IJLSSM
INTERNATIONAL JOURNAL OF LAW SOCIAL SCIENCES AND MANAGEMENT
E-ISSN: 3048 - 1317
Volume 1, No. 2
April 2024

Efforts to Reform Law Enforcement in Tackling Cybercrime

Wieke Dewi Suryandari
Faculty of Law, Universitas Darul Ulum Islamic Centre Sudirman GUPPI

*Corresponding Author:
wieke@undaris.ac.id

Abstract
Cybercrime in Indonesia has risen significantly, posing threats to personal data security and critical information systems. The Electronic Information and Transactions Law (UU ITE) provides a legal framework for addressing cybercrime by imposing criminal sanctions on offenders. The UU ITE covers various aspects, including personal data protection, online fraud, hacking, and malware dissemination. While UU ITE offers a solid legal foundation, challenges remain ineffective implementation and enforcement. Therefore, it is crucial to continuously update and strengthen regulations and enforcement mechanisms to effectively tackle increasingly complex cyber threats in the digital age.

Keywords: *Cybercrime; UU ITE.*

1. INTRODUCTION

The rapid development of information technology has had a significant and broad impact on various aspects of life, creating effects akin to two sides of the same coin. On one hand, technological advancements offer many benefits, such as increased efficiency, information accessibility, and innovation across various sectors, including education, healthcare, and business. Information technology enables faster and more effective communication, facilitates access to resources, and opens new opportunities in the digital economy. On the other hand, these developments also bring challenges and risks that cannot be ignored. Along with technological progress, the emergence of various threats, such as cybercrime, privacy violations, and dependence on technology, can lead to severe problems. (Djanggih & Qamar, 2018)

Technological advancements, particularly with the advent of the internet, have had a major impact on the rise of cybercrime. These developments have allowed perpetrators to find new methods to exploit vulnerabilities in systems and networks. As technological innovations continue to advance, criminals are becoming increasingly

creative and sophisticated in devising new ways to breach digital defenses, exploiting weaknesses in software and security infrastructure. Threats in the online world often do not involve large organizations but are more commonly dominated by individuals or small groups of hackers acting independently or in small teams. (Pearlman & CUnningham, 2012) Although they may not have the same resources or power as large organizations, the impact of their actions can be extremely damaging. Their activities, which can include data theft, system destruction, or malware distribution, have the potential to cause serious disruptions to public order, including creating chaos in financial systems, public services, or critical infrastructure. These attacks can also threaten national sovereignty and stability by compromising national security, disrupting communication and coordination among government agencies, and eroding public trust in digital systems and institutions reliant on information technology.

The challenges faced by authorities and cybersecurity professionals are increasingly complex. To address these threats, ongoing updates in policies, security technologies, and methods for detecting and responding to cybercrime are necessary. Efforts to protect systems and data from exploitation require interdisciplinary cooperation and adaptation to new techniques used by cybercriminals. The approach to law enforcement in cybercrime emphasizes the importance of collaboration between law enforcement agencies, the private sector, and the public. To effectively prevent cybercrime, there is a need for public awareness and education on cybersecurity. Continuous training is also required for law enforcement to tackle the increasingly complex and evolving threats in the cyber realm. (Farhan, Syaefunaldi, Hidayat, & Hosnah, 2023) Innovation in cybersecurity technology must also be a primary focus. The development and implementation of advanced technological solutions can help detect, prevent, and respond to cyber security attacks more quickly and efficiently. The involvement of the private sector in developing cybersecurity technology can create a strong synergy between government, businesses, and law enforcement agencies, strengthening collective efforts in combating cybercrime.

2. METHOD

The research method employed in this study is normative legal research. This approach emphasizes the analysis of legal norms, principles, and regulations, as well as their practical application. The study utilizes both the legislative approach, which examines the relevant statutes and regulations, and the conceptual approach, which explores the theoretical foundations and interpretations of the law.

3. RESULTS AND DISCUSSION

Indonesia is one of the most populous countries in the world. According to Worldometers, Indonesia ranks fourth globally, with 280,011,278 people. It places it behind the United States, India, and China, which have larger populations. With such a significant population, Indonesia faces major challenges and opportunities in various social, economic, and developmental aspects. The Indonesian Internet Service Providers Association (APJII) reports that by 2024, the number of internet users in Indonesia has reached 221,563,479. It makes Indonesia one of the countries with the largest number of internet users, reflecting a very high level of connectivity among its population. With such a large user base, the Internet has become an integral part of daily life in Indonesia, affecting how people communicate, shop, work, and access information. This high level of connectivity also opens opportunities for digital economic development, technological innovation, and enhanced online services, but it also presents challenges related to cybersecurity and personal data protection.

