JIHAD : Jurnal Ilmu Hukum dan Administrasi
Vol. 6 No. 4 Desember 2024
p-ISSN : 2745-9489, e-ISSNl 2746-3842
http://dx.doi.org/10.58258/jihad.v3i1.5614

Legal Analysis of Criminal Responsibility for Hackers From the Perspective of Cyber Law in Indonesia

I Putu Edi Rusmana[1], Tania Novelin[2]
[1]Universitas Pendidikan Nasional
[2]Universitas Udayana

Article Info
Article history:
Accepted: 7 November 2024
Publish: 1 December 2024

Keywords:
Cyber Law;
Cyber Crime;
Law Enforcement.

Abstract
Cybercrime, especially hacking, is a major challenge in the digital era, especially when perpetrators operate across countries. This study analyzes the effectiveness of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) in combating international hacking crimes and evaluating international cooperation in cyber law enforcement. Using a normative legal approach, this study shows that although the ITE Law provides a strong legal basis, its application to perpetrators abroad faces jurisdictional challenges, differences in legal systems, and limitations in international cooperation. Technical obstacles in identifying and prosecuting perpetrators are also significant. To overcome this problem, it is necessary to strengthen international cooperation through extradition agreements and mutual legal assistance (MLA), as well as participation in international conventions such as the Budapest Convention. Increasing the technical capacity of law enforcement officers is also important to strengthen law enforcement against transnational hacking crimes. This study concludes that legal arrangements in Indonesia need to be improved through regulatory reform and more effective international cooperation so that Indonesia can protect national interests in the increasingly complex digital era.

Corresponding Author:
I Putu Edi Rusmana
Universitas Pendidikan Nasional
Email: edirusmana@undiknas.ac.id

1. INTRODUCTION

In the era of increasingly rapid digitalization, cyberspace has become an integral part of modern society. Advances in information and communication technology have brought many benefits, but on the other hand have also given rise to various challenges, one of which is cybercrime, including hacking [1]. Hacking, or hacking, is an act of unauthorized access to a computer system or network for a specific purpose, often to steal data, change information, or even damage the system [2]. This crime poses a serious threat to information security, data integrity, and the privacy of individuals and organizations.

In Indonesia, hacking cases continue to increase along with the increasingly widespread use of digital technology [3]. One hacking case that received widespread attention was the hacking of the General Election Commission (KPU) website in 2019 [4]. Hackers managed to access election results data that should have been confidential, and spread it to the public. This case raises major concerns regarding the integrity of the election system in Indonesia and raises questions about how effective the law in Indonesia is in dealing with cybercrime, especially hacking.

Legally, hacking is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) which has been amended by Law Number 19 of 2016 and underwent a second amendment with Law Number 1 of 2024. Article 30 of the ITE Law expressly prohibits unauthorized access to computer systems, which is the core of hacking. However, even though there are clear legal regulations, law enforcement against hackers or commonly called hackers still faces various challenges. One of them is

the complexity of cybercrime itself, which often involves perpetrators who are in Indonesia or who are not in the jurisdiction of Indonesia, as well as the use of sophisticated technology that makes it difficult to track and arrest hackers.

This study identified several important findings related to law enforcement against hacking crimes in Indonesia. First, there are still legal loopholes in the ITE Law that need to be addressed to provide stronger protection for victims of cybercrime [5]. For example, the definition of "unauthorized access" in the ITE Law is still relatively narrow and often does not include more complex forms of hacking crimes, such as Distributed Denial of Service (DDoS) attacks that do not directly access data but paralyze the system. Second, from the law enforcement side, there are significant challenges in terms of the technical capabilities of law enforcement officers [6]. Cybercrime, especially hacking, requires a deep understanding of information technology that is often not possessed by most law enforcement officers in Indonesia. This results in the investigation and prosecution process being slow and ineffective. Third, there is legal uncertainty regarding criminal liability for hackers who operate across national borders [7]. Although the ITE Law provides a legal basis for prosecuting perpetrators domiciled abroad, in practice, the implementation of this law faces many obstacles, especially related to international cooperation in cyber law enforcement.

