JURNAL META-YURIDIS
No. P-ISSN : 2614-2031 / NO. E-ISSN : 2621-6450
Fakultas Hukum Universitas PGRI Semarang
Homepage: http://journal.upgris.ac.id/index.php/meta-yuridis/

Article History: Received: 2024-08-10 Accepted: 2024-09-29
Published: 2024-09-30

ANALYSIS OF CYBERSECURITY REGULATIONS IN ADDRESSING HACKING ACTIVITIES IN THE DIGITAL ERA BASED ON JUSTICE VALUE

Naavi'u Emal Maaliki
Faculty of Law, Sultan Agung Islamic University Semarang, Indonesia.
emal.maaliki@unissula.ac.id

Abstract

The rapid advancement of information technology in the digital era has led to a significant increase in cybercrime in Indonesia. Among the most prominent forms of cybercrime is hacking, which poses a serious challenge to law enforcement due to limitations in human resources and the country's cybersecurity infrastructure. While the ITE Law and the Personal Data Protection Law provide a foundational legal framework to combat cybercrime, these regulations require continuous updates to keep pace with the rapidly evolving nature of digital threats.

Furthermore, the vulnerability of the small business sector, stemming from a lack of technological sophistication and public awareness, further exacerbates the risks. To address these challenges effectively, a comprehensive approach is required, involving collaboration between government institutions, law enforcement agencies, the private sector, and the community. This article utilizes the normative legal method, focusing on the analysis of existing written regulations and secondary data from literature. The study concludes that an integrated and coordinated effort is necessary to enhance Indonesia's cyber resilience, including the strengthening of policies, improvement of cybersecurity infrastructure, and raising public awareness. Only through such measures can Indonesia effectively mitigate the growing threats in the digital era.

Keywords: *Legal Analysis, Cyber Security, Hacking, Justice Value.*

INTRODUCTION

The rapid advancement of information technology has significantly developed in Indonesia and other countries. Information technology has driven economic growth and the acquisition of global information. However, cybercrime has increased alongside these technological advancements. Technology has transformed civilization into a global community, with these changes largely attributed to information technology. The Internet, born from information technology, media, and computers, has fundamentally altered human life, affecting various aspects such as the economy, communication, and education. Despite the benefits brought about by these developments, the rise of cybercrime poses a serious challenge. Hacking activities have become more prevalent as society becomes increasingly reliant on digital technology, necessitating effective regulations to protect individual and organizational data privacy (Wahid, A. & Labib, M., 2020).

The presence of the Internet has introduced a new paradigm in human life, shifting from a purely physical (real) existence to a new virtual reality. Despite the law's aim to create a more peaceful existence, crimes continue to occur both directly in our surroundings and through social media (Hasan, Z., 2020). Nowadays, technology is not always used for positive purposes by the public; in fact, its continuous development has enabled criminals to commit cybercrimes. Crimes related to computers or

telecommunications are known as cybercrimes (Akub, M.S., 2018).

Cybercrime constitutes illegal actions conducted in cyberspace. Several examples of cybercrime in Indonesia include online fraud, check forgery, credit card fraud, identity theft, and hacking. The number of cybercrime cases in Indonesia has grown alongside technological developments in the digital era. In addition to weak security systems, these crimes often occur due to negligence on the part of the users themselves. One prominent form of cybercrime that has emerged is hacking. A notable example of a hacking incident involved one of the banks in Indonesia, where one of the bank's servers was down for several days, rendering customers unable to access their mobile banking applications. A Russian hacker group, Lockbit, claimed responsibility for the attack, stating that they had stolen 1.5 terabytes of data, including customers' and employees' personal data. They demanded a ransom in exchange for returning the data, threatening to sell it on the dark web if their demands were not met. This cybercrime case became one of the largest ransomware attacks in Indonesia (6 Kasus Cybercrime Di Indonesia Yang Menyerang Server, 2023).

