SRIWIJAYA CRIMEN AND LEGAL STUDIES
FACULTY OF LAW UNIVERSITAS SRIWIJAYA
Jalan Srijaya Negara, Palembang, 30139, Indonesia
Email: scls@fh.unsri.ac.id
http://journal.fh.unsri.ac.id/index.php/SCLS/index
E-ISSN: 2987-7350 P-ISSN: 2986-6367

JURISDICTIONAL CYBERCRIME CRIMINALIZATION POLICY IN THE USE OF INFORMATION TECHNOLOGY

Serlika Aprita[1], Wangmayum Hanif[2]

[1] *Faculty of Law, Muhammadiyah Palembang University, Indonesia, E-mail: 5312lika@gmail.com*
[2] *FIFA Games Company, India, E-mail: hanifwangmayum786@gmail.com*

Article

Keywords: **Information Technology, Cyber Crime, Criminalization**

DOI: 10.28946/scls.v2i2.3651

Abstract

The victim and the offender are frequently in separate nations, a crime known as cybercrime transcends all borders and periods. Cybercrime can be committed using the computer itself as the method of committing the crime and the computer network system as the target. Laws governing information technology must take into account its rapid growth. Information and communication technology laws must anticipate and lessen these negative consequences. For information, media, and communication technology to progress as much as possible, legal products about cyberspace, or mayantara, must offer security and legal certainty. In response to the increasing number of cybercrimes, the government adopted a policy on April 21, 2008, with the adoption of Law No. 11 of 2008 regarding Information and Electronic Transactions (UU ITE). The ITE Law is Indonesia's first legislation focusing on online regulation. Based on the research findings, it can be concluded that Indonesian law enforcement has been unable to combat cybercrime to the best of its abilities. Indonesian law enforcement is facing difficulties due to the growth in cybercrime. The reasons for this are a lack of public legal awareness in efforts to combat information technology crimes, limited facilities and infrastructure, and the fact that there are still relatively few law enforcement officials who are familiar with the ins and outs of information technology (internet).

A. INTRODUCTION

Globalization and information technology advancements, which occur in practically every aspect of life, define modern world civilization. Globalization and technological advancements happen in both developed and poor nations. Information technology is currently a major factor in international trade and economics, particularly the facilitation of information transmission. Countries around the world benefit greatly from information technology.[1] The availability of information has at least two benefits. First, demand for technological items is driven by information technology. Secondly, it facilitates additional business dealings. Second, these advantages confirm that there has been a change in society's transaction patterns and social patterns from conventional to electronic methods, which are more effective and efficient.[2]

Due to the advancement of digital information technology, people now live in a revolutionary business environment (the "digital revolution era") that makes communication and information collecting simpler, less costly, more practical, and more dynamic. Many daily activities in society have shifted from traditional to electronic systems, including purchasing daily necessities. People are more likely to order via the Internet using the services of available online sites, including booking plane tickets, train tickets, and other transportation. Electronically. Technological progress has brought many changes and ease in life. The development of information technology has brought about a dark, vulnerable side to the extent that it is concerning, with worries about the emergence of criminal acts in the field of information technology related to "cybercrime" or cybercrime. However, technological improvements have not only had favorable social effects. Didik et al. categorize technology-related crimes into several groups, including unauthorized access to computer systems and services, unlawful content, data forgery, cyber espionage, cyber sabotage and extortion, offense against intellectual property, and privacy violations. Since Mayantara crime is one of the extraordinary crimes (extraordinary crime), serious crimes (serious crimes), and transnational crimes (crimes between nations) that constantly endanger the lives of citizens, the nation, and the sovereign state, it is imperative that all parties give the issue of Mayantara crime careful consideration in light of future information technology development. This illegal act or crime is the worst part of modern life in the information society because of the speed at which technology is developing, the surge in computer crime, pornography, digital terrorism, junk information "war," information bias, hackers, crackers, and other related issues.[3]

Computers and the internet have drawbacks that can negatively affect human life and society despite their benefits and convenience. The evolution of information technology shifts thought patterns from manual to computerized/digital in terms of time, values, object shapes, territorial borders, work patterns, and logic of thought. These days, information technology has two sides: while it can be utilized to perpetrate crimes effectively, it can also be used to advance civilization, human welfare, and progress. Since it is evident that people are now heavily reliant on internet technology, information is seen as "power," defined as strength and authority that truly controls the fate of humans. The more reliant society is on information technology these days, the greater the vulnerabilities it confronts. Therefore, to prevent the adverse effects of internet technology, we as a community of users must be able to govern ourselves and logic.[4]

[1] Budi Surhayanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celah Hukumnya* (Depok: Raja Grafindo Persada, 2013).