To address cybercrime effectively, the implementation of cyber laws is necessary. According ro (Nugraha, 2021), Cyber Law is a field of law focused on regulating all aspects related to the use and application of internet and electronic technology. The term "Cyber Law" is derived from "Cyberspace Law," which encompasses regulations governing interactions between individuals or legal entities as they begin operating online or enter virtual space. Cyber Law covers various aspects, including regulations on internet access and usage, personal data protection, and law enforcement against cyber crimes such as hacking, online fraud, and malware distribution. Cyber Law serves to provide a clear legal foundation for addressing issues arising from digital activities, ensuring that

there are rules governing behavior in the virtual world and providing mechanisms to address violations.

As technology and people interact in cyberspace become increasingly complex, Cyber Law must continuously evolve to keep pace with rapid technological changes. (Rahmawati, 2017) It includes updating regulations to address new threats and challenges emerging in the digital ecosystem, ensuring that individual rights, and cybersecurity can be effectively protected. The implementation of Cyber Law is crucial for Indonesia, especially considering the ongoing advancements in technology. Proponents of Cyber Law argue that it is time for Indonesia to adopt cyber regulations, as traditional laws are no longer sufficient to handle the dynamics and complexities of the rapidly evolving virtual world (Marita, 2015). With the implementation of Cyber Law, Indonesia will have a more relevant and effective legal framework to address issues related to digital technology and the internet, as well as to protect individual rights and ensure cybersecurity in the modern era.

Cyber Crime Cases in Indonesia

As time goes by, cybercrime is increasingly occurring in various parts of the world, including Indonesia. (Arifah, 2011) Cybercrime cases in Indonesia encompass various offenses, such as embezzlement from banks using computers, the dissemination of pornography online, hacking activities, carding or credit card number theft for online transactions, and deliberate virus spreading. Additionally, there are cases of cybersquatting, which involves registering, selling, or using domain names to profit from trademarks or other people's names on the internet, as well as the theft of documents from national leaders. All these cases reflect a shift of social issues from the physical realm to the virtual world. This phenomenon indicates that social and legal challenges are now occurring not only in the real world but also in the digital space. With the rise in cybercrime cases, there is an urgent need to strengthen regulations and law enforcement in cyberspace. It requires a more sophisticated and integrated approach to address various types of cybercrime and ensure adequate protection for individuals and institutions from increasingly complex and diverse threats on the internet.

Cybercrime cases have indeed been prevalent in Indonesia. Some of these cases have surfaced due to issues with data security from the public. Here are some major cybercrime cases that have occurred in Indonesia according to Prima Cyber Solusi:

1. Data Leak of BPJS Kesehatan(2021)

   The data leaked in this case includes identification numbers (NIK), names, addresses, phone numbers, dates of birth, genders, marital statuses, and blood types. This data breach caused significant losses for BPJS Kesehatan and the Indonesian public. BPJS Kesehatan had to incur substantial costs to repair the damage caused by this incident. The breach occurred due to a security vulnerability in BPJS Kesehatan's information system, which was exploited by hackers to steal participants' data.
2. Hacking of DPR RI Youtube Channel (2023)

   On September 6, 2023, the YouTube channel of the Indonesian House of Representatives (DPR RI) was hacked by unauthorized parties, resulting in the channel broadcasting online gambling content for several hours. As a consequence of the attack, the DPR RI YouTube channel lost over 2 million subscribers and was temporarily disabled by Google for recovery purposes.
3. E-KTP Data Leak (2018)

   In 2018, Indonesia experienced a data breach involving electronic ID cards that exposed the personal information of 191 million residents. The leaked data included identification numbers (NIK), names, addresses, dates of birth, genders, religions, marital statuses, blood types, and educational histories. The breach raised serious concerns about personal data security and highlighted the need for stricter measures to protect sensitive information from cyber threats.
4. Emotet Malware Spread(2020)

   In 2020, the Emotet malware spread to more than 150 countries, including Indonesia. This malware-infected computers and stole user data, including personal, financial, and company information. In Indonesia, over 200,000 computers were infected by Emotet. The financial losses

> from this malware attack are estimated to reach hundreds of billions of rupiah, resulting in a significant financial impact from this cyber infection.