In addition to this case, numerous other cybercrimes target personal data from companies across Indonesia. One viral case involved the hacker Bjorka, who stole personal data from Bank Indonesia (BI), the Ministry of Communication and Informatics (Kominfo), patients from several hospitals in Indonesia, Pertamina job applicants, PLN customers, Jasa Marga customers, and more. Victims of Bjorka's data theft were primarily domestic companies with weak server security. Another type of cybercrime is website hijacking through web defacement. Web defacement involves altering the appearance of a website, including the homepage, index files, or other pages connected to the site's URL. Hackers exploit security vulnerabilities in their victims' systems to carry out these attacks. Government-run websites in Indonesia have also fallen victim to these attacks (Popa, D.F.T., 2023).

Given the increasing prevalence of cybercrime, particularly hacking cases, greater caution is required, as well as strengthening laws that regulate these matters. As a result, the government has implemented laws governing the use of information technology, such as Law No. 19 of 2016, which amended Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), to provide legal frameworks for the use of information technology (Zainudin Hasan, 2024). According to Law No. 19 of 2016 on Electronic Information and Transactions, the right to access information through the use of Information and Communication Technology (ICT) is intended to promote public welfare, enrich the intellectual life of the nation, and provide security, justice, and legal certainty for users and Electronic System Providers (Reyhan, R.P., 2023).

From the above examples, it is evident that the misuse of technological advancements can have severe negative consequences. Therefore, preventive and enforcement efforts are needed to address hacking crimes, particularly through legal regulations that can act as a deterrent to perpetrators and potential offenders. Based on this discussion, this research is titled Analysis of Cybersecurity Regulations in Addressing Hacking Activities in the Digital Era.

MAIN PROBLEM

Based on the aforementioned background, several issues will be examined. The issues discussed in this research are as follows:

1. How are cybersecurity regulations in addressing hacking activities in the digital era?
2. What are the weaknesses in cybersecurity regulations in addressing hacking activities in the digital era?

METHOD OF RESEARCH

This research employs a normative legal method, which focuses on the study of written regulations, thus relying heavily on secondary data from library sources. The research is conducted using a descriptive-analytical approach, which describes the condition of the research object, including the applicable laws and their current implementation, based on recent facts and data. In this research, the data collected includes both primary and secondary data. The main activity carried out is library research. The collected data will be analyzed using qualitative analysis methods, as the primary data are not numerical and cannot be measured quantitatively. This method is used to provide a comprehensive overview of the issues based on a normative juridical approach (I Made, P. D., 2016).

RESEARCH RESULT AND DISCUSSION

1. Cybersecurity regulations addressing hacking activities in the digital era

The issue of cybercrime cannot be separated from the problem of computer network security or internet-based information security in the digital era, especially when considering information as a commodity. Information as a commodity requires reliable services to ensure that what is presented does not disappoint its consumers (Ramadhan, M. F., 2021). To achieve such reliability, information must be continuously updated to prevent it from becoming outdated. Cybercrime has emerged alongside the rapid development of information technology. Every illegal activity involving the use of computers or the internet, referred to as cybercrime, is related to digital devices. Although cyber activities are virtual, their impact is very real, even though the evidence is often electronic in nature. As such, the perpetrators should be qualified as individuals who commit real legal actions. In his book, Barda Nawawi Arief writes that cybercrime is a new form or dimension of contemporary crime that has gained widespread attention in the international community. Vodymyr Golubev refers to it as "the new form of anti-social behavior." Several other notable terms for this new type of crime in various writings include cybercrime (cyber space/virtual space offense), a new dimension of high-tech crime, a new dimension of transnational crime, and a new dimension of white-collar crime (Barda Nawawi Arief, 2018). Cybercrime regulations in various countries use different terms based on their legal objectives and scope (Suseno, S., 2012). According to its typology, cybercrime is derived from the words "cyber" and "crime." Crime refers to illegal acts, criminal offenses, or similar events, while cyber refers to virtual space or cyberspace (Raharjo, A., 2002).

From the above definitions, cybercrime can be formulated as unlawful acts committed using the internet, based on the sophistication of computer and telecommunications technology, either for gain or not, that harm others. Based on the modus

operandi or type of activity, cybercrime can be classified into several types, one of which is hacking. A hacker is someone who uses their abilities for criminal purposes. Hacking can involve hijacking accounts, websites, spreading malware, or disabling a target. Denial of Service (DoS) attacks cause a target to crash, preventing them from providing the services they are supposed to. Another form of hacking-related crime is hijacking. Plagiarism, or hijacking, is the theft of someone else's work, with software piracy being the most common. Illegal content refers to the posting of false, unethical, or illegal information online. Examples include posting false news or defamatory content that can harm someone's dignity or reputation, pornography, state secrets, and agitation or propaganda against the government (Hasan, Z. & Fadia, N. K., 2023).

