Verdict: Journal of Law Science
3(2) (2024): 86-93
Online version available in:
https://www.ojs.wahanapublikasi.com/index.php/vjlaws
DOI: https://doi.org/10.59011/vjlaws.3.2.2024.86-93

Punishment for Cybercrime: A Major Challenge in Modern Legal Systems

Ridho Duha[1]*

Faculty of Law, Nias Raya University, South Nias 22865, Indonesia
Email: ridho2duha@gmail.com

ARTICLE INFO

Received:
15 Feb 2024

Accepted:
02 Apr 2024

Published:
02 Aug 2024

Keywords:

Cybercrime,
Punishment,
Global security,
Electronic transactions

ABSTRACT

Cybercrime represents a major challenge to modern legal systems due to its transnational nature and its continual evolution alongside digital technological advancements. The increasing intensity and complexity of cybercrime drives the need for an adaptive legal system that is able to provide effective legal protection. This study aims to analyze the application of penalties for cybercrime in Indonesia, assess its effectiveness, and compare it with legal practices at the international level. The approach used is normative juridical with qualitative analysis techniques on primary and secondary legal materials, including case studies of cybercrime in Indonesia, Singapore, and Estonia. The results of the study show that although Indonesia has a legal basis in the form of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and the Criminal Code, its implementation has not been optimal due to the weak technical capacity of the apparatus, minimal coordination across institutions, and the absence of a strong international cooperation mechanism. Comparative studies indicate that countries such as Singapore and Estonia have built a more proactive legal framework through a multi-level and integrative approach. The conclusion of this study emphasizes the importance of regulatory revision, increasing digital forensic capacity, and ongoing international cooperation. Practical implications of this study include the need to strengthen the law enforcement system, develop a national digital literacy policy, and greater involvement of the private sector in combating cybercrime.

Doi: https://doi.org/10.59011/vjlaws.3.2.2024.86-93

1. Introduction

The development of information and communication technology has brought about major changes in various aspects of life, including the way humans interact, work, and

* Corresponding Author
E-mail address: ridho2duha@gmail.com

conduct transactions.[2] However, this progress has also created a new gap for the development of cybercrime[3], which is now a global legal issue.[4] Cybercrime includes various criminal acts such as theft of personal data, online fraud, digital identity forgery, to attacks on critical systems such as banking infrastructure and national security[5]. This phenomenon shows that the characteristics of cybercrime are very different from conventional crimes, both in terms of modus operandi[6], perpetrators, and areas of operation that cross jurisdictional boundaries.[7]

The International Telecommunication Union (ITU), in its Global Cybersecurity Index 2020, reported a more than 200% increase in cybercrime over the past decade, correlating with growing connectivity and reliance on digital systems.[8] Research by Wall emphasizes that the complexity of cybercrime requires the legal system to respond with a more adaptive and transnational approach.[9] This is important considering that cybercriminals can come from different jurisdictions than the victims, thus creating challenges in terms of evidence, extradition, and cross-border law enforcement.

At the international level, cases such as the "WannaCry" ransomware attack that paralyzed the UK's healthcare system in 2017 are clear evidence that cyber attacks can have a broad and cross-country impact.[10] Meanwhile, in Indonesia, the attack on the National Data Center (PDN) server in 2023 showed that vulnerability to cybercrime not only affects individuals or the private sector, but also threatens strategic public institutions. Research conducted by Anwary noted that the unpreparedness of legal instruments and weak enforcement are the two main causes of the high level of cybercrime in developing countries, including Indonesia.[11]

Several previous studies have examined the technical and social aspects of cybercrime[12], but there are still few legal studies that specifically discuss the effectiveness of the application of punishment to cybercrime perpetrators in Indonesia,[13] especially