In addition to the hacking case of the KPU website, there have been several other hacking cases that have attracted public attention in Indonesia. One of the most prominent is the hacking case of the Telkomsel website in 2017 [8]. Hackers managed to replace the main page of the Telkomsel website with a protest message regarding internet rates that were considered too expensive. This case went viral on social media and created a negative reputation for Telkomsel. Although the hackers were eventually caught and punished, this case shows that large companies in Indonesia are still vulnerable to cyber attacks, and that existing laws are not yet fully effective in preventing this type of crime.

Another case is the hacking of personal data of users of the e-commerce platform Tokopedia in 2020 [9]. In this case, millions of Tokopedia user data, including personal information such as names, email addresses, and passwords, were successfully stolen by hackers and sold on the black market [10]. This case not only harms the individuals whose data was stolen, but also raises major concerns regarding data security on digital platforms that are frequently used by the Indonesian people. Although Tokopedia immediately took steps to improve security, this incident shows significant weaknesses in the data security systems of large companies in Indonesia.

From the various cases that have been mentioned, it can be concluded that hacking crimes are a serious threat that must be addressed with a more effective and comprehensive legal approach. Efforts are needed to update existing regulations, increase the capacity of law enforcement officers, and strengthen international cooperation in handling cybercrime. In addition, it is also important to increase public awareness of the dangers of hacking and the importance of maintaining the security of personal data in this digital era.

This background shows that although Indonesia already has regulations governing cybercrime, the challenges in law enforcement are still very large. Further legal reform is needed to ensure that existing laws are effective in dealing with hacking crimes. With the increasing number of cybercrimes in Indonesia, this study aims to provide a comprehensive legal analysis of criminal liability for hackers and how cyber law in Indonesia can be strengthened to provide better protection for the community. Based on the background that the author wrote, there are two formulations of the problem that the author discusses, the first is how is the legal regulation in dealing with hacking crimes in the digital era? And the second is how is criminal liability for cross-border hackers, and international cooperation in the context of cyber law in Indonesia?

2. RESEARCH METHOD

This study uses a normative legal approach, which focuses on the study of law as a norm or rule that applies in society. This approach was chosen because this study aims to analyze how existing laws in Indonesia, especially the ITE Law, are applied in overcoming cross-border hacking crimes, as well as to evaluate the effectiveness of international cooperation in the context of cyber law enforcement. This study uses secondary data consisting of primary legal materials including Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 19 of 2016 and Law Number 1 of 2024 as amendments to the ITE Law, related government regulations, and international conventions such as the Budapest Convention on Cybercrime which are references in international cooperation. Secondary Legal Materials are legal literature, journals, articles, and previous research results that discuss topics related to cybercrime, cross-border hacking, and international cooperation in cyber law enforcement. This literature will be used to strengthen the analysis of primary legal materials. The last is tertiary legal materials including legal dictionaries, encyclopedias, and indexes used to understand the basic concepts and terminology used in this study. The legal materials that have been collected will be analyzed qualitatively using analytical descriptive methods.

3. RESEARCH RESULTS AND DISCUSSION

3.1. Legal Regulations in Combating Hacking Crimes in the Digital Era

The development of information technology has provided many benefits to society, but has also opened up opportunities for cybercrime, such as hacking [11]. In Indonesia, Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is expected to be a strong legal basis in dealing with this cybercrime. However, the question of the effectiveness of the ITE Law in dealing with the ever-growing crime of hacking is still a relevant issue. This discussion will evaluate the effectiveness of legal regulations through the ITE Law from the past, present, and future in the context of hacking crimes in Indonesia.

