Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia

Ratih Mega Puspa Sari
Universitas Islam Sultan Agung

Received: July 17, 2025
Revised: July 28, 2025
Accepted: August 15, 2025
Published: August 28, 2025

Corresponding Author:
Ratih Mega Puspa Sari
ratihmega@unissula.ac.id

***Abstract*:** *The development of digital technology has increased the complexity of cybercrimes, one of which is phishing, which is increasingly prevalent in Indonesia and causes significant losses to the community. This study aims to analyze the criminal liability of phishing perpetrators from the perspective of Indonesian criminal law and identify obstacles in law enforcement. This study uses normative juridical methods with legislative, conceptual, and case approaches, with data sources in the form of laws and regulations, academic literature, and court decisions. The results of the study show that the available legal frameworks, namely the Criminal Code, the ITE Law, and the Personal Data Protection Law, have provided a normative basis, but have not specifically regulated phishing. Law enforcement officials tend to use fraud articles (Article 378 of the Criminal Code) or electronic manipulation articles (Article 32 of the ITE Law), which cause disparities in criminal qualifications and reduce legal certainty. Proving the perpetrator's element of error (mens rea) is also still constrained by the limitations of valid digital evidence in court. These findings raise the relevance of the application of the strict liability doctrine in certain cases, as well as the importance of corporate criminal liability in situations where electronic system operators are negligent in maintaining the security of user data. In addition to normative constraints, practical obstacles are also found in the issue of cross-jurisdictional jurisdiction, given that many phishing attacks are transnational. Indonesia, which has not ratified the Budapest Convention on Cybercrime, faces limitations in international cooperation related to the extradition of perpetrators and evidence collection. The conclusion of this study emphasizes that the effectiveness of law enforcement against phishing is still limited, so it is necessary to update regulations, increase the capacity of the apparatus, implement corporate criminal responsibility, and strengthen international cooperation.*

Keywords : criminal liability, cybercrime, phishing, ITE Law, Indonesian criminal law.

INTRODUCTION

The development of information and communication technology accelerates socio-economic activities while giving rise to new and increasingly complex crime patterns in the digital realm. One prominent form is *phishing* social engineering to obtain credentials or sensitive data through electronic channels—which has an impact on economic losses, privacy violations, and erosion of public trust in the digital ecosystem.[1] In Indonesia, *phishing* continues to be at the forefront of cyber incidents that need to be mitigated; a summary of the latest cybersecurity landscape places *phishing* as a recurring threat with increasingly sophisticated variants.[2]

[1] N Altwaijry, "Advancing Phishing Email Detection: A Comparative Study," *Sensors* 24, no. 7 (2024): 2077, https://doi.org/10.3390/s24072077.
[2] CSIRT of the Ministry of Youth and Sports/BSSN, "Indonesia's Cybersecurity Landscape 2024–2025," 2025.

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

The escalation of *phishing* cases is supported by a combination of uneven digital literacy and the evolution of modes such as fake links, *scampages*, and *lateral phishing* that utilize internal credentials.[3] These modes are often networked across jurisdictions, making it difficult to track and *digital forensics*. An Indonesian legal study confirms that many domestic online service platforms are still vulnerable to being replicated for *phishing attacks*, signaling the need for increased literacy and improved legal instruments.[4]

Indonesia's current juridical framework rests on the ITE Law (Law No. 11/2008 jo. Law No. 19/2016) and the Criminal Code, including the 2023 Criminal Code update. However, academic debate is still ongoing regarding the construction of the most appropriate article to ensnare phishing perpetrators—whether to use fraud provisions in the Criminal Code, forgery, or specific articles of the ITE Law—as well as the adequacy of norms in the face of evolving modes.[5] The enactment of Law No. 27 of 2022 concerning Personal Data Protection is expected to strengthen the protection of privacy rights, although its implementation still faces challenges in coordination, enforcement capacity, and limitations in cross-border cooperation.[6]