[2] Fatima Dakalbab et al., "Artificial Intelligence & Crime Prediction: A Systematic Literature Review," *Social Sciences and Humanities Open* 6, no. 1 (2022): 100342, https://doi.org/10.1016/j.ssaho.2022.100342.
[3] Thomas J Holt, "Understanding the State of Criminological Scholarship on Cybercrimes," *Computers in Human Behavior* 139 (2023): 107493, https://doi.org/10.1016/j.chb.2022.107493.
[4] Emmanuel Nnaemeka Vitus, "Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users— A Case of African States," *TIJER - International Research Journal* 10, no. 9 (2023): 975–89.
[5] M Yar and K. F Steinmetz, *Cybercrime and Society*, 4th ed. (New York: SAGE Publications Ltd, 2023).
[6] Bhavna Arora, "Exploring and Analyzing Internet Crimes and Their Behaviours," *Perspectives in Science* 8 (2016): 540–42, https://doi.org/10.1016/j.pisc.2016.06.014.
[7] Maria Grazia Porcedda, "Sentencing Data-Driven Cybercrime. How Data Crime with Cascading Effects Is Tackled by UK Courts," *Computer Law and Security Review* 48 (2023): 105793, https://doi.org/10.1016/j.clsr.2023.105793.
[8] ITU, *Global Cybersecurity Index 2020* (Geneva: International Telecommunication Union (ITU), 2021).
[9] David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (New York: John Wiley & Sons, Inc, 2007).
[10] NAO, *Investigation: WannaCry Cyber Attack and the NHS* (London, England: National Audit Office, 2017).
[11] Ichsan Anwary, "Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach," *International Journal of Cyber Criminology* 17, no. 1 (2023): 12–22, https://doi.org/10.5281/zenodo.4766601.
[12] So-Hyun Lee, Ilwoong Kang, and Hee-Woong Kim, "Understanding Cybercrime from a Criminal's Perspective: Why and How Suspects Commit Cybercrimes?," *Technology in Society* 75 (2023): 102361, https://doi.org/10.1016/j.techsoc.2023.102361.
[13] Anwary, "Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach."

with a normative legal approach and comparative analysis with other countries. In fact, the effectiveness of the legal system is very important in forming a sustainable protection and prevention system. Thus, this study aims to fill this gap by analyzing the legal basis, form of punishment, and the effectiveness of its application to cybercrime in Indonesia. This study also compares the policies and regulations implemented by Indonesia with the best practices of other countries such as Singapore and Estonia, which are known to have more advanced cyber law systems.[14]

2. Method and Legal Materials

This study uses a normative legal approach, which focuses on the analysis of applicable laws and regulations and relevant legal literature[15]. This approach was chosen to explore in depth the legal basis for the application of penalties for cybercrime, both nationally and internationally. In addition, this approach also allows the author to conduct a critical assessment of the effectiveness of the implementation of criminal sanctions in practice. This research method is descriptive-analytical, which aims to provide a comprehensive picture of the forms, types, and patterns of the application of penalties for cybercrime in Indonesia, and to compare them with the legal systems of several countries that are considered successful in dealing with cybercrime such as Estonia, Singapore, and the United States. The type of data used is secondary data, consisting of: Primary legal materials, in the form of:

- Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) as amended by Law Number 19 of 2016.
- Criminal Code (KUHP).
- International legal instruments such as the Convention on Cybercrime (Budapest Convention).
- Relevant laws and regulations in comparative countries (Singapore: Cybersecurity Act 2018; Estonia: Cybersecurity Strategy 2019).

Then, secondary legal materials, in the form of:

- Scopus-indexed scientific journals that discuss cybercrime and criminal law.
- Criminal law and cybersecurity textbooks.
- Court decisions related to cybercrime cases in Indonesia and abroad.
- Official reports from related institutions such as BSSN (National Cyber and Crypto Agency), Interpol, and Europol

In addition, tertiary legal materials, such as legal dictionaries and legal encyclopedias, are also used to clarify the definitions and important concepts used in this study. The data collection technique is carried out through library research, with an in-depth review of legal documents, scientific articles, and relevant case studies. The data that has been collected is then analyzed qualitatively using legal interpretation techniques and a comparative approach to the legal systems of other countries. The analysis is carried out by examining the extent to which national regulations provide legal protection and

[14] UNODC, *Cybercrime: A Global Perspective. United Nations Office on Drugs and Crime*, 2021.
[15] Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. XIV (Jakarta: Prenada Media Group, 2019).

impose sanctions on cybercriminals, as well as assessing the effectiveness and implementation of these regulations. The comparative approach is used to identify the weaknesses and strengths of the Indonesian legal system in dealing with cybercrime compared to countries that already have an established cyber law enforcement system.

3. Results and Discussion

3.1 The legal basis, form of punishment, and the effectiveness of its application to cybercrime in Indonesia

This section systematically describes the findings of normative and comparative legal analysis of the application of punishment for cybercrime in Indonesia and comparative countries. The discussion is divided into several main focuses to examine the effectiveness of regulations, implementation of punishment, and lessons learned from international practice.

1. Effectiveness of Criminal Regulation in Combating Cybercrime in Indonesia

Indonesia has a primary legal umbrella in the form of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) which was amended by Law No. 19 of 2016. In practice, this regulation has been used to prosecute perpetrators of various cybercrimes, such as theft of personal data, spreading hoaxes, and online defamation. However, law enforcement against cybercrime in Indonesia still faces various obstacles, ranging from limited resources of law enforcement officers to the multiple interpretations of articles in the ITE Law. As expressed by Suseno[16], the unclear subjective elements in several articles cause disparities in decisions and difficulties in providing evidence. Many cases of cybercrime such as hacking of public agency systems, misuse of personal data, and cyberbullying are difficult to solve due to the lack of digital forensic expertise among law enforcement and minimal coordination across agencies[17].