Before the enactment of the ITE Law in 2008, Indonesia did not have specific regulations governing cybercrime [12]. Crimes such as hacking are often prosecuted under the Criminal Code (KUHP), which includes articles on theft, destruction, or fraud. However, this approach has significant limitations because the Criminal Code is not designed to address crimes that occur in the digital realm. For example, theft in the Criminal Code refers to physical movable objects, while hacking involves the theft of digital data, which resulted in the effectiveness of law enforcement against hacking crimes before the ITE Law being very low [13]. Many hackers cannot be charged with articles in the Criminal Code because they are less relevant to the nature of the crime committed. In addition, law enforcement officers also face difficulties in interpreting existing laws for cyber cases, which often results in perpetrators escaping the law. This shows that before the ITE Law, the regulations in Indonesia were not effective in combating hacking crimes.

The enactment of the ITE Law in 2008 was a significant step in improving the weaknesses of legal regulations related to cybercrime in Indonesia because the ITE Law provides a clearer legal basis for prosecuting hacking crimes, especially with Article 30 which prohibits unauthorized access to computer systems and networks [14]. This provides a strong basis for law enforcement officers to prosecute hackers with the threat of imprisonment of up to 8 years and/or a fine of up to 800 million rupiah. However, the effectiveness of the ITE Law in combating hacking crimes still faces several challenges [15]. First, although the ITE Law has been clearly regulated,

the definition and scope of hacking crimes in this law are still considered limited [16]. For example, the ITE Law does not explicitly regulate cyber attacks such as Distributed Denial of Service (DDoS) or digital identity theft, which are increasingly common in the modern cyber world. Second, the implementation of the ITE Law in law enforcement is often hampered by the lack of technical capacity of law enforcement officers [17]. Cybercrime requires in-depth technical knowledge and skills, but many law enforcers in Indonesia do not yet have adequate expertise in this field. As a result, the investigation and prosecution process for hacking cases is often slow and ineffective, as seen in the Telkomsel hacking case in 2017 and the Tokopedia data hacking in 2020. Third, the ITE Law faces challenges in cross-border law enforcement [18]. Many hacking cases involve perpetrators operating from abroad, making law enforcement more complicated.

Although the ITE Law allows for action against transnational perpetrators, in practice, this implementation is still limited by constraints on international cooperation and jurisdiction. Facing future challenges, the effectiveness of the ITE Law in combating hacking crimes needs to be continuously improved [6]. One important step is to update and revise the ITE Law to expand the definition and scope of cybercrime, so that it includes various forms of more complex and sophisticated attacks that may emerge as this technology develops, including including DDoS attacks, digital identity theft, and other new threats into the regulation. In addition, to improve the effectiveness of law enforcement, the government needs to invest more in training and technical education for law enforcement officers in the field of information technology. Thus, law enforcement will be more prepared and responsive in dealing with hacking cases, and will be able to prosecute perpetrators more quickly and precisely. International cooperation is also key to increasing the effectiveness of the ITE Law in dealing with cross-border hacking crimes [19]. Indonesia needs to establish closer cooperation with other countries through bilateral or multilateral agreements that allow for the exchange of information, tracking of perpetrators, and more effective legal action because this is important because cybercrime often involves complex and difficult-to-trace international networks.

In the future, Indonesia may need to consider establishing a special agency that focuses on cybersecurity, including the prevention and handling of hacking crimes. This agency can function as a coordination center between various government agencies, law enforcement, and the private sector in dealing with cyber threats. With this agency, the response to hacking crimes can be more organized and coordinated, and can provide better protection for the community. The effectiveness of legal regulations in Indonesia against hacking crimes has increased since the enactment of the ITE Law, but there are still significant challenges that need to be overcome [20]. Expanding the scope of the law, increasing the technical capacity of law enforcement officers, and strengthening international cooperation are the keys to increasing the effectiveness of the ITE Law in the future. With these steps, it is hoped that the ITE Law can be more responsive to the dynamics of cybercrime that continue to develop, and be able to provide better legal protection for society in this digital era.