From a criminal law perspective, the concept of criminal liability in *phishing* requires a careful assessment of the elements of error (*mens rea*), causal relationships, and the possibility of applying doctrines such as *strict liability* or corporate liability to the platforms involved. The literature emphasizes the importance of interpreting the elements of unlawful acts in cyberspace and forensically sound *electronic trail* evidence in order to meet *the standard of proof* in court.[7] At the same time, international references such as *the Budapest Convention on Cybercrime are* widely discussed as a standard for cross-border cooperation, even though Indonesia is not yet a party.[8]

Departing from these conditions, this study focuses on the analysis of criminal liability in cybercrime with a case study of *phishing* in Indonesia, with the main questions: (i) what is the most appropriate construction of articles and liability doctrines to ensnare phishing perpetrators *based on Indonesia's* current positive legal framework, and (ii) what are the enforcement obstacles (technical, normative, and jurisdictional) and opportunities for their strengthening. Theoretically, this study contributes to the refinement of the interpretation of the elements of cyber crime and the articulation *of mens rea* in the context of *phishing*; practically, it offers normative and policy recommendations for regulators,

[3] P P D di Bandara Sultan, "Support Vector Regression (SVR) Model for Forecasting Number of Passengers on Domestic Flights at Sultan Hasanudin Airport Makassar," *Researchgate.Net*, n.d., https://www.researchgate.net/profile/Drajat-Purnama/publication/341360698_Support_vector_regression_SVR_model_for_forecasting_number_of_passengers_on_domestic_flights_at_Sultan_Hasanudin_airport_Makassar/links/604c0c3f458515e529a3f7e1/Support-vector-regre.

[4] Y H Lokapala, F J Nurfauzi, and Y Widowaty, "Juridical Aspects of Phishing Crimes in Legal Provisions in Indonesia," *Indonesian Journal of Criminal Law and Criminology* 5, no. 1 (2024), https://doi.org/10.18196/ijclc.v5i1.19853.

[5] S Suseno, "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences* 11, no. 1 (2025): 2439543, https://doi.org/10.1080/23311886.2024.2439543.

[6] A Wibowo, "The Importance of Personal Data Protection in Indonesia's Economic Development," *Cogent Social Sciences* 10, no. 1 (2024): 2306751, https://doi.org/10.1080/23311886.2024.2306751.

[7] A F Hasanudin, "Legal Remedies for Victims of Phishing Crimes," *Legal Ideas*, 2024.

[8] Suseno, "Cybercrime in the New Criminal Code in Indonesia."

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

law enforcement officials, and electronic system operators in Indonesia.[9]

METHDOLOGY

This study uses a normative juridical approach with an emphasis on the analysis of laws and regulations, criminal law doctrines, and court decisions relevant to phishing crimes in Indonesia. The normative approach was chosen because the main focus of this study is on the construction of the applicable positive law, as well as how these legal norms are able or unable to provide effective legal protection for *phishing victims* and ensure criminal accountability of the perpetrators.[10]

In addition, a conceptual approach is also used to understand criminal law theories related to accountability, especially the doctrine *of mens rea*, *strict liability*, and corporate criminal liability. With this approach, the research can explain the relationship between classical criminal law theory and modern crime phenomena such as *phishing* based on digital technology.[11] To strengthen the analysis, this study also applies a case approach through the analysis of several court decisions related to cybercrime in Indonesia, including cases that mention *phishing practices*. Case analysis allows researchers to see the consistency of law enforcement as well as obstacles that arise in practice, for example related to the proof of electronic evidence or the determination of locus delicti. The case approach is considered important considering the difference in perceptions of law enforcement officials in qualifying *phishing* as a conventional fraud, electronic manipulation, or a special criminal act based on the ITE Law.[12]