Another form of cybercrime is the intentional spread of viruses. Email is a common vector for virus dissemination. Users of infected email systems may not be aware of it, and the malware is then spread to other locations via email. Unauthorized access to computer systems and services involves committing crimes by illegally entering a computer network system without the owner's permission or knowledge. Hackers typically attempt to steal or disrupt sensitive data.

From several case examples in Indonesia, one of the key challenges in enforcing laws related to cybercrime is the limited technical understanding among law enforcement officers regarding the complexity of cyberspace. Although several regulations, such as Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and Law No. 27 of 2022 on Personal Data Protection, address cybersecurity, the implementation of these regulations in practice remains limited. Many cybercriminals evade legal consequences due to the lack of electronic evidence, slow handling procedures, and weak oversight. The EIT Law provides the legal framework to prosecute cybercrimes, and several articles related to hacking are as follows:

a. Article 30: Prohibits unauthorized access to other people's electronic systems by any means.
b. Article 31: Prohibits wiretapping or illegally obtaining information from electronic systems.
c. Article 32: Regulates the prohibition of damaging, altering, or manipulating electronic information or documents.
d. Article 33: Prohibits any actions that disrupt other people's electronic systems, such as Distributed Denial of Service (DDoS) attacks.

Sanctions for these violations are regulated in Article 46, which states that offenders can be sentenced to imprisonment for up to 8 years and/or a maximum fine of IDR 2 billion, depending on the type of violation committed.

In the Personal Data Protection Law, hacking or unauthorized access to personal data is explicitly regulated through several articles. Article 65 prohibits accessing personal data unlawfully without the consent of the data owner. This includes hacking or wiretapping of personal data

transmissions carried out without authorization. Furthermore, Article 66 prohibits the unlawful disclosure of personal data, which often follows hacking, where the stolen data is subsequently disseminated.

Moreover, Article 67 establishes criminal sanctions for individuals who illegally access personal data. Anyone who intentionally and unlawfully accesses or obtains personal data that does not belong to them may face imprisonment for up to 6 years or a maximum fine of IDR 6 billion. If the hacking is conducted for the purpose of personal gain or to harm others, the penalty can increase to 7 years in prison or a maximum fine of IDR 7 billion. Additionally, Article 68 also prohibits the unlawful processing of personal data, including hacking aimed at damaging or altering data.

Besides criminal penalties, Article 69 states that companies or organizations that fail to protect personal data, leading to data breaches or hacking, may also face administrative sanctions, including the revocation of business licenses or additional fines. This regulation highlights the seriousness of personal data protection in Indonesia and provides a strong legal framework to take action against hackers.

2. Weaknesses in cybersecurity regulations in addressing hacking activities in the digital era

In its implementation, existing regulations have not been fully responsive to the evolving modus operandi of cybercrime. For example, these regulations are still lacking specificity in regulating certain types of cyberattacks, such as ransomware or attacks on critical infrastructure, which have recently become a global concern. One of the main weaknesses of the implementation of the ITE Law is the absence of a clear legal framework regarding comprehensive digital data protection, especially in the context of companies that often do not prioritize customer data security. The Personal Data Protection Law actually provides a stronger legal basis for protecting individual rights, but this regulation has only been partially implemented, and its enforcement remains very minimal. The procedures for handling electronic evidence have also not been fully adapted to the speed of cyberattacks. Cyberattacks can occur within minutes or hours, while legal processes, including the collection and validation of electronic evidence, take much longer. This creates opportunities for perpetrators to erase their digital footprints before authorities can take action. As a result, many cases of cybercrime remain unresolved or even unreported due to a lack of swift and effective follow-up.

The knowledge and technical skills of law enforcement officials pose a significant challenge in addressing cybercrime cases. Most law enforcement personnel, especially at the regional level or in more remote areas, do not have a deep understanding of information and communication technology. This makes them vulnerable to confusion in understanding electronic evidence or the methods of crimes committed online, such as phishing, ransomware, or Distributed Denial of Service (DDoS) attacks. Law enforcement often relies on external experts to process electronic

evidence, which slows down the investigation process and adds operational costs.