3.2. Criminal Liability for Cross-Border Hackers and International Cooperation in the Context of Cyber Law in Indonesia

The development of information and communication technology has changed the face of modern crime, with the emergence of cybercrime that is often carried out across national borders [21]. Hacking, as a form of cybercrime, is a major challenge for countries around the world, including Indonesia. When hackers operate from

abroad and target systems or individuals in Indonesia, law enforcement becomes much more complicated. An important question that arises is how criminal liability can be applied to hackers who operate across national borders and to what extent international cooperation can be optimized in the context of cyber law in Indonesia.

Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), which was updated by Law Number 19 of 2016 and underwent a second amendment by Law Number 1 of 2024, is the main legal basis in Indonesia in regulating cybercrime, including hacking. Article 30 of the ITE Law explicitly prohibits unauthorized access to electronic systems, which is the core of hacking. Perpetrators who violate this provision are threatened with imprisonment and/or a fairly heavy fine. However, when hackers are abroad and commit crimes against systems in Indonesia, the application of this law becomes more complex. Indonesian criminal law, which is territorial in principle, faces challenges in prosecuting perpetrators who are in other jurisdictions. In situations like this, international law and cooperation between countries become very important. Indonesia as a sovereign country has limitations in enforcing the law against perpetrators of crimes outside its jurisdiction [22]. Therefore, international cooperation in the form of extradition agreements, Mutual Legal Assistance (MLA), and participation in international conventions related to cybercrime, such as the Budapest Convention, is key to holding transnational hackers criminally accountable.

Although the ITE Law provides a legal basis for prosecuting hackers, its application to perpetrators who operate across national borders faces various challenges [15]. First, not all countries have regulations that are in line with the ITE Law or even recognize hacking as a serious crime. This makes it difficult for Indonesia to extradite or request legal assistance from other countries in prosecuting perpetrators. For example, if a hacker in another country attacks a system in Indonesia, Indonesia needs to rely on international agreements or bilateral cooperation to be able to bring the perpetrator to justice. However, if the country where the perpetrator is located does not have an extradition agreement with Indonesia or does not consider hacking a serious crime, efforts to prosecute the perpetrator become very difficult. Second, jurisdictional issues are often an obstacle in enforcing the law against cross-border hackers. Many countries apply the principle of strict territorial jurisdiction, which means that crimes committed outside the territory of the country may not be prosecuted in the perpetrator's home country. This creates legal obstacles for Indonesia in prosecuting hackers operating from abroad. In addition, technical challenges also arise in terms of collecting evidence and identifying perpetrators. Cybercrime is often carried out through highly complex and encrypted networks, which makes tracking the perpetrators difficult [23]. Even if the perpetrators are successfully identified, the process of collecting sufficient evidence to prosecute the perpetrators in court is often a challenge in itself.

To overcome these challenges, international cooperation is the main solution. Indonesia has participated in various international forums and collaborated with other countries in order to combat cybercrime. One of the most important forms of cooperation is the extradition agreement, which allows Indonesia to request the surrender of cybercriminals who are abroad to be tried in Indonesia [24]. In addition, Indonesia is also active in Mutual Legal Assistance (MLA) cooperation, which allows the exchange of information and evidence between countries for law enforcement purposes. This cooperation is very important in cases of cybercrime, where evidence is often spread across countries and requires international coordination to be collected and used in court [25]. Indonesia's participation in international conventions such as

the Budapest Convention on Cybercrime is also an important step in strengthening international cooperation. This convention provides a legal framework for countries to work together to combat cybercrime, including hacking. Although Indonesia is not yet a full member of the Budapest Convention, active participation in the discussion and implementation of the principles of this convention can improve Indonesia's ability to enforce the law against cross-country hackers.