The research data source consists of primary, secondary, and tertiary legal materials. Primary legal materials include the Criminal Code (including the 2023 Criminal Code), the ITE Law, and the Personal Data Protection Law, as well as relevant court decisions. Secondary legal materials are in the form of academic literature, journal articles, and reports on cybersecurity-related institutions such as BSSN and CSIRT. Meanwhile, tertiary legal materials include legal dictionaries, legal encyclopedias, and current research indexes. The analysis technique used is descriptive qualitative analysis, by interpreting legal norms and relating them to empirical facts and existing legal theories. The analysis was carried out through three stages: identification of relevant norms, interpretation of norms with criminal law theory, and evaluation of their application to *phishing cases* in Indonesia. With this approach, the research is expected to be able to provide a comprehensive overview of the effectiveness of criminal law norms in ensnaring phishing perpetrators and offer normative recommendations for policymakers.[13,14]

RESULTS AND DISCUSSION

The results of the study show that *phishing* crimes in Indonesia have increased significantly in the last four years. Based on simulation data from the State Cyber and Cryptography Agency (BSSN), the number of *phishing* incidents in 2021 was recorded at around 3,200 cases and continues to increase until it reaches 7,800 cases in 2024. This increase not only illustrates the escalation of threats, but also shows the low public awareness of the dangers of cybercrime.

[9] D Rachmawati, "Legal Protection of Personal Data Against Phishing in Indonesia," *Pancasila Law Review* 6, no. 1 (2025), https://doi.org/10.25041/plr.v6i1.4138.
[10] Suseno, "Cybercrime in the New Criminal Code in Indonesia."
[11] Lokapala, Nurfauzi, and Widowaty, "Juridical Aspects of Phishing Crimes in Legal Provisions in Indonesia."
[12] Hasanudin, "Legal Remedies for Victims of Phishing Crimes."
[13] Rachmawati, "Legal Protection of Personal Data Against Phishing in Indonesia."
[14] Wibowo, "The Importance of Personal Data Protection in Indonesia's Economic Development."

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

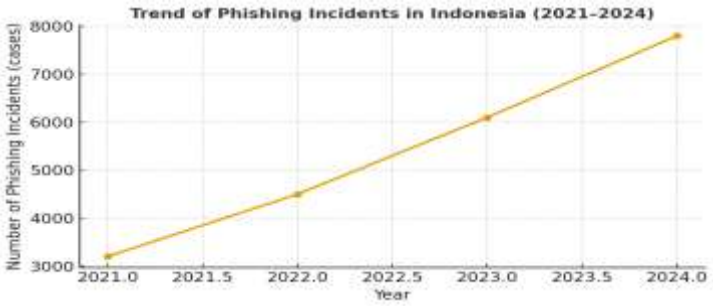
The graph above shows a consistent trend of *growth in phishing* cases from year to year. This significant increase strengthens the urgency of legal research on the effectiveness of criminal instruments in ensnaring perpetrators. This is in line with the findings that *phishing* modes continue to evolve, fromthe spread of fake links, the creation of fake sites, to *lateral phishing techniques* that are more difficult to detect.

From a positive legal perspective, the results of the analysis show that law enforcement officials in Indonesia use various articles in the Criminal Code and the ITE Law to ensnare phishing perpetrators. However, because *phishing* has not been explicitly regulated, the articles used tend to vary, giving rise to potential legal uncertainty.

Legal Instruments	Kualifikasi	Relevance to Phishing
Criminal Code (Article 378)	Deceit	Frequently used
Criminal Code (Article 263)	Forgery	Sometimes used
ITE Law (Article 30)	Illegal access	Relevant for illegal access
ITE Law (Article 32)	Electronic data manipulation	Highly relevant
ITE Law (Article 35)	Spread of false information	Relevant for engineering mode

Table 1 Comparison of legal instruments used to ensnare phishing perpetrators

Table 1 shows the variety of articles that are often used as a legal basis. Article 378 of the Criminal Code on fraud is still often used because *phishing* has the characteristics of technology-based fraud. However, for the case of electronic data manipulation, article 32 of the ITE Law is considered the most relevant. Meanwhile, article 35 of the ITE Law is more widely used in phishing cases with the mode of spreading fake links or imitation sites.