Data from the National Cyber and Crypto Agency (BSSN) indicates a significant increase in the number of hacking incidents in Indonesia, primarily targeting the banking, healthcare, and government sectors. DDoS attacks and phishing are the most common types of attacks, followed by ransomware, which continues to evolve alongside the use of more advanced encryption technology (BSSN, 2022).

Several case studies show that companies affected by cyberattacks experience significant losses, not only financially but also in terms of reputation. For example, a ransomware attack on a technology company in Indonesia in 2022 resulted in operational downtime for several days, leading to losses exceeding 10 billion rupiah (Prasetyo & Sari, 2023). Cases like this emphasize the importance of investing in cybersecurity, both in terms of software and human resource training.

In addition to the lack of technical understanding, the limited digital forensic tools available to law enforcement also hinder efforts to combat cybercrime. Investigating cybercrime requires sophisticated digital forensic equipment capable of identifying, collecting, and analyzing electronic evidence from the hardware and software used by perpetrators. Unfortunately, only a few law enforcement agencies in Indonesia possess this advanced equipment and technology. In many cases, they have to send evidence to more advanced digital forensics centers in Jakarta or other major cities, which consumes time and hampers the investigation process.

Coordination among law enforcement agencies, such as between the police, courts, and the National Cyber and Crypto Agency (BSSN), is often suboptimal. This slows down the handling of hacking cases that require inter-agency cooperation. Poor coordination also complicates the sharing of cyber intelligence data and electronic evidence among agencies, which is essential for resolving cross-jurisdictional cybercrime cases. Given the cross-border nature of cyberattacks, international cooperation is also crucial in tackling cybercrime; however, Indonesia still needs to strengthen its international networks for law enforcement in this regard. The BSSN, tasked with monitoring and coordinating national cybersecurity, also faces challenges related to human resource capacity and technology. While BSSN has made various efforts to raise awareness of cyber threats, the shortage of trained personnel in digital forensics and the development of cybersecurity surveillance technology remains a significant challenge for effective oversight (BSSN, 2022).

Despite these challenges, the Indonesian government has taken several steps to address these barriers. One of the ongoing efforts is providing technical training to law enforcement through cooperation with international organizations and countries that are more advanced in cybersecurity. This training program aims to strengthen law enforcement's capabilities in conducting cyber investigations and efficiently

collecting electronic evidence (Kominfo, 2023). The government is also working to enhance international cooperation in enforcing laws against cybercriminals operating abroad, considering the global nature of this threat.

In addition to law enforcement and regulatory strengthening, education on cybersecurity also plays a key role in reducing the risk of attacks. Public awareness of cyber threats is still relatively low, especially among SMEs and individual internet users. Many of them are unaware of the importance of safeguarding personal information while using online platforms (Rachman & Rachmat, 2022). Cybersecurity education programs need to be promoted, both through formal educational institutions and public campaigns organized by the government and private sector. A study by Setiawan (2023) found that individuals who received basic cybersecurity training tended to be more vigilant against phishing or malware attacks compared to those without such understanding.

Collaboration between the public and private sectors is key to creating a resilient cybersecurity ecosystem. The Indonesian government has begun to forge various strategic partnerships with global technology companies in an effort to enhance national cybersecurity resilience. Additionally, companies in the financial and healthcare sectors, which are often primary targets of cyberattacks, have started investing in advanced security technologies and risk management systems (Sutrisno & Rahman, 2023).

However, to maximize the outcomes of this collaboration, a stronger commitment is required from all parties, especially regarding transparency and the exchange of information related to the cyber threats faced. With good synergy between the public and private sectors, Indonesia is expected to address the ongoing cybersecurity challenges as technology continues to advance.