2. Case Study: Cyber Violations and the Implementation of Penalties in Indonesia

One prominent case is the Bjorka case, which claims to have hacked into various government systems and leaked the personal data of state officials. Although it caused a public uproar, law enforcement did not reach the main perpetrator who was suspected of being outside Indonesia's jurisdiction. In other cases, such as the spread of personal information (doxxing) and the spread of hoax content on social media, the perpetrator can be charged with Article 27 paragraph (3) of the ITE Law. However, the effectiveness of legal prosecution depends on how quickly digital evidence can be collected and how strong the evidence is in the eyes of the law. As discussed by Syahranuddin and

[16] Sigid Suseno et al., "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences* 11, no. 1 (2025), https://doi.org/10.1080/23311886.2024.2439543.
[17] Yee Ching Tok and Sudipta Chattopadhyay, "Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling," *Forensic Science International: Digital Investigation* 45 (2023): 301540, https://doi.org/10.1016/j.fsidi.2023.301540.

Ramadani[18], the lack of standardization in digital evidence is a major obstacle in the cybercrime justice process in Indonesia.

3. Comparison with Legal Systems of Other Countries

In comparison, Estonia is known as a country with the most advanced cybersecurity system and cyber law in the world. They have implemented a national Cybersecurity Strategy since the early 2000s and have close cooperation with NATO and the European Union. Its criminal law provides strict restrictions on online crime and fast and accurate enforcement procedures. In Singapore, the Cybersecurity Act 2018 not only regulates the protection of critical infrastructure, but also requires reporting of cyber incidents and gives the Cyber Security Agency (CSA) extensive powers to conduct investigations[19]. The justice system in Singapore provides strict penalties and serves as a strong warning to perpetrators. The results of a study by Khan[20] shows that Singapore's proactive approach to preventing cybercrime is more effective in reducing the frequency of attacks than the reactive approach in Indonesia.

4. Weaknesses and Challenges in Implementing Cyber Law Enforcement in Indonesia

Despite having a legal basis, Indonesia still faces a number of structural challenges, such as limited capacity of human resources of law enforcement officers in digital forensics, weak coordination between institutions such as the Ministry of Communication and Information, the Police, and BSSN. Then, the absence of a protection mechanism for victims of cybercrime, especially those of a psychological and social nature. According to Ariyaningsih et al., cyber law enforcement in Indonesia tends to be reactive and is not yet based on a comprehensive digital risk management system[21]. As a result, perpetrators are often faster than law enforcement, both in terms of technology and tactics

4. Conclusion

This study shows that the implementation of punishment for cybercrime in Indonesia has a sufficient legal basis through the ITE Law and the Criminal Code, but in practice it still experiences various obstacles, both normative, technical, and institutional. The results of the study show that although there have been a number of cases that have been successfully processed, such as the spread of hoaxes and defamation on social media, law enforcement against more complex forms of cybercrime such as hacking, data theft, and transnational crimes has not been fully effective. Comparison with the legal systems of other countries, such as Estonia and Singapore, shows that a more comprehensive,

[18] S Syahranuddin and Suci Ramadani, "Criminal Law Policies in Overcoming Cyber Crime in Indonesia," *Proceedings of The International Conference on Multi-Disciplines Approaches for The Sustainable Development*, 2023, 738–42.
[19] Iqbal Ramadhan, "ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia," 2022, https://doi.org/10.4108/eai.31-3-2022.2320684.
[20] Azfer A. Khan, "Reconceptualizing Policing for Cybercrime: Perspectives from Singapore," *Laws* 13, no. 4 (2024): 1–19, https://doi.org/10.3390/laws13040044.
[21] Sindy Ariyaningsih et al., "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia," *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11, https://doi.org/10.56457/jjih.v1i1.38.

integrative, and prevention-based approach and strengthening of technical institutions can provide more effective results in dealing with cyber threats. Singapore, with its Cybersecurity Act 2018, has been able to create a legal framework that not only punishes but also encourages strengthening national preparedness against cyber attacks[22]. Meanwhile, Estonia has integrated its security system comprehensively through regional and international cooperation.