Given the developments and challenges, the prospects for implementing criminal liability for cross-border hackers in Indonesia will depend heavily on increasing international cooperation [26]. In this context, Indonesia needs to continue to strengthen bilateral and multilateral relations with other countries, especially those with jurisdictions where hackers may operate. In addition, it is important for Indonesia to continue to develop the capacity of law enforcement in dealing with cybercrime. This includes improving technical capabilities in identifying, tracking, and collecting evidence against hackers operating across borders. Training and continuing education in the field of information technology and digital forensics for law enforcement officers are important steps in facing this challenge. In the future, Indonesia also needs to consider strengthening national regulations that can support international cooperation more effectively, including more detailed regulations on extradition and MLA in the context of cybercrime, as well as more active participation in relevant international conventions. With these steps, it is hoped that criminal liability for cross-border hackers can be implemented more effectively, so that Indonesia can better protect its national interests in this increasingly connected digital era.

Criminal liability for cross-border hackers in Indonesia still faces various challenges, both in terms of law, jurisdiction, and technical aspects. However, with the strengthening of international cooperation and the enhancement of law enforcement capacity, these challenges can be overcome. The future of law enforcement against transnational cybercrime in Indonesia will depend greatly on the country's ability to establish closer cooperation with other countries and adopt regulations that are more adaptive to the dynamics of cybercrime in the digital era.

4. CONCLUSION

This study analyzes the effectiveness of legal regulations in Indonesia, especially Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), in combating cross-border hacking crimes. Based on the analysis conducted, it can be concluded that although the ITE Law has provided sufficient legal basis to prosecute hackers, the application of this law to perpetrators operating from abroad still faces a number of challenges. The main challenges include limited jurisdiction, where Indonesia's territorial criminal law has difficulty reaching perpetrators in other jurisdictions. In addition, there are differences in legal regulations between countries regarding cybercrime, which often hinder international cooperation in law enforcement. Technical challenges in identifying and collecting evidence against cross-border hackers also add complexity to the prosecution process. To overcome these challenges, strengthening international cooperation through extradition agreements and mutual legal assistance (MLA) is essential. Indonesia's active participation in international conventions such as the Budapest Convention on Cybercrime is also needed to strengthen cyber law enforcement capabilities at the global level. In addition, increasing the technical capacity of law enforcement officers through training and continuing education in the field of information technology is an important step to increase the effectiveness of law enforcement. Overall, although the legal arrangements in Indonesia are quite adequate, more adaptive regulatory reforms and closer international cooperation are needed to effectively address cross-border hacking crimes.

With these steps, Indonesia can improve legal protection for its people and better face the challenges of cybercrime in the digital era.

5. REFFERENCE

[1] M. R. Habibi and I. Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun J. Pemikir. Dan Pembaharuan Huk. Islam*, vol. 23, no. 2, pp. 400–426, 2020.

[2] M. R. Z. Akbar, "TINDAK PIDANA HACKING DALAM CYBER CRIME DI INDONESIA".

[3] R. D. Hapsari and K. G. Pambayun, "Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023.

[4] S. A. Rakhmat Nur Hakim, "Peretasan Situs KPU, dari IP Address Luar Negeri hingga Disinformasi Rekapitulasi Suara," *Kompas.com*, 2019. https://nasional.kompas.com/read/2019/03/15/10060741/peretasan-situs-kpu-dari-ip-address-luar-negeri-hingga-disinformasi?page=all. (accessed Aug. 27, 2024).

[5] H. A. Putri, "Strategi Pencegahan Cyberstalking Dan Upaya Perlindungan Hukum," *J. BATAVIA*, vol. 1, no. 03, pp. 115–122, 2024.

[6] A. R. Widianingrum, "ANALISIS IMPLEMENTASI KEBIJAKAN HUKUM TERHADAP PENANGANAN KEJAHATAN SIBER DI ERA DIGITAL," *J. IURIS Sci.*, vol. 2, no. 2, pp. 90–102, 2024.

[7] J. F. Kemit and K. L. Kleden, "Yurisdiksi Kejahatan Siber: Borderless," in *Seminar Nasional-Hukum dan Pancasila*, 2023, vol. 2, pp. 55–70.

[8] B. Agung, "Kronologi Peretasan Situs Versi Telkomsel," *CNN Indonesia*, 2017. https://www.cnnindonesia.com/teknologi/20170428174948-185-211012/kronologi-peretasan-situs-versi-telkomsel (accessed Aug. 27, 2024).