Given the increasing prevalence of cybercrime in Indonesia, which presents significant risks to data security and national defense, there is a pressing need for comprehensive legal frameworks to address these threats. The implementation of effective legislation is anticipated to provide a crucial safeguard, enabling Indonesian society to engage with the internet securely and without the pervasive threat of cyberattacks. (Ersya, 2017)

Law Enforcement Against Cybercrime in Indonesia

In Indonesia, regulations regarding personal data protection are currently governed by Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 on Information and Electronic Transactions. This law, commonly referred to as the ITE Law, encompasses various aspects related to personal data protection as well as regulations on electronic transactions. The content of the ITE Law includes protection of personal rights, principles of electronic commerce, jurisdictional issues, rules on unfair competition, and consumer protection. It also covers intellectual property rights, cybercrime, and relevant international law. Although it addresses several important aspects, the ITE Law does not fully accommodate the comprehensive needs for personal data protection. This highlights the need for more specific and focused regulations to ensure more effective personal data protection in the digital age. (Sari, 2021)

In Law Number 19 of 2016, commonly known as the ITE Law, Article 45 states:

(1) Any person who intentionally and without authorization distributes, transmits, or makes accessible Electronic Information and/or Electronic Documents containing immoral content as referred to in Article 27 paragraph (1) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

(2) Any person who intentionally and without authorization distributes, transmits, or makes accessible Electronic Information and/or Electronic Documents containing

gambling content as referred to in Article 27 paragraph (2) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

(3) Any person who intentionally and without authorization distributes, transmits, or makes accessible Electronic Information and/or Electronic Documents containing insults or defamation as referred to in Article 27 paragraph (3) shall be subject to a maximum imprisonment of 4 (four) years and/or a maximum fine of IDR 750,000,000.00 (seven hundred fifty million rupiahs).

(4) Any person who intentionally and without authorization distributes, transmits, or makes accessible Electronic Information and/or Electronic Documents containing extortion or threats as referred to in Article 27 paragraph (4) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

Additionally, Article 45A of the ITE Law specifies two criminal penalties that may be imposed on cybercriminals for spreading false information or inciting hatred and hostility:

(1) Any person who intentionally and without authorization spreads false and misleading information that causes consumer losses in Electronic Transactions as referred to in Article 28 paragraph (1) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

(2) Any person who intentionally and without authorization spreads information intended to incite hatred or hostility towards individuals or specific community groups based on ethnicity, religion, race, or inter-group relations (SARA) as referred to in Article 28 paragraph (2) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

Furthermore, Article 45B of the ITE Law provides that "Any person who intentionally and without authorization sends Electronic Information and/or Electronic Documents containing threats of violence or intimidation directed personally, as referred

to in Article 29, shall be subject to a maximum imprisonment of 4 (four) years and/or a maximum fine of IDR 750,000,000.00 (seven hundred fifty million rupiahs)."

Indonesia has established legal measures against cybercrime through the Electronic Information and Transactions Law (ITE Law). This legislation explicitly sets criminal sanctions for those involved in various forms of cybercrime, including hacking, online fraud, and malware distribution. The ITE Law provides a specific legal framework for addressing and prosecuting violations occurring in cyberspace. However, despite the comprehensive provisions of the ITE Law concerning criminal penalties for cybercrime, challenges remain in the effective implementation and enforcement of these regulations to combat the continuously evolving threats in the digital age.

4. CONCLUSION

Cybercrime in Indonesia has become a significant issue, with various incidents underscoring the urgent need for enhanced protection in the digital realm. The Electronic Information and Transactions Law has established a clear legal framework for regulating and prosecuting cybercriminals, with criminal sanctions designed to address various forms of violations. While the ITE Law provides an essential legal foundation, challenges persist in its implementation and enforcement, particularly in dealing with increasingly sophisticated criminal techniques. Therefore, ongoing efforts are required to strengthen the law enforcement system and enhance cybersecurity in Indonesia to confront the evolving threats.

References

Arifah, D. A. (2011). kasus cybercrome di Indonesia. *jurnal Bisnis dan Ekonomi, 18*(2).

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal, 13*(1), 10-23.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education, 1*(1), 50-62.

Farhan, M., Syaefunaldi, R., Hidayat, D. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, 1*(6), 8-20.

Marita, L. S. (2015). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia. *Cakrawala-Jurnal Humaniora, 15*(2).

Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia. *Jurnal Ilmiah Hukum Dirgantara, 11*(2).

Pearlman, W., & CUnningham, K. G. (2012). "Non State Actors, Fragmentation, and Conflict Processes". *Journal of Conflict Resolution, 2*(56), 6.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense. *Jurnal Pertahanan dan Bela Negara, 7*(2), 35-50.

Sari, U. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia, 2*(1), 58-77.

[Website] **https://www.primacs.co.id/post/kasus-kasus-cyber-crime-terbesar-yang-pernah-terjadi-di-indonesia**

[Website] **https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang**

[Website] **https://www.worldometers.info/world-population/indonesia-population/**

[Website UU ITE]

https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf