JOURNAL OF HUMANITIES, SOCIAL SCIENCES AND BUSINESS (JHSSB)

THE ENFORCEMENT OF CYBERCRIME LAW WITHIN THE LEGAL SYSTEM OF INDONESIA

Patih Ahmad Rafie[1], M. Martindo Merta[2], Junaidi[3*]
[1-3]Faculty of Law, Universitas Sjakhyakirti
E-mail: [3)] junaidi@unisti.ac.id

Abstract

This study aims to analyze the legal regulations on cyber crime in the Indonesian legal system. The research method used is document analysis, by examining Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and other related literature. The analysis results show that the legal regulations on cyber crime in Indonesia are governed by the ITE Law, which regulates various criminal actions related to the use of information and communication technology. In addition to the ITE Law, there are also other regulations that govern cyber crimes. However, there is a need for the enactment of the Cyberlaw Bill to provide a more specific and comprehensive legal basis for addressing cyber crimes. With specific laws regulating cyber crimes, law enforcement can be carried out more effectively and efficiently, providing legal certainty for cyber crime victims, and offering better legal protection for them. Therefore, this study concludes that legal regulations on cyber crimes need to be continuously developed and updated in accordance with the development of technology and the evolving trends of cyber crimes.

Keywords: *Cyber Crime, Cyberlaw Bill, Criminal Acts*

1. INTRODUCTION

The advancement of information technology in the era of globalization has become a major driver of societal progress. This phenomenon is not only happening in developed countries but also in developing countries. It has spurred the development of information technology worldwide. However, the rapid development of technology also has negative impacts on human life (Anggriani & Arifin, 2019). Globalization is one of the main factors in accelerating this technological development. In addition, the development of human intellectual capacity also plays a role in increasing knowledge. However, not everyone can use this knowledge wisely and correctly, which ultimately harms many people. For example, crimes against computer systems or crimes that utilize computer facilities are increasing (Arief, 2006).

Cyber hacking crimes are one form of cybercrime that emerges as a result of technological advancements. This is regulated in Article 30 paragraphs (1), (2), (3) of Law No. 19 of 2016 amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, hereinafter referred to as the EITE Law. Criminal sanctions for hacking offenses have been stipulated in Article 46 paragraphs (1), (2), (3) of the EITE Law. In addition to providing benefits and positive value, technology also has negative impacts that harm the nation's livelihood (Singgi et al., 2020).

The increasing number of cyber crimes is a problem faced by all countries in the world. This is evidenced by the inclusion of cyber crime as one of the topics discussed at the 8th United Nations Congress on Crime Prevention and Criminal Justice in Havana, Cuba, and the 10th Congress in Vienna, Austria (Singgi et al., 2020). The number of cyber crime cases or crimes in the virtual world that occur in Indonesia is the highest in the world, partly due to the activities of hackers in the country. Cyber crime cases in

Indonesia rank first in the world. Cyber crimes against children have also become a new trend in many countries, including Indonesia. Uncontrolled internet usage makes children vulnerable to various crimes in the virtual world. Sexual crimes, pornography, human trafficking, bullying, and other forms of online crimes pose a growing threat to the future generation of the nation (Singgi et al., 2020).

Currently, the regulations used as the legal basis for cybercrime cases are the Telecommunications Law, electronic transactions, and the Criminal Code. However, sometimes the interpretation of the articles in the Criminal Code in cybercrime cases is not suitable for application. This is due to the differences in the characteristics of cybercrime compared to conventional crimes that are usually regulated in the Criminal Code. Therefore, the importance of enacting the Cyberlaw Bill must be prioritized to face the era of cyberspace with all its consequences, including the recent surge in cybercrime. The Cyberlaw Bill will provide a more specific and comprehensive legal framework for addressing cybercrime. With a specific law governing cybercrime, law enforcement can be carried out more effectively and efficiently.

The Cyberlaw Bill will also provide clarity regarding the definition of cybercrime, the types of crimes that fall under this category, and the sanctions that will be imposed on perpetrators. In addition, this bill will also regulate efforts to prevent and protect against cybercrime attacks. The enactment of the Cyberlaw Bill will also provide legal certainty for cybercrime victims. With a specific law governing cybercrime, victims will receive better legal protection and can obtain justice.

2. RESEARCH METHODS

This research method is a descriptive and analytical method, which collects data from various sources and critically analyzes it to produce accurate and objective conclusions. The descriptive and analytical method can be carried out by collecting data from various sources, such as literature, legal documents, and related research reports. The collected data is then critically analyzed to identify patterns, trends, and relationships between variables related to the research topic. The results of the analysis are then used to generate accurate and objective conclusions regarding the research topic.

3. RESULTS AND DISCUSSION

Cybercrime or traditional crime is a type of crime that includes fraud, identity theft, child pornography, and so on. In cybercrime, the most damaging aspect is the presence of harmful codes that can hack computer networks and disrupt computer operations globally, as well as threats to electronic commerce. The transnational nature of most computer crimes has rendered law enforcement methods respected domestically and internationally ineffective, especially in developed countries. On the other hand, the digital divide provides a safe haven for cybercriminals. To address the threat of cybercrime, reform of international legal cooperation methods and the development of cross-border law enforcement capabilities are required (Broadhurst, 2006).

Cybercrime is a type of crime that occurs in cyberspace and is not limited by jurisdictional boundaries or internet usage by anyone, anywhere in the world. Cybercrime can encompass various criminal activities such as identity theft, online fraud, cyber attacks, dissemination of illegal content, and so on.

In the context of transnational crime, cybercrime is a serious concern for the Indonesian state. Due to its transnational nature, cybercrime can involve perpetrators from various countries and cross jurisdictional boundaries. Therefore, proving cybercrime is crucial for Indonesia in efforts to enforce the law and determine the jurisdiction of these transnational crimes in accordance with the applicable procedural law in Indonesia.

The existence of cybercrime has become a pressing issue that needs to be addressed due to its continuous growth alongside the advancement of information and communication technology. Cybercrime can cause harm to individuals, companies, and even nations on a large scale. Therefore, it is crucial to understand and effectively combat cybercrime.

Cybercrime is a criminal act that arises from the misuse of information technology, especially with the emergence of the internet which forms the cyber space. In the Draft Convention on Cybercrime (Draft No. 19 and No.25 Rev.5) in 2000 and the Draft Explanatory Memorandum to the Draft Convention on Cybercrime in 2001, prepared by the European Committee on Crime Problems, various categories of cybercrimes are identified, such as: (Broadhurst, 2006)

a. Joy Computing refers to the unauthorized use of someone else's computer, including the theft of computer operating time.
b. Hacking is the act of accessing a terminal without proper authorization or permission.
c. Trojan Horse involves manipulating data or programs by altering the data or instructions in a program for personal or other purposes.
d. Data Leakage refers to the unauthorized disclosure of data, especially data that should be kept confidential.
e. Data Diddling is the unauthorized alteration of valid or legitimate data.
f. Frustrate Data Communication or computer misuse.
g. Software Piracy is the unauthorized copying or distribution of copyrighted software.
h. Cyber Espionage is the act of spying through the internet by infiltrating the targeted computer network system.
i. Infringements of Privacy involve crimes against highly confidential personal information.
j. Data Forgery is the falsification of data on important documents through the internet.
k. Unauthorized Access to Computer System and Service is the act of entering or infiltrating a computer network system without permission.
l. Cyber Sabotage and Extortion involve the destruction or sabotage of data, programs, or computer network systems connected to the internet.
m. Offense against Intellectual Property refers to crimes against intellectual property rights on the internet.
n. Illegal Contents involve the insertion of data or information on the internet that violates the law or disrupts public order (Raharjo, 2002).

From the various forms of cybercrime mentioned above, it is evident that cybercrime fundamentally involves attacks on the content, computer systems, and communication systems belonging to others or society in cyberspace.