[2] Agus Raharjo, *Cybercrime: Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: Citra, 2002).

[3] Mansur dan Elisataris Ghultom Didik M. Arif, *Cyber Law: Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2010).

[4] Sultan M. Aswandi R, Muchin PRN, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps)," *Legislatif* 20, no. 1 (2020): 167–90.

As social media continues to evolve, there are several factors that consumers need to consider when utilizing it. The first thing to pay attention to is the precautionary principle. This needs to be instilled in social media users always to be careful when using social media or "Think before click". When regulating the use of technology and electronic transactions, the ITE Law ensures that the following principles are maintained: benefit, prudence, good faith, legal clarity, and technological freedom. This is reflected in paragraphs (1) and (2) of article 40 of Law No. 19 of 2016 regulating ITE. The process of collecting, compiling, storing, processing, releasing, analyzing, and/or disseminating information so that it can be utilized in a wide range of human endeavors is known as information technology. The existence of technology in various fields of life helps humans implement electronic systems to complete activities. The rule that more clearly outlines the rights of data owners is Law No. 11 of 2008 concerning Electronic Information and Transactions, as revised by Law No. 19 of 2016 concerning the ITE Law. Article 26 of the ITE Law states that the law provides the framework for data protection—individual data obtained via an electronic system.[5]

The author of this individual assignment focuses on researching cybercrime, defined as crimes committed unlawfully into computer network systems without authorization or the owner's knowledge. Cybercrime is defined as authorized access to computer systems and services. Hackers and other criminals typically do this to steal or sabotage sensitive data. As internet technology advances, this crime is becoming more and more common, and multiple hacker lawsuits are being filed against website hackers. Now, hackers are behaving more violently. The breadth of cybercrimes in Indonesia is growing annually. In 2016, hackers made 32% more attempts at hacking.

Massive tangible and immaterial losses have resulted from the various new criminal activities due to technological advancements. Laws controlling the use of technology have to be established because of the numerous crimes created due to its rapid growth. Cyberlaw, also called telematics law, is a new law or cyber law, a word used globally to refer to legal issues about the use—of technology for information and communication. Cybercrime laws are necessary for enforcing criminal law, especially crimes that arise from this technology. Cybercrime has pushed Indonesia to the top of the global crime rankings, surpassing Ukraine, which was previously in the top spot, demonstrating this rule's significance. The information is from Verisign Research, a California-based organization that offers internet intelligence services. The question of what the policy is about cybercrime in the use of information technology, particularly in hacking cases, emerges from the foregoing brief overview.

B. RESEARCH METHOD

The author employs a normative research approach with a descriptive model to examine several facets of cybercrime-related legislation. Documents from printed and electronic journals, articles, papers, and other sources were gathered as part of the data collection process. After comparison, the data was chosen to be presented in this report. As a result, it is hoped that the author's study findings may at least offer some insight for anyone interested in Indonesian cyber law. Both a statutory and a conceptual approach are employed. Both primary and secondary legal materials are engaged in the author's analysis of the law about cyber law. Legal materials derived from legislative rules about this writing are primary legal materials. Legal materials from books, journals, or scientific articles relevant to this inquiry are known as secondary legal materials.[6]

[5] Dewi PET. Mantili R, "Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia," *Jurnal Aktual Justice* 2, no. 5 (2020): 132–45.

[6] Soerjono dan Sri Marmudji Soekanto, *Penelitian Hukum Normatif* (Jakarta: Raja Grafindo Persada, 2000).

