Lex Publica
Jurnal Ilmu Hukum Asosiasi Pimpinan Perguruan Tinggi Hukum Indonesia
e-ISSN: 2579-8855
p-ISSN: 2354-9181
https://journal.appthi.org/index.php/lexpublica

Criminal Law Policy on Carding in Indonesia: Addressing Legal Certainty and Regulatory Fragmentation

Wenggedes Frensh[1*], Rizkan Zulyadi[1], Nindya Dhaneswara[2]

[1]Faculty of Law, Universitas Medan Area, Medan, Indonesia
[2]Department of International and Area Studies, Pukyong National University, Busan, South Korea

**Corresponding author: wenggedesfrensh@staff.uma.ac.id*

Abstract. This study examines the adequacy of legal regulations governing credit card misuse (carding) in cyberspace in Indonesia and their implications for legal certainty and law enforcement effectiveness. Using a normative juridical method, it analyzes key statutes, including Law No. 1 of 2024 (EIT Law amendment), Law No. 27 of 2022 on Personal Data Protection, and Law No. 1 of 2023 on the Criminal Code, supported by conceptual and doctrinal approaches. The findings show that, although these regulations provide a general framework for addressing cybercrime, they remain fragmented and do not explicitly regulate carding as a distinct offense. This gap weakens legal certainty and limits effective enforcement. Two main issues are identified: the absence of specific criminal norms on carding and the lack of harmonization across criminal, cyber, and data protection laws. Current legal policy is also predominantly repressive, with limited preventive and victim-oriented measures.

Keywords: Carding, Cybercrime, Criminal Law Policy, Personal Data Protection, Electronic Transactions Law.

Abstrak. *Studi ini meneliti kecukupan regulasi hukum yang mengatur penyalahgunaan kartu kredit (carding) di dunia maya di Indonesia dan implikasinya terhadap kepastian hukum dan efektivitas penegakan hukum. Dengan menggunakan metode yuridis normatif, studi ini menganalisis undang-undang utama, termasuk Undang-Undang No. 1 Tahun 2024 (Amandemen UU Teknologi Informasi), Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang No. 1 Tahun 2023 tentang KUHP, yang didukung oleh pendekatan konseptual dan doktrinal. Temuan menunjukkan bahwa, meskipun regulasi-regulasi ini memberikan kerangka kerja umum untuk mengatasi kejahatan siber, regulasi tersebut masih terfragmentasi dan tidak secara eksplisit mengatur carding sebagai tindak pidana tersendiri. Kesenjangan ini melemahkan kepastian hukum dan membatasi penegakan hukum yang efektif. Dua isu utama diidentifikasi: tidak adanya norma pidana spesifik tentang carding dan kurangnya harmonisasi di seluruh hukum pidana, hukum siber, dan hukum perlindungan data. Kebijakan hukum saat ini juga didominasi oleh kebijakan represif, dengan langkah-langkah pencegahan dan berorientasi pada korban yang terbatas.*

Kata kunci: *Carding, Kejahatan Siber, Kebijakan Hukum Pidana, Perlindungan Data Pribadi, Hukum Transaksi Elektronik.*

1. Introduction

The rapid development of information and communication technology has transformed legal, economic, and social relations in Indonesia, accelerating the use of digital systems and non-cash payment instruments such as credit cards.[1] While digitalization enhances efficiency and convenience,[2] it also creates new vulnerabilities, particularly through cybercrime that exploits weaknesses in electronic systems and user behavior.[3] In this context, credit card misuse has evolved into a sophisticated form of cybercrime involving unauthorized access and use of financial data, making it an urgent legal issue amid the continued growth of digital transactions in Indonesia.

Data from Bank Indonesia demonstrate a consistent increase in both the volume and value of credit card transactions. In August 2024, credit card transactions grew by 22.79% annually, reaching 41.59 million transactions, while in November 2024, the volume remained high at 41.15 million transactions with a growth rate of 21.1%. In terms of value, transactions reached IDR 35.18 trillion in May 2024.[4] These figures indicate that credit cards remain a significant component of Indonesia's digital payment ecosystem. However, this growth is accompanied by increased risks, particularly the potential misuse of electronic payment data, which may result in financial losses, reputational damage, and reduced public trust in digital financial systems.

The risks associated with credit card misuse are not merely theoretical but are reflected in empirical developments in cybercrime cases. The Financial Services Authority defines carding as the use of illegally obtained debit or credit card data for online transactions without the physical presence of the card.[5] This form of

[1] Dadang Suhendi, and Erwin Asmadi, "Cyber laws related to prevention of theft of information related to acquisition of land and infrastructure resources in Indonesia," *International Journal of Cyber Criminology* 15, no. 2 (2022): 141. See also, Ahmad Syaufi et al., "Employing forensic techniques in proving and prosecuting cross-border cyber-financial crimes," *International Journal of Cyber Criminology* 17, no. 1 (2023): 89.

[2] Rahel Octora et al., "The Urgency of the Indonesian Non-Penal Policy in Regulating Misuse of Bank Accounts as a Means of Online Frauds," *Croatian International Relations Review* 28, no. 90 (2022): 146. See also, Sigid Suseno et al., "Cybercrime in the new criminal code in Indonesia." *Cogent Social Sciences* 11, no. 1 (2025): 2439544.

[3] Bank Indonesia, "Tips dan Transaksi Aman", *Bank Indonesia*, December 1, 2018. See also, Otoritas Jasa Keuangan, "Bijak Ber-eBanking", *OJK*, October 22, 2015.

[4] Bank Indonesia, "Tinjauan Kebijakan Moneter Desember 2024", *Bank Indonesia*, December 19, 2024a. See also, Bank Indonesia, "Tinjauan Kebijakan Moneter Juni 2024", *Bank Indonesia*, June 21, 2024b.; Bank Indonesia, "Tinjauan Kebijakan Moneter September 2024", *Bank Indonesia*, September 19, 2024c.

[5] Dossy Iskandar Prasetyo, and M. Sholehuddin, "Ratio Legis of Cybercrime Legislation Policy in Indonesia," *International Journal of Cyber Criminology* 18, no. 2 (2024): 64. See also, Ahmad Syaufi et

cybercrime is often facilitated through techniques such as phishing, social engineering, and data breaches, which exploit weaknesses in both technological systems and human behavior.[6] Furthermore, data from the Indonesian National Police indicate a significant increase in prosecutions for electronic data manipulation crimes, rising from 11,286 cases in 2023 to 13,922 cases in 2024, representing a 23.35% increase.[7] Although these statistics do not specifically isolate carding, they demonstrate a broader trend of increasing cybercrime involving electronic data misuse, within which credit card fraud constitutes an important component.

From a conceptual perspective, credit card misuse is generally categorized as a subset of cybercrime involving unauthorized access to financial information, illegal use of payment instruments, and resulting economic harm to individuals and financial institutions. Previous studies emphasize that carding represents a serious form of cybercrime that requires robust legal and institutional responses.[8] In practice, however, the legal framework governing such activities in Indonesia remains fragmented. The regulation of credit card misuse relies on a combination of provisions derived from the Criminal Code, the Law on Information and Electronic Transactions (ITE Law), originally Law No. 11 of 2008 and updated by Law No. 19 of 2016 and Law No. 1 of 2024 and other sectoral regulations, rather than a unified and specific legal regime addressing carding as a distinct offense.[9]

This fragmentation creates significant challenges in law enforcement and legal interpretation. Existing legal provisions are often general in nature and not specifically designed to address the complexities of cyber-based financial crimes.

al., "Employing forensic techniques in proving and prosecuting cross-border cyber-financial crimes," *International Journal of Cyber Criminology* 17, no. 1 (2023): 92.