CONCLUSION

Based on the discussion above, it can be concluded that combating cybercrime in Indonesia faces various challenges. Law enforcement against cybercrime is hindered by the limited technical knowledge among officials, as well as the lack of adequate digital forensic tools. Additionally, existing regulations such as the Republic of Indonesia Law No. 11 of 2008 on Information and Electronic Transactions and the Republic of Indonesia Law No. 27 of 2022 on Personal Data Protection, while providing a legal framework, still require updates to effectively address the various forms of evolving cyberattacks. Cybersecurity infrastructure is also a concern, especially in small and medium-sized enterprises (SMEs) and remote areas. Many SMEs remain unaware of the importance of cybersecurity, making them easy targets for criminals. Furthermore, the shortage of skilled human resources in cybersecurity poses a barrier to effectively managing cyber threats. Community involvement in safeguarding their own digital security through increased digital literacy is also crucial, but this awareness still needs to be continuously improved. In terms of policy, the government needs to keep updating the existing legal frameworks and procedures to be more adaptive to technological advancements such as

artificial intelligence (AI) and the Internet of Things (IoT), which create new challenges in cybersecurity. Cooperation among domestic agencies, as well as collaboration with international entities, is vital in addressing the increasing cross-border cyberattacks. Overall, coordinated efforts from the government, law enforcement, the private sector, and society are required to strengthen Indonesia's cybersecurity resilience in facing threats in this digital era.

REFERENCE

[1] Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. Al-Ishlah: Jurnal Ilmiah Hukum. Vol. 21. No. 2.

[2] Badan Cyber dan Sandi Negara. (2022). *Laporan Tahunan Keamanan Siber 2021*. Jakarta: BSSN.

[3] Barda Nawawi Arief, S. H. (2018). Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan. Kencana Prenada Media Group.

[4] Hasan, Z., Apriano, I. D., Simatupang, Y. S., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. Jurnal Multidisiplin Dehasen (MUDE). Vol. 2. No.3.

[5] Hasan, Z., & Fadia, N. K. (2023). Pertanggung Jawaban Pelaku Tindak Pidana Dengan Sengaja Menyebarkan Informasi Yang Ditunjukan Untuk Menimbulkan Rasa Kebencian Atau Permusuhan Individu Dan Kelompok Masyarakat Tertentu Berdasarkan Sara. UNES LawReview. Vol. 5. No. 3.

[6] Hasan, Z., & Martinouva, R. A. (2020). Penanggulangan Kejahatan Begal Di Tulang Bawang Barat (Dalam Perspektif Kriminologi). Jurnal Hukum Malahayati. Vol. 1. No. 1.

[7] I Made Pasek Diantha, (2016). Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum. Prenada Media Group.

[8] Kementerian Komunikasi dan Informatika. (2023). *Kerjasama Internasional di Bidang Keamanan Siber*. Jakarta: Kominfo.

[9] Rachman, I., & Rachmat, D. (2022). Ancaman siber terhadap UKM di Indonesia: Studi kasus dan strategi pencegahan. *Jurnal Keamanan Informasi dan Teknologi*, 5(2), 89-102.

[10] Raharjo, A. (2002). Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi. Citra Aditya Bakti.

[11] Ramadhan, M. F. (2021). Analisis Hukum Terhadap Penyebaran Berita Bohong/Hoax sebagai Bentuk Cyber Crime di Indonesia (Studi Putusan No. 3478/Pid. Sus/2019/Pn. Mdn). Universitas Medan Area.

[12] Reyhan, R. P., Irfan, M., Alfido, M. T. B., & Zai, M. C. A. (2023). Pengaturan Tindak Pidana Elektronik di Indonesia Beserta Permasalahannya. Innovative: Journal Of Social Science Research. Vol. 3. No. 2.

[13] Sutrisno, A., & Rahman, F. (2023). Penguatan infrastruktur keamanan siber di Indonesia. *Jurnal Teknologi dan Inovasi*, 7(1), 55-70.

[14] Suseno, S. (2012). Yurisdiksi Tindak Pidana Siber. Refika Aditama.

[15] Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[16] Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
[17] Undang-Undang Republik Indonesia No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[18] Wahid, A., & Labib, M. (2010). Kejahatan Mayatantra (Cyber Crime). Bandung: Refika Aditama.
[19] Zainudin Hasan. 2023. *Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online*. Jurnal Multi Disiplin Dehasen. Vol. 2. No. 3.
[20] Zainudin Hasan. 2024. Kejahatan Mayantara. Berupa Tindak Pidana Perjudian Melalui Media Elektronik. Journal Innovative: Journal of Social Science Research. Vol. 4 No. 1.