This study provides several important implications, namely 1) The need for revision and harmonization of cyber regulations in Indonesia. In this case, it is necessary to update the ITE Law, including clarification of criminal elements, increased protection for victims, and stricter regulations on transnational crimes and the responsibilities of digital platform providers; 2) Strengthening the Capacity of Law Enforcement Officers and Digital Forensic Infrastructure. The state must allocate sufficient resources to increase the capacity of human resources in the field of digital forensics and information technology in law enforcement agencies, such as the police and prosecutors; 3) International Cooperation to Combat Global Cybercrime Given the cross-jurisdictional nature of cybercrime, Indonesia needs to strengthen international legal cooperation, such as through Interpol, ASEAN, and UNODC, to track perpetrators and enforce cross-country laws; 4) Encourage Private Sector and Community Participation Combating cybercrime is not enough just through a repressive approach, but also requires active participation from digital service providers, educational institutions, and the wider community in the form of digital literacy and incident reporting.

Conflict of Interest Statement

There is no conflict of interest in the creation of this article.

Author's contribution Statement

The author made a major contribution to the conception and design of the research. The author takes responsibility for data analysis, interpretation and discussion of results with the assistance of ChatGPT, OpenAI. The author reads and approves this final text.

References

Anwary, Ichsan. "Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach." *International Journal of Cyber Criminology* 17, no. 1 (2023): 12–22. https://doi.org/10.5281/zenodo.4766601.

Ariyaningsih, Sindy, A. Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11. https://doi.org/10.56457/jjih.v1i1.38.

Arora, Bhavna. "Exploring and Analyzing Internet Crimes and Their Behaviours." *Perspectives in Science* 8 (2016): 540–42. https://doi.org/10.1016/j.pisc.2016.06.014.

Dakalbab, Fatima, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas,

[22] Republic of Singapore, "Cybersecurity Act," 2018.

and Qassim Nasir. "Artificial Intelligence & Crime Prediction: A Systematic Literature Review." *Social Sciences and Humanities Open* 6, no. 1 (2022): 100342. https://doi.org/10.1016/j.ssaho.2022.100342.

Holt, Thomas J. "Understanding the State of Criminological Scholarship on Cybercrimes." *Computers in Human Behavior* 139 (2023): 107493. https://doi.org/10.1016/j.chb.2022.107493.

ITU. *Global Cybersecurity Index 2020*. Geneva: International Telecommunication Union (ITU), 2021.

Khan, Azfer A. "Reconceptualizing Policing for Cybercrime: Perspectives from Singapore." *Laws* 13, no. 4 (2024): 1–19. https://doi.org/10.3390/laws13040044.

Lee, So-Hyun, Ilwoong Kang, and Hee-Woong Kim. "Understanding Cybercrime from a Criminal's Perspective: Why and How Suspects Commit Cybercrimes?" *Technology in Society* 75 (2023): 102361. https://doi.org/10.1016/j.techsoc.2023.102361.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Cet. XIV. Jakarta: Prenada Media Group, 2019.

NAO. *Investigation: WannaCry Cyber Attack and the NHS*. London, England: National Audit Office, 2017.

Porcedda, Maria Grazia. "Sentencing Data-Driven Cybercrime. How Data Crime with Cascading Effects Is Tackled by UK Courts." *Computer Law and Security Review* 48 (2023): 105793. https://doi.org/10.1016/j.clsr.2023.105793.

Ramadhan, Iqbal. "ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia," 2022. https://doi.org/10.4108/eai.31-3-2022.2320684.

Republic of Singapore. "Cybersecurity Act," 2018.

Suseno, Sigid, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita, and Bernadette Aurellia Nathania Tiarma. "Cybercrime in the New Criminal Code in Indonesia." *Cogent Social Sciences* 11, no. 1 (2025). https://doi.org/10.1080/23311886.2024.2439543.

Syahranuddin, S, and Suci Ramadani. "Criminal Law Policies in Overcoming Cyber Crime in Indonesia." *Proceedings of The International Conference on Multi-Disciplines Approaches for The Sustainable Development*, 2023, 738–42.

Tok, Yee Ching, and Sudipta Chattopadhyay. "Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling." *Forensic Science International: Digital Investigation* 45 (2023): 301540. https://doi.org/10.1016/j.fsidi.2023.301540.

UNODC. *Cybercrime: A Global Perspective. United Nations Office on Drugs and Crime*, 2021.

Vitus, Emmanuel Nnaemeka. "Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users— A Case of African States." *TIJER - International Research Journal* 10, no. 9 (2023): 975–89.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. New York: John Wiley & Sons, Inc, 2007.

Yar, M, and K. F Steinmetz. *Cybercrime and Society*. 4th ed. New York: SAGE Publications Ltd, 2023.