[6] Kemal Farouq Mauladi et al., "Exploring the link between cashless society and cybercrime in Indonesia," *Journal of Telecommunications and the Digital Economy* 10, no. 3 (2022): 67. See also, Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 138.

[7] Pusiknas Bareskrim Polri, "Kasus Kejahatan Manipulasi Data secara ITE Meningkat", *Pusiknas Bareskrim Polri*, June 16, 2025.

[8] Sardjana Orba Manullang, "The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws," *Society* 10, no. 2 (2022): 493. See also, Unzur Jefri Tambunan et al., "Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)," *Jurnal Gagasan Hukum* 6, no. 02 (2024): 147.

[9] Reda Manthovani, "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law," *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 448. See also, Roberth Kurniawan Ruslak Hammar, "Common law approaches to addressing cybercrime and adolescent bullying in Indonesia: Focusing on accountability and protection in the digital age," *International Journal of Cyber Criminology* 16, no. 2 (2022): 169.; Ermanto, Vicko Taniady Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 14.

As a result, law enforcement authorities may face difficulties in applying legal norms to cases involving sophisticated methods of data theft and cross-border transactions. Moreover, the lack of harmonization with international legal standards, such as those reflected in the Budapest Convention on Cybercrime, further complicates efforts to address transnational aspects of carding offenses.[10] These challenges highlight the need for a more coherent and comprehensive legal framework that can effectively respond to the evolving nature of cybercrime.

Credit card fraud poses serious risks to economic stability and consumer trust by undermining confidence in digital transactions and e-business platforms, thereby affecting market behavior.[11] Financial institutions also face reputational damage and operational losses, requiring stronger fraud risk management and cybersecurity measures.[12] However, these efforts must be supported by a clear and robust legal framework to ensure effective and sustainable prevention.

Despite the growing body of literature on cybercrime and credit card fraud in Indonesia, existing studies tend to focus primarily on specific aspects such as law enforcement practices, victim protection, or the criminal liability of perpetrators. While these contributions are valuable, they often overlook the broader dimension of criminal law policy, particularly in terms of evaluating the adequacy and coherence of existing legal norms. There is still limited research that explicitly positions credit card misuse in cyberspace as an object of normative legal analysis aimed at assessing regulatory substance, legal certainty, and policy direction.[13]

Moreover, recent legal developments in Indonesia further underscore the importance of such analysis. The enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) and the amendment to the ITE Law represent significant steps toward strengthening the legal framework governing electronic data and cyber activities. However, there remains a lack of comprehensive studies examining the extent to which these legal instruments are

[10] Ermanto, Vicko Taniady Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 14. See also, M. Erham Amin, and Mokhamad Khoirul Huda, "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia," *International Journal of Cyber Criminology* 15, no. 1 (2021): 88.

[11] Ramakrishna Ayyagari, "Data breaches and carding," In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Cham: Springer International Publishing, 2020), 949. See also, Muhammad Sibawaihi et al., "Islamic Legal Strategies in Indonesian Contexts to Combat Cybercrime and the Spread of Illegal Data Dissemination," *Justicia Islamica* 21, no. 2 (2024): 360.

[12] Yuli Dewi et al., "Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks," *Banks and Bank Systems* 18, no. 4 (2023a): 42.

[13] Mohammad Fadil Imran, "Cyber criminology: An analysis of the Indonesian and the United States police perception," *International Journal of Cyber Criminology* 17, no. 2 (2023): 255. See also, Reda Manthovani, "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law," *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 441.

coherent and effective in addressing specific cybercrimes such as carding. In particular, questions arise regarding whether the existing regulatory framework provides sufficient legal certainty, whether it supports effective law enforcement, and whether it aligns with broader principles of criminal law policy.

This gap highlights the need for a policy-oriented analysis of credit card misuse in cyberspace. Such an approach should not only examine legal norms, but also assess regulatory adequacy, legal certainty, enforcement effectiveness, and policy coherence. It should further include both penal and non-penal strategies to provide a more comprehensive response.[14] Based on the foregoing discussion, this study seeks to analyze criminal law policy concerning credit card misuse in cyberspace in Indonesia. Specifically, this research aims to address three main issues. First, it examines the extent to which existing legal regulations adequately and clearly regulate credit card misuse (carding) in cyberspace. Second, it analyzes how current legal provisions influence legal certainty and the effectiveness of law enforcement in addressing such crimes. Third, it formulates the direction of future criminal law policy to develop a more coherent and comprehensive regulatory framework for combating credit card misuse in Indonesia.

This study contributes theoretically by enriching cybercriminal law through a normative analysis of credit card misuse. Practically, it provides guidance for policymakers and law enforcement in developing effective strategies to address cybercrime. Strengthening the legal framework is essential to protect interests and maintain public trust in Indonesia's digital economy.

2. Research Methods

This study employs a normative legal research method, also known as doctrinal legal research, focusing on the analysis of positive legal norms governing carding as a form of cybercrime in Indonesia.[15] In this approach, law is understood as a system of norms, principles, and doctrines that are systematically examined to

[14] Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 137. See also, M. Erham Amin, and Mokhamad Khoirul Huda, "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia," *International Journal of Cyber Criminology* 15, no. 1 (2021): 86.; Elfian Fauzy, and Nabila Alif Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022): 453.

[15] Yudho Taruno Muryanto, "The urgency of sharia compliance regulations for Islamic Fintechs: a comparative study of Indonesia, Malaysia and the United Kingdom," *Journal of Financial Crime* 30, no. 5 (2023): 1271. See also, Craig Webber, and Michael Yip, "Humanizing the cybercriminal: Markets, forums, and the carding subculture," In *The human factor of cybercrime* (Oxfordshire: Routledge, 2019), 269.

address legal issues. Unlike empirical research, this method does not rely on field data but emphasizes the identification, interpretation, and systematization of applicable law.[16] This approach is appropriate for examining the adequacy and coherence of legal frameworks regulating carding in cyberspace.

The study applies two approaches: the statute approach and the conceptual approach. The statute approach analyzes relevant legal instruments, including the Criminal Code, ITE Law and PDP Law This enables an evaluation of how far existing regulations accommodate carding as a specific cybercrime offense. The conceptual approach is used to examine key legal concepts such as cybercrime, criminal law policy, personal data protection, and unauthorized access to electronic financial data based on legal doctrines and scholarly perspectives.[17]

The legal materials used consist of primary and secondary sources. Primary materials include statutory regulations and relevant court decisions. Secondary materials comprise books, journal articles, and prior studies on cybercrime, criminal law, and data protection. All materials are collected through library research involving systematic identification and review of relevant sources.[18]

The analysis is conducted qualitatively using descriptive-analytical and prescriptive approaches. The descriptive-analytical method explains and interprets existing legal provisions, while the prescriptive approach evaluates their adequacy and formulates recommendations for future legal reform. This reflects the nature of normative legal research, which addresses both the law as it is (*das sein*) and the law as it ought to be (*das sollen*).[19] The study is limited to criminal law policy on carding in cyberspace, focusing on regulatory substance, legal certainty, and the direction of legal reform in Indonesia.