C. ANALYSIS AND DISCUSSION

1. Hacking as Cybercrime

New terms for the offenders have emerged due to developments in cybercrime. "Hackers" are persons who enjoy playing online games and browsing other people's websites; "hacking" is the term used to describe their activities; a "cracker" is a hacker who sneaks onto other people's websites and does harm. The development of computer hacking abroad is growing very rapidly, as is the case in Indonesia. Of course, this is very different from ordinary crimes such as robbery. For example, a bank robbery in New York will have no influence or connection with a bank robbery in Jakarta. However, hacking that occurs and is carried out in New York can influence Indonesia and have consequences because hackers in New York can directly attack websites in Indonesia. Therefore, it is necessary to know the development of computer hacking outside Indonesia.

Hackers are those who, for financial gain or out of a sense of challenge, investigate, examine, alter, and breach computers and computer networks. According to Revelation LoaAsh, "hacking is the act of penetrating a computer system to gain knowledge about the system and how it works, and hacking is illegal because we demand free access to all data, and we get it." The skill of breaking into a computer system to discover more about it and how it functions is known as hacking. People are annoyed by this, and we are shunned by society. We have to conceal that we are hackers or phreakers to avoid going to jail.[7]

Since hacking is unlawful, hackers always conceal their identities because it is tantamount to insulting or deceiving people by secretly accessing and reading someone else's data without authorization. But if we dig deeper, this isn't the case because the hacker community has specific cultures and rules, like different goals and motivations. According to American hacker expert Emmanuel Goldstein, "one of the common misconceptions is that anyone considered a hacker is doing something illegal." When someone is essentially looking for knowledge, it's a depressing reflection on the state of our society. Furthermore, it is presumed that the truth is up to something evil. It couldn't be further from the reality. In their idealistic naivete, hackers disclose that they have uncovered government cover-ups and corporate secrets without considering financial gain.[8]

2. Criminal Law Policy in Indonesia

Theoretically, a law is a set of rules encompassing societal and individual attitudes and behaviors, and the state can punish those who break them. Despite being a virtual environment, laws are still required to control people's behavior and attitudes in at least two ways. First, individuals in the virtual world are real people, and society has interests and values that need to be safeguarded on both an individual and group level. Second, public transactions impact the actual world, both economically and non-economically, despite occurring in the virtual realm. Understanding the definition of the policy itself is crucial before delving into the topic of criminal policy and criminal law policy. Mayer and Ernest Greenwood created a policy to determine the best and most efficient means of achieving their jointly established objectives.[9] In this instance, policy is seen in the concepts of criminal policy and criminal law policy, which Sudarto explains in two ways: (2) State policy through authorized authorities to construct the desired rules that are expected to be utilized to convey

[7] Maskun, *Kejahatan Siber CyberCrime : Suatu Pengantar* (Jakarta: Kencana, 2013).

[8] *Ibid.*

[9] Indah dan Nawawi Barda Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara* (Semarang: Universitas Diponegoro, 2000).

what is contained in society and to achieve what is aspired to; (1) initiatives to build good regulations at any given moment following the circumstances and situations;[10]

Political and criminal policy, according to Sudarto, is a logical attempt by society to combat crime. Protecting society to attain social welfare is the primary objective of criminal politics. According to Barda Nawawi, deciding (1) what behaviors should be considered criminal activities and (2) what penalties should be applied to violators are two issues that are fundamental to criminal policy. "Criminal law policy is not just a legislative, technical work that can be carried out in a normative juridical manner," said Barda Nawawi Arief. A factual, social, historical, or comparative legal approach is also necessary for criminal law policy.[11] It even calls for a thorough approach from several different social science fields. Criminal law policy is essentially how criminal law can be properly drafted and guide legislators (legislative policy), judges (judicial policy), and executives (executive policy). Therefore, criminal law policies need to be applied with awareness and purpose. When deciding to implement criminal law as a way to combat crime, it is important to consider all the elements that can help the law function in practice. In criminal law, punishment can be understood as both the process of establishing and enforcing punishments. According to Sudarto, punishment is punishment in the strictest sense. Sudarto went on to clarify that punishment is a legal judgment (*berechten*) for incidents involving both civil and criminal law. Punishment is just an action taken against a criminal. Punishment is not to punish someone for committing a crime, but to deter future criminal activity and make others fearful of committing the same offense.[12]