In Indonesia, cybercrime is regulated under positive criminal law. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) serves as the main legal basis governing cybercrime. The ITE Law regulates various criminal actions related to the use of information and communication technology, such as the dissemination of pornography, online fraud, and cyber attacks. In addition to the ITE Law, there are also other regulations that govern cybercrime, such as Law Number 19 of 2016 concerning Amendments.

Criminal acts involving technology are known as cybercrimes, such as cyberbullying. The criminal responsibility for perpetrators of cybercrimes is regulated by Law Number 19 of 2016 in Indonesia (Anggriani & Arifin, 2019; Makhali, 2023). In Indonesian criminal law, those who commit cybercrimes can be held accountable for offenses stipulated in the Criminal Code (Galed, 2022). The purpose of this regulation is to maintain security and human interests in the preservation of information technology. In handling the majority of criminal acts, the state needs to set aside legal regulations to punish offenders and maintain social order.

The regulation of laws regarding cyber crime in Indonesia is governed by Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). The ITE Law serves as the main legal foundation used in law enforcement against various forms of cyber crime, such as online gambling, defamation, and other information technology crimes. However, several studies have shown that there are still obstacles in the implementation of these laws, as well as in the careful and proportional use of prohibited acts by law enforcement agencies (Akub, 2018; Djarawula et al., 2023; Hermansyah et al., 2023). Therefore, despite the existence of a legal framework to combat cyber crime, efforts are still needed to improve the implementation and enforcement of laws related to cyber crime in Indonesia.

Criminal acts against electronic systems are acts committed by utilizing electronic systems to cause harm or disruption to the electronic system. These criminal acts are regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Criminal acts against electronic systems include:

a) Hacking (Article 30 of the ITE Law)

Hacking is the act of unauthorized access to another person's electronic system with the intention of obtaining information, altering data, or damaging the electronic system. Offenders of hacking may face a maximum prison sentence of 8 years and/or a fine of up to IDR 5 billion.

b) Electronic System Access Interference (Article 31 of the ITE Law)

Electronic system access interference is the intentional and unauthorized act of obstructing, limiting, or disabling access to an electronic system. Perpetrators of electronic system access interference may be subject to a maximum prison sentence of 6 years and/or a fine of up to IDR 3 billion.

c) Electronic System Destruction (Article 32 of the ITE Law)

Electronic system destruction is the intentional and unauthorized act of destroying, altering, moving, adding, reducing, or hiding stored information in an electronic system. Those who engage in electronic system destruction may face a maximum prison sentence of 10 years and/or a fine of up to IDR 6 billion.

d) Creation, use, and/or distribution of hardware and/or software to damage electronic systems (Article 33 of the ITE Law)

The creation, use, and/or distribution of hardware and/or software to damage electronic systems is an intentional act to create, use, or distribute hardware and/or software that can be used to damage electronic systems. Perpetrators of the creation, use, and/or distribution of hardware and/or software to damage electronic systems may be subject to a maximum prison sentence of 12 years and/or a fine of up to IDR 7.5 billion.

The regulation of cyber crime is based on the current legal sources both in the Criminal Code and laws outside the Criminal Code. The UN Congress has called on member states to tackle cybercrime with penal means. Legal protection for victims of cybercrime is a necessity that must be immediately made by the State, considering that cybercrime cases have caused unrest for the community, especially for those who use computer and information facilities. Therefore, the importance of passing the Cyberlaw Bill must be prioritized to face the era of cyberspace with all its consequences, including the rise of cyber crime lately.