[16] Zainuddin Ali, *Metode Penelitian Hukum*, (Jakarta: Sinar Grafika, 2021), 39. See also, Terry Hutchinson, and Nigel Duncan, "Defining and describing what we do: doctrinal legal research," *Deakin law review* 17, no. 1 (2012): 96.; M.M. Peter, *Penelitian Hukum*, (Jakarta: Kencana, 2009), 76.

[17] Ali Fikri Hamdhani, and Fajrianto Fajrianto, "Relevansi Penerapan Metode Omnibus Law dalam Sistem Peraturan Perundang-Undangan di Indonesia," *Jurnal Al Azhar Indonesia Seri Ilmu Sosial* 5, no. 1 (2024): 36.

[18] Zainuddin Ali, *Metode Penelitian Hukum*, (Jakarta: Sinar Grafika, 2021), 39. See also, S. Soekanto, *Pengantar Penelitian Hukum*, (Depok: Universitas Indonesia, 1981), 115.

[19] M.M. Peter, *Penelitian Hukum*, (Jakarta: Kencana, 2009), 76. See also, Terry Hutchinson, and Nigel Duncan, "Defining and describing what we do: doctrinal legal research," *Deakin law review* 17, no. 1 (2012): 96.

3. Results and Discussion

3.1. Adequacy and Clarity of Indonesian Legal Framework in Regulating Carding

Indonesian positive law has formally recognized carding as part of cybercrime; however, the adequacy and clarity of its regulation remain fundamentally limited. This limitation stems from the absence of a single, integrated legal framework that explicitly defines and regulates carding as a distinct criminal offense. Instead, the legal response to carding is dispersed across multiple legal instruments, resulting in a fragmented and interpretative regulatory structure.

At a conceptual level, carding is generally understood as a form of cybercrime involving the unauthorized acquisition and use of credit or debit card information for financial transactions without the consent of the legitimate cardholder. It typically involves techniques such as phishing, hacking, data breaches, or social engineering to obtain card data, followed by its use in online transactions.[20] In the Indonesian context, this understanding is also reflected in institutional interpretations, such as those of the Financial Services Authority (OJK), which describes carding as online transactions conducted using illegally obtained payment card data without physical possession of the card. This definition highlights that carding is inherently linked to the misuse of electronic data and digital identity, placing it firmly within the domain of cybercrime rather than conventional fraud.

Despite this relatively clear conceptual understanding, Indonesian law does not provide a specific statutory definition of carding. Instead, the regulation of such conduct is indirectly accommodated within broader cybercrime provisions, particularly under ITE Law. This law serves as the primary legal instrument for addressing cyber-related offenses in Indonesia, including unauthorized access, illegal interception, data manipulation, and misuse of electronic information. These provisions are frequently applied in prosecuting carding cases, as the core elements of the crime, namely unauthorized access to electronic systems and unlawful use of data, fall within their scope.[21]

---

[20] Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 139. See also, Raj Singh Deora, and Dhaval Chudasama, "Brief study of cybercrime on an internet," *Journal of communication engineering & Systems* 11, no. 1 (2021): 3.

[21] Unzur Jefri Tambunan et al., "Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)," *Jurnal Gagasan Hukum* 6, no. 02 (2024): 146. See also, Pemerintah Pusat Indonesia, "Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", *Database Peraturan*, January 2, 2024.

In addition to the ITE Law, PDP Law introduces an important complementary dimension by recognizing financial data, including credit card information, as protected personal data. This law establishes obligations for data controllers and processors to ensure the security and confidentiality of personal data, as well as sanctions for unlawful processing, disclosure, or misuse. From this perspective, carding can also be interpreted as a violation of personal data protection, as it involves unauthorized access and exploitation of sensitive financial information.[22] The legal framework addressing carding in Indonesia operates at the intersection of cybercrime and data protection law. However, it lacks conceptual clarity, as carding is not explicitly defined as a distinct offense.[23]

As a result, carding is better described as being "legally accommodated" rather than "specifically regulated." This distinction is crucial from a doctrinal perspective. A legal norm is considered adequate not merely when it exists, but when it clearly defines the prohibited conduct, identifies the subject of the offense, and determines the legal consequences.

For example, the act of obtaining credit card data through hacking may fall under provisions on unauthorized access, while the use of such data for transactions may be classified as fraud or data manipulation. Similarly, the possession or distribution of stolen card data may be interpreted as a violation of personal data protection. This creates ambiguity in defining carding. It reflects a broader issue in cybercrime law, where new digital crimes are handled through general, adaptive norms rather than clear, specific regulations.[24]

The lack of specificity in regulating carding also has implications for the systematic coherence of criminal law. In a well-structured legal system, criminal offenses are formulated in a manner that reflects the distinctive characteristics of the conduct being regulated. This includes not only the physical elements of the act (*actus reus*), but also the mental elements (*mens rea*), the method of commission, and the resulting harm. In the case of carding, these elements are closely linked to technological processes, such as data extraction, digital transmission, and online transactions. However, the current legal framework does not fully integrate these elements into a unified offense structure, resulting in a partial and fragmented representation of the crime.

---

[22] Pemerintah Pusat Indonesia, "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi", *Database Peraturan*, October 17, 2022.

[23] Reda Manthovani, "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law," *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 445. See also, Lenny Nadriana, and Pandji Sukmana, "Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges," *International Journal of Cyber Criminology* 16, no. 2 (2022): 198.

[24] Giovanni Tuzet, "Certainty Beyond a Reasonable Doubt: A Pragmatist Understanding of the Criminal Standard of Proof," *Contemporary Pragmatism* 20, no. 4 (2023): 416.

The rapid growth of digital transactions in Indonesia, particularly in the use of credit cards, has significantly increased the exposure to carding risks. Data from Bank Indonesia indicate substantial growth in both the volume and value of credit card transactions throughout 2024, reflecting the expanding role of electronic payment systems in the national economy.[25] At the same time, there has been a notable increase in cases involving electronic data manipulation, as evidenced by law enforcement statistics showing a 23.35% rise in such cases between 2023 and 2024.[26]

These developments indicate that carding is not an isolated phenomenon, but part of a broader trend of cybercrime that is structurally embedded within the digital economy. In this context, the absence of a clear and specific legal framework weakens the preventive function of criminal law.[27] Another important aspect of regulatory adequacy concerns the ability of the legal framework to adapt to the transnational nature of carding. Cybercrime often involves cross-border elements, such as the use of foreign servers, international payment systems, and global networks of perpetrators.[28] However, the current Indonesian legal framework is primarily oriented toward domestic regulation and does not fully address the complexities of transnational cybercrime. Studies have shown that the lack of alignment with international standards and cooperation mechanisms further limits the effectiveness of legal responses to carding.[29]

In addition, the existing regulatory framework has not yet achieved full integration between preventive, protective, and repressive dimensions, particularly regarding the legal responsibilities of financial institutions and electronic system

[25] Bank Indonesia, "Tinjauan Kebijakan Moneter Desember 2024", *Bank Indonesia*, December 19, 2024a. See also, Bank Indonesia, "Tinjauan Kebijakan Moneter Juni 2024", *Bank Indonesia*, June 21, 2024b.; Bank Indonesia, "Tinjauan Kebijakan Moneter September 2024", *Bank Indonesia*, September 19, 2024c.