According to Petrus Reinhard Golosecan use the following passages from the Indonesia Criminal Code (KUHP). to analyze the Mayan world:

a. According to Petrus Reinhard Golose, the following passages from KUHP can be used to analyze the Mayan world.
b. According to Pasal 378 KUHP, a transaction occurs when a person acts as a seller and offers goods by advertising a website to elicit interest in the product in question and then receiving payment from the seller.
c. Article 335 KUHP describes ancaman and pemerasan via email.
d. Article 331 of the Criminal Code contains a case of defamation that encourages bold media. Pelaku typically sends a series of emails with vital information through Milis or sends an email to the victim about a story that isn't very detailed.
e. It is possible to use Pasal 303 KUHP to highlight the online gambling activities carried out by Indonesian authorities.
f. Pasal 282 KUHP refers to pornographic situations or situations that are easy to access and that are boldly displayed.
g. If someone daringly displays a private image or video, they can be identified by Pasal 282 and 311 KUHP.
h. Because the buyer wants to buy something and uses the credit card number that has been canceled, Pasal 378 and 262 KUHP can be used in the case of a credit card revocation.
i. In the case of the company's website, Articlel 406 KUHP can be accessed because the user changes the website's content after accessing the victim website.[13]

Because it differs from ordinary crime in terms of perpetrator, victim, method of operation, and crime scene, TI/Cybercrime necessitates special attention and investigation

[10] Sudarto, *Hukum Pidana Dan Perkembangan Masyarakat* (Bandung: Sinar Baru, 1983).

[11] Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*.

[12] Budi Suhariyatno, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celah Hukumnya* (Depok: Raja Grafindo Persada, 2013).

[13]Petrus Reinhard Golose, "Perkembangan Cybercrime Dan Upaya Penanggulangannya Di Indonesia Oleh Polri," *Buliten Hukum Perbankan Dan Kebanksentralan* 2, no. 4 (2006): 38–39.

outside of KUHP. To prevent repression, it is necessary to pay attention to the rules outside of KUHP that are based on the *ultimum remedium* (also known as the ultima ratio) and that prevent the general public from living in a way that is overly critical of the law.[14]

3. Use of the ITE Law for Hacking Crimes

Hacking is a criminal act that falls under the category of illicit access, as was mentioned in the previous debate. Cybercrimes compromising the availability, confidentiality, and integrity of electronic systems, data, or documents may be categorized as a subset of illegal access crimes. Acts of unlawful access are, in theory, comparable to crimes covered by Article 167 of the Criminal Code, which include forcing one's way into a house, yard, or closed space and remaining in a home or closed space after being asked to leave by those who are authorized to do so. 18 Article 30 paragraph (1) of the ITE Law defines the general offense of illegal access, which is the primary distinction between that act and the entry into another person's yard or home, governed by Article 167 of the Criminal Code. The first paragraph of this article regulates Illegal Access as the main offense, stating that any action, including a computer or electronic system, without the consent of the rightful party is prohibited. The legal protection that will be provided through this article is the protection of a person's property and privacy. Article 30, paragraph (2) concerning illegal access to information. This article is an offense that qualifies from the previous paragraph. In this paragraph, the element of the purpose of access is added, namely, to obtain electronic information or documents. This setting is essential, considering electronic systems are personal, confidential, or economic. Article 30, paragraph (2) discusses illegal access by breaking through, exceeding, or breaching security. If we look at the elements of punishment in Article 30, it is appropriate to prosecute criminal acts of hacking. Because of action hacking is included in the Illegal Access category. Articles 35 and 36 of the ITE Law also state the punishment for illegal access cases.[15]

After Ukraine, Indonesia has the second highest cybercrime rate worldwide.[16] Cybercrime is a new type of crime that involves computer technology in its implementation. Hacking, phishing, pornography, internet fraud, and credit card number theft are all considered forms of cybercrime. Online fraud and the dissemination of offensive content are the most frequent cybercrimes in Indonesia. From January to December 2022, the National Police will report 8,831 virtual criminal instances worldwide.[17] among Indonesia's cybercrimes, software piracy, cyberterrorism, fraud (including cyber-based fraud and illegal electronic transactions), hacking, data manipulation, web phishing, and cyberattacks against digital security systems.[18] Fraud currently constitutes the most common type of crime in Indonesia. The e-commerce boom has contributed to the increase in fraud cases.