The regulation of cybercrime in the Criminal Code can be seen in the following articles:

a. Article 362 of the Criminal Code on theft: Regulates the crime of theft, which in the context of cybercrime can include the theft of electronic data or important information through illegal access to computer systems.
b. Article 369 of the Criminal Code on Extortion and Threats: Regulates the criminal offense of extortion and threatening, which in the context of cybercrime may include threats or extortion made through electronic media.
c. Article 372 of the Criminal Code on Embezzlement: Regulates the criminal offense of embezzlement, which in the context of cybercrime can include embezzlement of electronic data or digital assets.
d. Article 386 of the Criminal Code on Fraudulent Acts: Regulates the criminal offense of fraudulent acts, which in the context of cybercrime can include fraud, manipulation, or fraud committed through information technology.
e. Article 506 of the Criminal Code on Violation of Public Order: Regulates the criminal offense of violation of public order, which in the context of cybercrime may include acts that disturb public order through electronic media.
f. Article 382 bis of the Criminal Code and Article 383 of the Criminal Code: These articles are not explained in the context of cybercrime in the text provided.

The Information and Electronic Transactions (ITE) Law in force has defined various categories of cybercrimes, providing a comprehensive legal framework to address various forms of violations in the digital space. Article 27 deals with illegal content such as pornography, gambling, defamation, extortion, and threats. This reflects concern for morality and the protection of individual reputations in the digital environment. Article 28 further addresses the issues of fake news and hate speech, emphasizing the importance of information integrity and social harmony in the digital era.

Article 29 highlights threats to individuals through violence or intimidation, demonstrating the seriousness of the law towards personal online security. Meanwhile, Articles 30 and 31 specifically address illegal access and interception of information, targeting those who illegally access or intercept data without authorization, highlighting the importance of data security and privacy.

Articles 32 and 33 focus on data breaches, espionage, and system disruptions. This illustrates the importance of maintaining the integrity of data and electronic systems from unauthorized manipulation. Articles 34 and 35 deal with device misuse and data interference, targeting those who create or use tools to facilitate cybercrimes and those who intentionally manipulate data to create the impression of authenticity.

Overall, the ITE Law demonstrates a serious effort in addressing the challenges posed by technological advancements, targeting a wide range of behaviors from the dissemination of illegal content to unauthorized access, interception, and data manipulation. This law reflects an awareness of the need to protect the rights and freedoms of individuals in the virtual world, while ensuring the security and stability of the digital space.

4. CONCLUSION

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) serves as the main legal basis governing cybercrime in Indonesia. The ITE Law regulates various criminal actions related to the use of information and communication technology. There are negative impacts of the development of information technology on human life, such as the increase in cybercrime, dependence on information technology, the spread of hoaxes, the loss of privacy and personal data security, as well as negative impacts on physical and mental health.

The enactment of the Cyberlaw Bill is expected to provide a more specific and comprehensive legal foundation in addressing cybercrime, as well as clarity regarding the definition of cybercrime, the types of crimes included in this category, and the sanctions to be imposed on perpetrators. The implementation and enforcement of cybercrime laws in Indonesia still face challenges, including the careful and proportional use of prohibited acts by law enforcement agencies. Therefore, efforts are needed to improve the implementation and enforcement of cybercrime laws in Indonesia.

REFERENCES

Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *Al-Ishlah: Jurnal Ilmiah Hukum*, *21*(2), 85–93.

Anggriani, A., & Arifin, R. (2019). Tindak Pidana Kesusilaan Dalam Kaitannya Dengan Kejahatan Mayantara Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik di Indonesia. *Jurnal Hukum PRIORIS*, *7*(1), 16–30.

Arief, B. N. (2006). *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408–433.

Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, *2*(10), 3799–3806.

Galed, D. O. (2022). Tindak Pidana Apostasia (Murtad) Studi Kanonik. *Studia*

Philosophica et Theologica, *22*(1), 138–157.
Hermansyah, H., Mustamam, M., & Putra, P. S. (2023). Peran Cyber Crime Ditreskrimsus Kepolisian Daerah Sumatera Utara Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Judi Online (Studi di Kepolisian Daerah Sumatera Utara). *Jurnal Meta Hukum*, *2*(3), 115–127.
Makhali, I. (2023). Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara. *Transparansi Hukum*, *6*(1).
Raharjo, A. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.
Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339.

Copyrights