[26] Pusiknas Bareskrim Polri, "Kasus Kejahatan Manipulasi Data secara ITE Meningkat", *Pusiknas Bareskrim Polri*, June 16, 2025.

[27] Eric Rutger Leukfeldt, and Thomas J. Holt, "Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals," *Computers in Human Behavior* 126, no. 8 (2022): 106979. See also, Yuli Dewi et al., "What is the key determinant of the credit card fraud risk assessment in Indonesia? An idea for brainstorming," *Banks and Bank Systems* 18, no. 1 (2023b): 24.

[28] Eddy Rifai, and H. S. Tisnanta, "Role of law enforcement to prevent cyber laundering and asset recovery from overseas," *International Journal of Cyber Criminology* 16, no. 1 (2022): 118. See also, Graeme R. Newman, "Cybercrime," In *Handbook on crime and deviance* (New York: Springer New York, 2009), 568.

[29] Ermanto Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 13. See also, Ichsan Anwary, "Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach," *International Journal of Cyber Criminology* 17, no. 1 (2023): 17.

providers.[30] Although the PDP Law introduces obligations for data controllers, these obligations remain only partially connected to criminal law enforcement mechanisms and are not systematically aligned with provisions under the ITE Law or the Criminal Code. As a result, regulatory design tends to emphasize ex post criminal liability rather than ex ante risk mitigation, compliance standards, and systemic prevention. The Indonesian legal framework governing carding is formally established but substantively insufficient. The absence of a clear legal definition, fragmented norms across multiple laws, and the lack of coherent criminal formulations result in a regulatory structure that lacks clarity, consistency, and doctrinal completeness. Current regulation remains dependent on interpretation rather than a unified legal framework.

3.2. Legal Certainty and Effectiveness of Law Enforcement in Addressing Carding

Although existing regulations, primarily the ITE Law and related legal instruments, provide a formal basis for prosecuting cybercrime, their fragmented and generalized nature creates structural challenges in interpretation and implementation.[31] As a result, the enforcement of law against carding operates within a framework that is normatively available but practically inconsistent.

From the perspective of legal certainty, the absence of a specific legal formulation of carding as a distinct criminal offense creates ambiguity in legal classification. Carding, commonly understood as a cybercrime involving the unauthorized acquisition and use of credit card data, is not explicitly defined in Indonesian legislation. Instead, law enforcement authorities must interpret carding conduct through a variety of general provisions, such as unauthorized access, electronic data manipulation, fraud, or violations of personal data protection. This multiplicity of legal bases leads to inconsistent legal qualification of similar acts, depending on the interpretation adopted by investigators, prosecutors, or judges. Consequently, this condition undermines the principle of *lex certa*, which requires that criminal norms be clearly defined, precise, and predictable.[32]

---

[30] Romi Fadillah Rahmat et al., "News articles classification for electronic information and transaction law in indonesia using support vector machine," In *2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA)* (New Jersey: IEEE, 2021), 108.

[31] Maxim Malina, "The use of artificial intelligence in the administration of criminal justice: problems and prospects," *Gosudarstvo i pravo* 1, no. 4 (2022): 95. See also, Reda Manthovani, "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law," *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 443.

[32] Winahyu Erwiningsih, "Enhancing legal certainty in land collateral: Bridging regulatory gaps, mitigating vulnerabilities, and promoting credit access in Indonesia," *Croatian International Relations Review* 29, no. 93 (2023): 34. See also, Ratih Mega Puspa Sari, "Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia," *Jurnal Hukum dan Keadilan* 2, no. 5 (2025): 52.

In Indonesia, emerging digital crimes like phishing, hacking, and carding are addressed through flexible, non-specific legal norms. While this allows authorities to adapt and prosecute offenders, it creates uncertainty, as individuals cannot clearly foresee what constitutes a crime. This interpretative approach also leads to inconsistent court decisions, weakening legal predictability and public trust. The lack of a precise legal definition of carding highlights a doctrinal gap in the regulatory framework, undermining legal certainty and the rule of law, where clarity and predictability are essential for individuals to regulate their behavior according to established norms.[33]

From the perspective of law enforcement effectiveness, the reliance on general legal provisions significantly complicates the prosecution of carding cases. Law enforcement authorities must construct legal arguments by linking the factual elements of carding, such as unauthorized data acquisition, digital transactions, and financial fraud, to broader legal norms that were not specifically designed to address such conduct. This process often requires complex interpretation and technical understanding, which may exceed the capacity of traditional criminal justice mechanisms.[34]

Moreover, the technological nature of carding introduces additional enforcement challenges. Carding is typically conducted through sophisticated methods, including phishing, malware attacks, data breaches, and anonymization technologies such as Virtual Private Networks (VPNs) and cryptocurrencies. These techniques obscure the identity and location of perpetrators, making it difficult for law enforcement agencies to collect evidence and establish jurisdiction. The rapid development of digital technology further exacerbates this challenge, as legal frameworks and enforcement capacities often lag behind technological innovation.[35]

In this context, the effectiveness of law enforcement is not solely determined by the existence of legal norms, but also by institutional capacity and technological readiness. Studies indicate that Indonesian law enforcement agencies face limitations in digital forensic expertise, technical infrastructure, and inter-agency

[33] Michael Yip et al., "Trust among cybercriminals? Carding forums, uncertainty and implications for policing," In *Policing cybercrime* (Oxfordshire: Routledge, 2017), 121.

[34] Ermanto Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 13. See also, M. Erham Amin, and Mokhamad Khoirul Huda, "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia," *International Journal of Cyber Criminology* 15, no. 1 (2021): 83.

[35] Erwin Asmadi et al., "Data theft and the law on protection of personal data: A thematic analysis," *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 143. See also, Ferry Irawan Febriansyah et al., "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," *International Journal of Law and Society* 5, no. 1 (2026): 34.

coordination, all of which are critical for addressing cybercrime.[36] Another significant issue concerns the lack of integration between criminal law and data protection regimes. The enactment of the PDP Law represents an important development in recognizing financial data, including credit card information, as a protected legal interest. However, its relationship with criminal law provisions remains insufficiently harmonized. As a result, violations involving personal financial data may be treated inconsistently, either as administrative infractions, civil disputes, or criminal offenses, depending on the interpretative approach taken by authorities.

In addition, the current legal framework demonstrates a limited orientation toward victim protection. Carding is often treated primarily as a property crime, focusing on financial loss suffered by victims or institutions. However, contemporary scholarship emphasizes that cybercrimes such as carding also involve violations of privacy and personal data security, which have broader implications for individual rights.[37] Despite this, Indonesian criminal law provisions remain predominantly punitive, emphasizing the punishment of offenders rather than the restoration of victims or the protection of their data. This approach is inconsistent with modern cybercrime policies, which advocate a balance between repressive (penal) and preventive or restorative measures.[38]

Furthermore, public awareness and perception play a crucial role in determining the effectiveness of law enforcement. Empirical studies suggest that low levels of public understanding of cyber law, including the ITE Law, contribute to the persistence of cybercrime.[39] When individuals are not adequately informed about legal risks or reporting mechanisms, the likelihood of prevention and early detection decreases. Additionally, weak public confidence in law enforcement effectiveness may reduce compliance and discourage victims from reporting carding incidents, thereby perpetuating under-enforcement.