Indonesia's Law on Information and Electronic Transactions (UU ITE) makes cyber law enforcement more challenging. The primary issue is terminology, which affects how the ITE Law is interpreted and discussed. Even though the ITE Law has been used to deal with cyber crimes such as spreading harmful content and hoaxes, its implementation is controversial because it is considered too broad and potentially restrictive of freedom of expression. Due to insufficient technology and human resources, Indonesia faces challenges implementing cyber law. To combat the threat of cybercrime, better cybersecurity awareness, education, and more efficient law enforcement are required. These dangers include the potential to compromise national security, corrupt data, steal confidential information, and interfere with services. This study suggests that the government should seriously consider improving public education

[14] Muladi, "Kebijakan Kriminal Terhadap Cybercrime," *Majalah Media Hukum* 3, no. 1 (2003).

[15] Widodo, *Sistem Pemidanaan Dalam Cyber Crime* (Yogyakarta: Laksbang Mediatama, 2009).

[16] Kominfo, "Indonesia Peringkat Ke-2 Dunia Kasus Kejahatan Siber," 2015.

[17] Pusiknas Polri, "Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat" (Pusiknas Polri, 2022).

[18] A.P.U Saragih, Y.M., & Siahaan, "Cyber Crime Prevention Strategy in Indonesia," *J.Humanit.Soc.Sci, SSRG Int.* 6, no. 3 (2016): 22–26.

regarding cybercrime prevention and bolster law enforcement against cybercriminals in Indonesia.

D. CONCLUSION

Furthermore, the development of society is influenced by technological advances. Technology positively impacts society by facilitating social interaction, accelerating the flow of information, and influencing political and economic systems. However, there are also disadvantages, as the development of this technology contributes to the emergence of various forms of cybercrime, commonly known as cybercrime. Legal policy regimes around the world face significant difficulty in regulating society in the virtual world to safeguard and secure society against a variety of crimes and to combat crimes that are becoming more and more prevalent. Since crimes are not only a local issue in one country but can also affect other countries, legal jurisdiction has started to change from the local law that applied in traditional life to the global law that applies in this technological age and is not constrained by certain regional boundaries. This phenomenon led to the creation of cyber law, which governs the social interactions within online communities. Indonesia created Law No. 11 of 2008 on Electronic Information and Transactions. This law was created because it was believed that the issues that arise in the virtual world could not be adequately addressed by the laws in place.

REFERENCES

Arief, Indah dan Nawawi Barda. *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*. Semarang: Universitas Diponegoro, 2000.

Aswandi R, Muchin PRN, Sultan M. "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps)." *Legislatif* 20, no. 1 (2020): 167–90.

Didik M. Arif, Mansur dan Elisataris Ghultom. *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2010.

Golose, Petrus Reinhard. "Perkembangan Cybercrime Dan Upaya Penanggulangannya Di Indonesia Oleh Polri." *Buliten Hukum Perbankan Dan Kebanksentralan* 2, no. 4 (2006): 38–39.

Kominfo. "Indonesia Peringkat Ke-2 Dunia Kasus Kejahatan Siber," 2015.

Mantili R, Dewi PET. "Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia." *Jurnal Aktual Justice* 2, no. 5 (2020): 132–45.

Maskun. *Kejahatan Siber CyberCrime : Suatu Pengantar*. Jakarta: Kencana, 2013.

Muladi. "Kebijakan Kriminal Terhadap Cybercrime." *Majalah Media Hukum* 3, no. 1 (2003).

Polri, Pusiknas. "Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat." Pusiknas Polri, 2022.

Raharjo, Agus. *Cybercrime: Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra, 2002.

Saragih, Y.M., & Siahaan, A.P.U. "Cyber Crime Prevention Strategy in Indonesia." *J.Humanit.Soc.Sci, SSRG Int.* 6, no. 3 (2016): 22–26.

Soekanto, Soerjono dan Sri Marmudji. *Penelitian Hukum Normatif*. Jakarta: Raja Grafindo Persada, 2000.

Sudarto. *Hukum Pidana Dan Perkembangan Masyarakat*. Bandung: Sinar Baru, 1983.

Suhariyatno, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celah Hukumnya*. Depok: Raja Grafindo Persada, 2013.

Surhayanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celah Hukumnya*. Depok: Raja Grafindo Persada, 2013.

Widodo. *Sistem Pemidanaan Dalam Cyber Crime*. Yogyakarta: Laksbang Mediatama, 2009.