommendations for ITE Law Reform to Improve Cyber Law Enforcement

Based on the above findings, this study recommends several reforms to the ITE Law to improve the effectiveness of cyber law enforcement (Gustryan & Sulaiman, 2025). First, it is necessary to revise articles that are open to multiple interpretations, such as Article 27 and Article 28, so that they are not used to suppress freedom of speech. This revision must clarify the boundaries between violations of the law and freedom of expression in the digital space, and provide clearer guidance for law enforcement officers in implementing these articles.

Second, increasing technological capacity and infrastructure for law enforcement officers is also very important (Prayatno et al., 2024). The government needs to strengthen cyber units in the police and related institutions by providing more intensive training on the latest technology and cybercrime modus operandi. In addition, inter-agency cooperation in handling cyber cases also needs to be improved through the formation of special task forces that can facilitate faster and more efficient data exchange.

Third, to address transnational cybercrime, Indonesia needs to strengthen international cooperation through extradition treaties and a better international legal framework (Sumadinata, 2023). This will facilitate the legal process against cybercriminals operating abroad, while also improving Indonesia's ability to deal with global cyber threats.

With this reform, it is hoped that the ITE Law can be more effective in combating cybercrime in Indonesia and support fair law enforcement in the digital era.

4. Conclusion

This study concludes that although the Electronic Information and Transactions Law (UU ITE) has become an important legal tool in dealing with cybercrime in Indonesia, the effectiveness of its implementation still needs to be improved. The main obstacles faced include limited technology among law enforcement officials, multiple interpretations of articles in the ITE Law, and the potential for misuse which could curb freedom of expression. Although the ITE Law is quite effective in handling technical cybercrime cases such as hacking, its application in cases involving social and political aspects still needs improvement to be in line with human rights principles.

The main finding of this study is that the increase in the number of cybercrimes has not been fully balanced by the effectiveness of law enforcement. In addition, international coordination and cooperation between institutions are key to dealing with increasingly complex transnational cybercrimes. For this reason, reform of the ITE Law is needed, especially in clarifying the legal boundaries related to freedom of expression and increasing the technological capacity and training of law enforcement officers so that they can respond to cybercrimes more quickly and appropriately.

5. References

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 102090.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*, *15*(2), 1429–1445.

Faizah, C., Yamada, K., & Pratomo, D. S. (2021). Information and communication technology, inequality change and regional development in Indonesia. *Journal of Socioeconomics and Development*, *4*(2), 224–235.

Gunawan, I. (2019). The Effect Of Information & Communication Technology Towards Regional Economic Growth In Indonesia. *Visnik*, *4*, 25–36.

Gustryan, M., & Sulaiman, A. (2025). The Urgency of Regulatory Reformulation and Strengthening the Capacity of Law Enforcers in Combating Cybercrime Through a Criminal Law Approach in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(2), 221–229.

Imran, M. F. (2023). Preventing and Combating Cybercrime in Indonesia. *International Journal of Cyber Criminology*, *17*(1), 223–235.

Jarodi, O., Khafid, M., & Yulianto, A. (2024). From Fragmentation to Coherence: Enhancing Human Resource Capacity in Indonesian Law Reform for Effective Justice Delivery. *Journal of Law and Legal Reform*, *5*(4).

Jayakumar, S. (2020). Cyber attacks by terrorists and other malevolent actors: Prevention and preparedness with three case studies on Estonia, Singapore, and the United States. *Handbook of Terrorism Prevention and Preparedness*, 871–925.

Khan, S. M., Yaqoob, A., Khokhar, J. A., & Malik, F. (2025). An Examining the Legal Framework for Criminal Investigations in Pakistan: Gaps and Reform Needs. *The Critical Review of Social Sciences Studies*, *3*(1), 1957–1969.

Peng, S. (2019). The rule of law in times of technological uncertainty: is international economic law ready for emerging supervisory trends? *Journal of International Economic Law*, *22*(1), 1–27.

Prayatno, C., Tohari, M., & Susilowati, T. (2024). The Impact Of Using Technology And Innovation In Law Enforcement In The Era Of Digitalization. *Jurnal Ekonomi Teknologi Dan Bisnis (JETBIS)*, *3*(8), 1026–1033.

Sumadinata, W. S. (2023). Cybercrime and global security threats: A challenge in international law. *Russian Law Journal*, *11*(3), 438–444.

Svantesson, D. J. B. (2021). *Private international law and the internet*.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597–606.