In light of the foregoing analysis, the need to strengthen legal certainty and enforcement effectiveness in addressing carding in Indonesia becomes both

[36] Erwin Asmadi et al., "Data theft and the law on protection of personal data: A thematic analysis," *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 136.

[37] Melvin RJ Soudijn, and Birgit CH T. Zegers, "Cybercrime and virtual offender convergence settings," *Trends in organized crime* 15, no. 2 (2012): 119. See also, Finda Pratiwi Yuwono, "Legal Implications of the Merauke Food Estate: A Critical Analysis of Customary Rights and Environmental Concerns," *Lex Publica* 11, no. 2 (2024): 304.

[38] Dicky Malik Ibrahim et al., "Legal Protection of Banking Customers Who Are Victims of Information and Electronic Transaction Crimes," *Jurnal Ilmiah Penegakan Hukum* 11, no. 1 (2024): 111.

[39] Erik O. Eriksen, "Three modes of administrative behaviour: Differentiated policy implementation and the problem of legal certainty," *Journal of European Public Policy* 30, no. 12 (2023): 2633. See also, Erwin Asmadi et al., "Data theft and the law on protection of personal data: A thematic analysis," *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 149.

normatively and practically imperative.[40] From a criminal law policy perspective, the absence of specific legal provisions on carding not only weakens the principle of *lex certa*, but also limits the ability of law enforcement institutions to respond consistently to increasingly sophisticated cybercrimes. An effective policy framework requires a balance between penal and non-penal approaches, supported by clearer legal formulations that explicitly recognize carding as a distinct offense.[41] This is particularly important given the growing intersection between criminal law, technological development, and digital commercial transactions, which demands a more adaptive and context-sensitive legal framework.[42] Furthermore, the rising incidence of data theft underscores the urgency of harmonizing criminal law with personal data protection regimes to ensure comprehensive legal protection.[43]

Legal certainty, in this regard, can only be achieved when legal norms are not merely formally enacted but also coherently structured and consistently enforced.[44] At the same time, the rapid evolution of digital technology necessitates a broader transformation of legal strategies, including strengthening cybersecurity systems, enhancing digital forensic capabilities, and improving institutional coordination among enforcement bodies. From a sociological perspective, ineffective enforcement and regulatory ambiguity risk undermining public trust and compliance, particularly within the expanding fintech ecosystem where legal awareness remains uneven.[45]

3.3. Direction of Criminal Law Policy Reform for a Coherent Carding Framework

Based on the identified normative deficiencies and enforcement challenges, the reformulation of criminal law policy concerning carding in Indonesia must be positioned within a forward-looking framework of *ius constituendum*, namely the

[40] Ferry Irawan Febriansyah et al., "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," *International Journal of Law and Society* 5, no. 1 (2026): 36.

[41] Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 139. See also, Yuli Dewi et al., "What is the key determinant of the credit card fraud risk assessment in Indonesia? An idea for brainstorming," *Banks and Bank Systems* 18, no. 1 (2023b): 23.

[42] Ridwan Arifin et al., "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud," *Jurnal Hukum Novelty* 11, no. 2 (2020): 234.

[43] Erwin Asmadi et al., "Data theft and the law on protection of personal data: A thematic analysis," *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 142.

[44] Muhammad Dahlan, and Husni Jalil, "Electronic Traffic Law Enforcement Policy Within the Framework of Legal Certainty," *PETITA* 8, no. 2 (2023): 278.

[45] Trubus Rahardiansah, "Sociological Analysis of Fintech Law Enforcement in the Digital Era," *Revista de Gestao Social e Ambiental* 18, no. 2 (2024): 664.

development of law that is responsive to technological evolution and capable of addressing regulatory gaps.[46]

The first and most fundamental direction of reform is the explicit recognition of carding as a distinct criminal offense within Indonesian law. Doctrinally, the principle of legality, particularly *nullum crimen sine lege certa*, requires that criminal conduct be formulated in clear, precise, and unambiguous terms.[47] Therefore, a reformed legal framework should clearly articulate the constitutive elements of carding, including: (i) unauthorized acquisition of financial or payment card data through technological means such as phishing, hacking, or data breaches; (ii) possession or distribution of such data; and (iii) the use of such data for fraudulent transactions. This explicit formulation would not only fulfill the principle of *lex certa*, but also provide clearer guidance for law enforcement and judicial authorities.

The second direction of reform concerns the harmonization of existing legal instruments. At present, the regulation of carding is dispersed across multiple legal regimes, including the ITE Law, the PDP Law, and the Criminal Code. This fragmentation creates overlaps, inconsistencies, and potential conflicts in legal interpretation and enforcement.[48] Harmonization, therefore, should aim to integrate these legal regimes into a unified and systematic framework. This includes aligning the definitions of offenses, standardizing sanctions, and clarifying the relationship between administrative, civil, and criminal liabilities. The integration of data protection principles into criminal law is particularly important, given that carding inherently involves the misuse of personal financial data. As highlighted in recent studies, effective cybercrime regulation requires an approach that bridges criminal law with data protection and cybersecurity governance.[49]

The third critical dimension of reform is the adoption of a victim-oriented approach within criminal law policy. Traditionally, carding has been treated primarily as a property crime, focusing on financial loss suffered by individuals or

[46] Reda Manthovani, "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law," *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 442.

[47] Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 140. See also, Ridwan Arifin et al., "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud," *Jurnal Hukum Novelty* 11, no. 2 (2020): 232.

[48] Ermanto Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 9. See also, M. Erham Amin, and Mokhamad Khoirul Huda, "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia," *International Journal of Cyber Criminology* 15, no. 1 (2021): 86.

[49] Roger A. Shiner, "Theorizing criminal law reform," *Criminal Law and Philosophy* 3, no. 2 (2009): 178. See also, Eyad Abdel Latif Marazqah Btoush et al., "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," *PeerJ Computer Science* 9, no. 3 (2023): 1195.; Erwin Asmadi et al., "Data theft and the law on protection of personal data: A thematic analysis," *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 146.

financial institutions. However, contemporary perspectives emphasize that carding also constitutes a violation of privacy and personal data rights, which requires a broader framework of victim protection.[50] Accordingly, legal reform should incorporate mechanisms for victim protection, compensation, and recovery.

This includes strengthening reporting mechanisms, ensuring accessible complaint procedures, and providing legal remedies that address both material and immaterial harm. In addition, financial institutions should be assigned clearer responsibilities in safeguarding customer data and mitigating risks associated with digital transactions. Such an approach aligns with modern cybercrime policies, which emphasize not only punitive measures but also restorative justice and victim empowerment.[51]

Fourth, the reformulation of criminal law policy must incorporate a balanced integration of penal and non-penal strategies. While criminal sanctions remain an essential tool for deterrence and retribution, overreliance on punitive measures may lead to inefficiencies and fail to address the root causes of cybercrime. The principle of *ultimum remedium* requires that criminal law be used as a last resort, complemented by preventive and regulatory approaches.[52] In the context of carding, this means combining criminalization with broader measures such as public education, cybersecurity enhancement, and institutional capacity building.