[9] Redaksi, "Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia," *CNBC Indonesia*, 2020. https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia (accessed Aug. 27, 2024).

[10] J. P. P. P. D. B. Gunawan, M. S. SH, B. J. P. D. B. Mulyo, and S. I. K. Ratmono, *KUASA SIBER: Sebuah Refleksi Kritis*. PT. Rayyana Komunikasindo, 2022.

[11] Y. Ngamal and M. A. Perajaka, "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia," *J. Manaj. Risiko*, vol. 2, no. 2, pp. 59–74, 2022.

[12] B. K. Arrasuli and K. Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES J. Swara Justisia*, vol. 7, no. 2, pp. 369–392, 2023.

[13] A. R. A. Dzaky, M. Kamal, and B. Badaru, "Efektivitas Penegakan Hukum Terhadap Korban Melalui Aplikasi Pinjaman Online Ilegal Yang Terjadi Di Masyarakat," *J. Lex Theory*, vol. 5, no. 2, pp. 711–729, 2024.

[14] F. R. Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *AL-BAHTS J. Ilmu Sos. Polit. dah Huk.*, vol. 2, no. 1, pp. 8–16, 2024.

[15] A. F. Najwa and A. Husna, "Efektifitas yurisdiksi cybercrime di tengah perkembangan teknologi informasi," *J. Huk. dan Sos. Polit.*, vol. 2, no. 3, pp. 126–135, 2024.

[16] A. M. Rohmy, T. Suratman, and A. I. Nihayaty, "UU ITE dalam Perspektif Perkembangan teknologi informasi dan komunikasi," *Dakwatuna J. Dakwah dan Komun. Islam*, vol. 7, no. 2, pp. 309–339, 2021.

[17] M. Farhan, R. Syaefunaldi, D. R. D. Hidayat, and A. U. Hosnah, "Penerapan Hukum

Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber," *Kult. J. Ilmu Hukum, Sos. dan Hum.*, vol. 1, no. 6, pp. 8–20, 2023.

[18] F. Ramadhani, "Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan Siber," *Kult. J. Ilmu Hukum, Sos. Dan Hum.*, vol. 1, no. 1, pp. 89–97, 2023.

[19] B. Handoyo, M. Z. Husamuddin, and I. Rahma, "Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008," *MAQASIDI J. Syariah dan Huk.*, pp. 40–55, 2024.

[20] Z. A. W. Yuda, H. Rahmasari, and T. A. Gunawan, "EFEKTIVITAS DAN PENERAPAN HUKUM PIDANA TERHADAP CYBERCRIME DI INDONESIA," *Causa J. Huk. dan Kewarganegaraan*, vol. 4, no. 10, pp. 61–70, 2024.

[21] E. Fahamsyah, V. Taniady, K. V. Rachim, and N. W. Riwayanti, "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention," *J. Huk. Dan Syariah Jure*, vol. 14, 2022.

[22] A. ANDIHAR, "REKONSTRUKSI PENANGGULANGAN KEJAHATAN PROSTITUSI DAN PERDAGANGAN ORANG MELALUI CYBER CRIME." Universitas Islam Sultan Agung Semarang, 2024.

[23] N. Aini and F. Lubis, "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN SIBER," *Judge J. Huk.*, vol. 5, no. 02, pp. 55–63, 2024.

[24] J. S. Maringka, *Ekstradisi Dalam Sistem Peradilan Pidana*. Sinar Grafika, 2022.

[25] S. A. N. Wahdini and F. F. B. Irfansyah, "Analisis Keselarasan Pengaturan Yurisdiksi Cyber Crime dengan Implementasinya di Kehidupan Nyata," *Indones. J. Law Justice*, vol. 1, no. 3, p. 11, 2024.

[26] T. W. Putra, H. Abdurrachman, and A. I. Hamzani, *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Penerbit NEM, 2023.