Studies highlight the importance of non-penal strategies in reducing cybercrime risks. Public awareness campaigns, digital literacy programs, and responsible financial behavior can significantly reduce vulnerabilities to carding.[53] At the same time, strengthening cybersecurity infrastructure and fraud detection systems within financial institutions can prevent unauthorized access to sensitive data.[54] Institutional capacity building, including training in digital forensics and cyber

[50] Melvin RJ Soudijn, and Birgit CH T. Zegers, "Cybercrime and virtual offender convergence settings," *Trends in organized crime* 15, no. 2 (2012): 119.

[51] Dicky Malik Ibrahim et al., "Legal Protection of Banking Customers Who Are Victims of Information and Electronic Transaction Crimes," *Jurnal Ilmiah Penegakan Hukum* 11, no. 1 (2024): 111. See also, Erika Kraemer-Mbula et al., "The cybercrime ecosystem: Online innovation in the shadows?," *Technological Forecasting and Social Change* 80, no. 3 (2013): 547.

[52] A. V. Endol'tseva et al., "Bazovye nachala ugolovnoi politiki: ot teoreticheskikh rassuzhdenii k de lege ferenda [Basic Principles of Criminal Policy: From Theoretical Reasoning to de Lege Ferenda]," *Vserossiiskii kriminologicheskii zhurnal* 13, no. 4 (2019): 646.

[53] Muhammad Isnaeni Puspito Adhi, and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform* 17, no. 2 (2021): 140. See also, Ioan Durnescu, and Kristel Beyens, "The avalanche of technology: Critical perspectives on digital penality in Europe," In *The Routledge Handbook of European Penology* (London: Routledge, 2025), 285.

[54] Yuli Dewi et al., "Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks," *Banks and Bank Systems* 18, no. 4 (2023a): 40. See also, Cornelius Friesendorf, and Philipp Neubauer, "Best Practices in Security Sector Reform: EU Efforts to Change Ukraine's Public Order Policing," *Journal of Intervention and Statebuilding* 19, no. 3 (2025): 380.

investigation techniques, is also essential for improving enforcement effectiveness.[55]

The fifth direction of reform relates to the need for technological adaptability and responsiveness within the legal framework. Carding is inherently dynamic, evolving in response to technological advancements and changes in digital ecosystems. Therefore, legal norms must be flexible enough to accommodate new forms of cybercrime without requiring constant legislative revision. This can be achieved through the use of technology-neutral language, adaptive regulatory mechanisms, and periodic legal reviews.[56] At the same time, safeguards must be established to ensure that the use of advanced technologies in law enforcement, such as artificial intelligence and data analytics, remains consistent with principles of due process and human rights.[57]

In addition, the transnational nature of carding necessitates stronger international cooperation and alignment with global legal standards. Carding operations often involve cross-border transactions, distributed networks, and international data flows, which cannot be effectively addressed through purely domestic legal frameworks. Therefore, Indonesia should enhance its participation in international cybercrime cooperation mechanisms and align its legal framework with global standards and best practices.[58] This includes cooperation in information sharing, joint investigations, and harmonization of legal definitions and procedures.

Furthermore, sociological considerations must also inform the direction of criminal law reform. Cybercrime, including carding, is not only a legal issue but also a social phenomenon influenced by factors such as economic inequality, digital literacy, and public trust in institutions. As noted in socio-legal studies, ineffective

---

[55] Ferry Irawan Febriansyah et al., "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity," *International Journal of Law and Society* 5, no. 1 (2026): 32.

[56] Djoni Sumardi Gojali, "Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective," *International Journal of Cyber Criminology* 17, no. 1 (2023): 6.

[57] Miguel Ramón Viguri Axpe, "Ethical challenges from artificial intelligence to legal practice," In *International Conference on Hybrid Artificial Intelligence Systems* (Cham: Springer International Publishing, 2021), 201. See also, Ilia S. Dikarev, and Vitalii F. Vasyukov, "Perspectives of implementing "smart" digital technologies in criminal justice," In *Institute of Scientific Communications Conference* (Cham: Springer International Publishing, 2020), 1309.

[58] Ermanto Fahamsyah et al., "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention," *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 9. See also, Tofik Chandra, and Ji Hyun Park, "Enforcing legal measures against illegal fishing by foreign fishermen in territorial waters: Challenges and solutions," *Lex Publica* 10, no. 2 (2023): 71.; Andri Yanto Faisal et al., "Genuine paradigm of criminal justice: rethinking penal reform within Indonesia New Criminal Code," *Cogent Social Sciences* 10, no. 1 (2024): 2301630.

law enforcement and regulatory ambiguity can erode public confidence and reduce compliance with legal norms.[59]

Finally, the reformulation of criminal law policy must be understood as part of a broader transformation of the legal system in response to digitalization. The integration of criminal law, technology, and commercial regulation is essential for addressing the complex nature of carding as a cyber-enabled financial crime.[60] This requires a holistic approach that combines doctrinal clarity, institutional capacity, technological innovation, and societal awareness.

In conclusion, the direction of criminal law policy reform for carding in Indonesia must focus on several key dimensions: explicit criminalization, harmonization of legal regimes, victim protection, integration of penal and non-penal strategies, technological adaptability, and international cooperation. These reforms are grounded in fundamental principles of criminal law, including legal certainty, *lex certa*, and *ultimum remedium*, and are necessary to address the evolving challenges of cybercrime in the digital era.

4. Conclusion

This study concludes that carding, as a form of credit card misuse in cyberspace, constitutes a complex and evolving cybercrime that challenges the adequacy of Indonesia's existing legal framework. This research finds that although current regulations, such as the Electronic Information and Transactions Law, the Personal Data Protection Law, and general criminal provisions, provide a foundational basis, they remain fragmented and lack a specific formulation of carding as a distinct criminal offense. This normative gap weakens the principle of legal certainty (*lex certa*) and limits the effectiveness of law enforcement in addressing increasingly sophisticated cybercrime practices. The study further identifies two principal structural issues: the absence of explicit criminal norm formulation on carding and the lack of harmonization between criminal law, cyber law, and personal data protection regimes.

In addition, the prevailing legal policy remains predominantly repressive and has not fully incorporated a victim-oriented approach, particularly in terms of restitution, protection of personal data, and preventive obligations for financial service providers. In line with the research objectives, this study emphasizes the

[59] Trubus Rahardiansah, "Sociological Analysis of Fintech Law Enforcement in the Digital Era," *Revista de Gestao Social e Ambiental* 18, no. 2 (2024): 611.

[60] Ridwan Arifin et al., "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud," *Jurnal Hukum Novelty* 11, no. 2 (2020): 234. See also, Jack Nicholls et al., "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," *Ieee Access* 9, no. 3 (2021): 163972.

urgency of reformulating criminal law policy through several strategic directions: the explicit criminalization of carding, regulatory harmonization across relevant legal instruments, and the strengthening of victim protection mechanisms. Furthermore, legal policy must be adaptive to technological developments and responsive to the transnational nature of cybercrime. Overall, this study affirms that a coherent, integrated, and forward-looking legal framework is essential to ensure legal certainty, enhance enforcement effectiveness, and provide comprehensive protection in the digital financial ecosystem in Indonesia.

References

Adhi, Muhammad Isnaeni Puspito, and Eko Soponyono. "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law." *Law Reform* 17, no. 2 (2021): 135-144.

Ali, Zainuddin. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2021.

Amin, M. Erham, and Mokhamad Khoirul Huda. "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia." *International Journal of Cyber Criminology* 15, no. 1 (2021): 79-94.

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.

Arifin, Ridwan, Hartini Atikasari, and Waspiah Waspiah. "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud." *Jurnal Hukum Novelty* 11, no. 2 (2020): 229-246.

Asmadi, Erwin, Adi Mansar, Triono Eddy, Mukti Fajar Nur Dewata, Farid Wajdi, and Norhasliza Binti Ghapa. "Data theft and the law on protection of personal data: A thematic analysis." *Jurnal Hukum Novelty (1412-6834)* 15, no. 2 (2024): 122-171.

Axpe, Miguel Ramón Viguri. "Ethical challenges from artificial intelligence to legal practice." In *International Conference on Hybrid Artificial Intelligence Systems*, pp. 196-206. Cham: Springer International Publishing, 2021.

Ayyagari, Ramakrishna. "Data breaches and carding." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 939-959. Cham: Springer International Publishing, 2020.

Bank Indonesia. "Tinjauan Kebijakan Moneter Desember 2024". *Bank Indonesia*, December 19, 2024a. https://www.bi.go.id/id/publikasi/laporan/Pages/TKM-Desember-2024.aspx.

Bank Indonesia. "Tinjauan Kebijakan Moneter Juni 2024". *Bank Indonesia*, June 21, 2024b. https://www.bi.go.id/id/publikasi/laporan/Pages/TKM-Juni-2024.aspx.

Bank Indonesia. "Tinjauan Kebijakan Moneter September 2024". *Bank Indonesia*, September 19, 2024c. https://www.bi.go.id/id/publikasi/laporan/Pages/TKM-September-2024.aspx.

Bank Indonesia. "Tips dan Transaksi Aman". *Bank Indonesia*, December 1, 2018. https://www.bi.go.id/id/edukasi/Pages/Tips-dan-Transaksi-Aman.aspx.

Btoush, Eyad Abdel Latif Marazqah, Xujuan Zhou, Raj Gururajan, Ka Ching Chan, Rohan Genrich, and Prema Sankaran. "A systematic review of literature on credit card cyber fraud detection using machine and deep learning." *PeerJ Computer Science* 9, no. 3 (2023): 1169-1264.

Chandra, Tofik, and Ji Hyun Park. "Enforcing legal measures against illegal fishing by foreign fishermen in territorial waters: Challenges and solutions." *Lex Publica* 10, no. 2 (2023): 64-78.

Dahlan, Muhammad, and Husni Jalil. "Electronic Traffic Law Enforcement Policy Within The Framework of Legal Certainty." *PETITA* 8, no. 2 (2023): 245-305.

Deora, Raj Singh, and Dhaval Chudasama. "Brief study of cybercrime on an internet." *Journal of communication engineering & Systems* 11, no. 1 (2021): 1-6.

Dewi, Yuli, Harry Suharman, Poppy Sofia Koeswayo, and Nanny Dewi Tanzil. "Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks." *Banks and Bank Systems* 18, no. 4 (2023a): 33-48.

Dewi, Yuli, Harry Suharman, Poppy Sofia Koeswayo, and Nanny Dewi Tanzil. "What is the key determinant of the credit card fraud risk assessment in Indonesia? An idea for brainstorming." *Banks and Bank Systems* 18, no. 1 (2023b): 19-28.

Dikarev, Ilia S., and Vitalii F. Vasyukov. "Perspectives of implementing "smart" digital technologies in criminal justice." In *Institute of Scientific Communications Conference*, pp. 1306-1312. Cham: Springer International Publishing, 2020.

Durnescu, Ioan, and Kristel Beyens. "The avalanche of technology: Critical perspectives on digital penality in Europe." In *The Routledge Handbook of European Penology*, pp. 279-293. London: Routledge, 2025.

Endol'tseva, A. V., Yu V. Endoltseva, and N. I. Platonova. "Bazovye nachala ugolovnoi politiki: ot teoreticheskikh rassuzhdenii k de lege ferenda [Basic Principles of Criminal Policy: From Theoretical Reasoning to de Lege Ferenda]." *Vserossiiskii kriminologicheskii zhurnal* 13, no. 4 (2019): 641-650.

Eriksen, Erik O. "Three modes of administrative behaviour: Differentiated policy implementation and the problem of legal certainty." *Journal of European Public Policy* 30, no. 12 (2023): 2623-2642.

Erwiningsih, Winahyu. "Enhancing legal certainty in land collateral: Bridging regulatory gaps, mitigating vulnerabilities, and promoting credit access in Indonesia." *Croatian International Relations Review* 29, no. 93 (2023): 26-49.

Fahamsyah, Ermanto, Vicko Taniady, Kania Venisa Rachim, and Novi Wahyu Riwayanti. "Penerapan prinsip aut dedere aut judicare terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention." *Jurnal Hukum dan Syariah De Jure* 14, no. 1 (2022): 1-18.

Faisal, Andri Yanto, Derita Prapti Rahayu, Dwi Haryadi, Anri Darmawan, and Jeanne Darc Noviayanti Manik. "Genuine paradigm of criminal justice: rethinking penal reform within Indonesia New Criminal Code." *Cogent Social Sciences* 10, no. 1 (2024): 2301626-2301639.

Fauzy, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2022): 445-461.

Febriansyah, Ferry Irawan, Afiful Ikhwan, Ulya Shafa Firdausi, and Ayub Dwi Anggoro. "Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity." *International Journal of Law and Society* 5, no. 1 (2026): 26-44.

Friesendorf, Cornelius, and Philipp Neubauer. "Best Practices in Security Sector Reform: EU Efforts to Change Ukraine's Public Order Policing." *Journal of Intervention and Statebuilding* 19, no. 3 (2025): 370-391.

Gojali, Djoni Sumardi. "Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective." *International Journal of Cyber Criminology* 17, no. 1 (2023): 1-11.

Hamdhani, Ali Fikri, and Fajrianto Fajrianto. "Relevansi Penerapan Metode Omnibus Law dalam Sistem Peraturan Perundang-Undangan di Indonesia." *Jurnal Al Azhar Indonesia Seri Ilmu Sosial* 5, no. 1 (2024): 31-40.

Hammar, Roberth Kurniawan Ruslak. "Common law approaches to addressing cybercrime and adolescent bullying in Indonesia: Focusing on accountability and protection in the digital age." *International Journal of Cyber Criminology* 16, no. 2 (2022): 162-174.

Hutchinson, Terry, and Nigel Duncan. "Defining and describing what we do: doctrinal legal research." *Deakin law review* 17, no. 1 (2012): 83-119.

Ibrahim, Dicky Malik, Yusuf Hidayat, and Fokky Fuad Wasitaatmadja. "Legal Protection of Banking Customers Who Are Victims of Information and Electronic Transaction Crimes." *Jurnal Ilmiah Penegakan Hukum* 11, no. 1 (2024): 102-120.

Imran, Mohammad Fadil. "Cyber criminology: An analysis of the Indonesian and the United States police perception." *International Journal of Cyber Criminology* 17, no. 2 (2023): 250-261.

Kraemer-Mbula, Erika, Puay Tang, and Howard Rush. "The cybercrime ecosystem: Online innovation in the shadows?." *Technological Forecasting and Social Change* 80, no. 3 (2013): 541-555.

Leukfeldt, Eric Rutger, and Thomas J. Holt. "Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals." *Computers in Human Behavior* 126, no. 8 (2022): 106961-106984.

Malina, Maxim. "The use of artificial intelligence in the administration of criminal justice: problems and prospects." *Gosudarstvo i pravo* 1, no. 4 (2022): 91-97.

Manthovani, Reda. "Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law." *International Journal of Criminal Justice Sciences* 18, no. 1 (2023): 439-452.

Manullang, Sardjana Orba. "The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws." *Society* 10, no. 2 (2022): 489-502.

Mauladi, Kemal Farouq, I. Made Laut Mertha Jaya, and Miguel Angel Esquivias. "Exploring the link between cashless society and cybercrime in Indonesia." *Journal of Telecommunications and the Digital Economy* 10, no. 3 (2022): 58-76.

Muryanto, Yudho Taruno. "The urgency of sharia compliance regulations for Islamic Fintechs: a comparative study of Indonesia, Malaysia and the United Kingdom." *Journal of Financial Crime* 30, no. 5 (2023): 1264-1278.

Nadriana, Lenny, and Pandji Sukmana. "Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges." *International Journal of Cyber Criminology* 16, no. 2 (2022): 192-204.

Newman, Graeme R. "Cybercrime." In *Handbook on crime and deviance*, pp. 551-584. New York: Springer New York, 2009.

Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape." *Ieee Access* 9, no. 3 (2021): 163965-163986.

Octora, Rahel, Demson Tiopan, Shelly Kurniawan, Hassanain Haykal, P. Lindawaty S. Sewu, Christian Andersen, and Yohanes Hermanto Sirait. "The Urgency of the Indonesian Non-Penal Policy in Regulating Misuse of Bank Accounts as a Means of Online Frauds." *Croatian International Relations Review* 28, no. 90 (2022): 135-153.

Otoritas Jasa Keuangan. "Bijak Ber-eBanking". *OJK*, October 22, 2015. https://www.ojk.go.id/id/kanal/perbankan/berita-dan-kegiatan/info-terkini/Documents/Pages/Buku-eBanking/.

Pemerintah Pusat Indonesia. "Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik". *Database Peraturan*, January 2, 2024. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024.

Pemerintah Pusat Indonesia. "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi". *Database Peraturan*, October 17, 2022. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

Peter, M.M. *Penelitian Hukum*. Jakarta: Kencana, 2009.

Prasetyo, Dossy Iskandar, and M. Sholehuddin. "Ratio Legis of Cybercrime Legislation Policy in Indonesia." *International Journal of Cyber Criminology* 18, no. 2 (2024): 57-70.

Pusiknas Bareskrim Polri. "Kasus Kejahatan Manipulasi Data secara ITE Meningkat". *Pusiknas Bareskrim Polri*, June 16, 2025. https://pusiknas.polri.go.id/detail_artikel/kasus_kejahatan_manipulasi_data_secara_ite_meningkat.

Rahardiansah, Trubus. "Sociological Analysis of Fintech Law Enforcement in the Digital Era." *Revista de Gestao Social e Ambiental* 18, no. 2 (2024): 591-723.

Rahmat, Romi Fadillah, Sharfina Faza, Silmi Adnan, Dina Tya Erawati Situmorang, Dani Gunawan, and Tifani Zata Lini. "News articles classification for electronic information and transaction law in indonesia using support vector machine." In *2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA)*, pp. 106-110. New Jersey: IEEE, 2021.

Rifai, Eddy, and H. S. Tisnanta. "Role of law enforcement to prevent cyber laundering and asset recovery from overseas." *International Journal of Cyber Criminology* 16, no. 1 (2022): 110-122.

Sari, Ratih Mega Puspa. "Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia." *Jurnal Hukum dan Keadilan* 2, no. 5 (2025): 49-55.

Shiner, Roger A. "Theorizing criminal law reform." *Criminal Law and Philosophy* 3, no. 2 (2009): 167-186.

Sibawaihi, Muhammad, Devika Rosa Guspita, and Badriyah Badriyah. "Islamic Legal Strategies in Indonesian Contexts to Combat Cybercrime and the Spread of Illegal Data Dissemination." *Justicia Islamica* 21, no. 2 (2024): 357-376.

Soekanto, S. *Pengantar Penelitian Hukum*. Depok: Universitas Indonesia, 1981.

Sogenbits, Thea, and Umut Turksen. "Cracking the code: Unveiling carding crime through the darknet-acquired criminal carding manual and the business model canvas." *Journal of Economic Criminology* 5, no. 5 (2024): 100069-100083.

Soudijn, Melvin RJ, and Birgit CH T. Zegers. "Cybercrime and virtual offender convergence settings." *Trends in organized crime* 15, no. 2 (2012): 111-129.

Suhendi, Dadang, and Erwin Asmadi. "Cyber laws related to prevention of theft of information related to acquisition of land and infrastructure resources in Indonesia." *International Journal of Cyber Criminology* 15, no. 2 (2022): 135-143.

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): 2439539-2439552.

Syaufi, Ahmad, Aurora Fatimatuz Zahra, and Fatham Mubina Iksir Gholi. "Employing forensic techniques in proving and prosecuting cross-border cyber-financial crimes." *International Journal of Cyber Criminology* 17, no. 1 (2023): 85-101.

Tambunan, Unzur Jefri, Puguh Aji Hari Setiawan, and Dewi Iryani. "Penegakan Hukum Tindak Pidana Carding Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Pembangunan Hukum Tindak Pidana Siber (Cybernetics)." *Jurnal Gagasan Hukum* 6, no. 02 (2024): 140-153.

Tuzet, Giovanni. "Certainty Beyond a Reasonable Doubt: A Pragmatist Understanding of the Criminal Standard of Proof." *Contemporary Pragmatism* 20, no. 4 (2023): 398-423.

Webber, Craig, and Michael Yip. "Humanizing the cybercriminal: Markets, forums, and the carding subculture." In *The human factor of cybercrime*, pp. 258-285. Oxfordshire: Routledge, 2019.

Yip, Michael, Craig Webber, and Nigel Shadbolt. "Trust among cybercriminals? Carding forums, uncertainty and implications for policing." In *Policing cybercrime*, pp. 108-131. Oxfordshire: Routledge, 2017.

Yuwono, Finda Pratiwi. "Legal Implications of the Merauke Food Estate: A Critical Analysis of Customary Rights and Environmental Concerns." *Lex Publica* 11, no. 2 (2024): 294-316.