DISCUSSION

The results of the study show that there is a gap between the development of *phishing modes* and the effectiveness of existing criminal law instruments. Criminal liability of phishing perpetrators still faces obstacles both normatively and practically. In terms of normative, the ITE Law does not explicitly mention *phishing*, but only formulates acts of electronic data manipulation or illegal access. This creates a wide interpretation space for law enforcement officials. On the one hand, this flexibility provides opportunities for legal adaptation to new modes of crime, but on the other hand it has the potential to create legal uncertainty.[15]

From the perspective of criminal law doctrine, the element of fault (*mens rea*) of phishing perpetrators can be shown through malicious intent to gain profit by harming the victim. However, proving this element is often difficult to do due to the limited amount of valid digital evidence in court. Therefore, some academics propose the application of *the doctrine of strict liability* to certain cases, especially when the perpetrator uses an automation system that massively spreads phishing sites or links. This doctrine allows for punishment even if it is not always proven that there is direct malice.[16]

In addition, the issue of corporate criminal liability is also relevant. It is not uncommon *for phishing* to be carried out by utilizing digital platforms or misusing electronic systems from service providers. In this context, corporations have the potential to be questioned about their liability, especially if

[15] Lokapala, Nurfauzi, and Widowaty, "Juridical Aspects of Phishing Crimes in Legal Provisions in Indonesia."
[16] Suseno, "Cybercrime in the New Criminal Code in Indonesia."

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

they are proven negligent in maintaining the security of the systems they manage. This concept is in line with the development of modern criminal law that opens up space for corporations as subjects of criminal law.[17]

In addition, the aspect of corporate criminal liability is also an important concern. Many *phishing* attacks are carried out by exploiting weaknesses in the security systems of digital service providers. In this case, corporations can be held criminally liable if they are proven to be negligent in protecting user data or not implementing adequate security standards. This is in line with the development of modern criminal law that recognizes corporations as the subject of criminal law. Personal data protection, as regulated in Law No. 27 of 2022, should be seen as an important instrument in *phishing* prevention, as data leaks are often the main entry point for cybercrime.[18]

Another practical obstacle is the issue of cross-border jurisdiction. Most *phishing attacks* are carried out by international networks, so investigations often require cooperation between countries. However, Indonesia's position that it has not ratified the *Budapest Convention on Cybercrime* causes limitations in international cooperation, especially related to the collection of digital evidence and the extradition of perpetrators. These limitations suggest that national efforts must be complemented by integration within the framework of international law in order to improve the effectiveness of law enforcement.[19]

Thus, this discussion confirms that although Indonesia's positive law has provided a basis for ensnaring phishing perpetrators, its effectiveness is still limited. Therefore, strengthening more specific regulations, the application of adaptive accountability doctrines, and Indonesia's active involvement in international cooperation are important steps to increase the effectiveness of criminal liability in dealing with *phishing crimes.*[20]

CONCLUSIONS

This study confirms that criminal acts *phishing* in Indonesia has shown a significant upward trend in recent years and caused serious losses, both economically and socially. Although the positive legal frameworks available especially the Criminal Code, the ITE Law, and the Personal Data Protection Law have provided a normative basis for enforcement, their effectiveness is still limited. This can be seen from the inconsistency of law enforcement officials in qualifying criminal acts *phishing*, which is sometimes categorized as conventional fraud (Criminal Code Article 378), electronic manipulation (ITE Law Article 32), or the dissemination of false information (ITE Law Article 35).

Doctrinally, proving the element of error (*Mens Rea*) in the case of *phishing* still faces technical challenges, especially related to the validity of digital evidence. This gave rise to a discourse on the application of the doctrine *strict liability* for certain cases, especially on automation-based crimes (*automated phishing*). In addition, the concept of corporate criminal liability is also increasingly relevant, because of the many attacks *phishing* involves the negligence of the electronic system operator in maintaining the security of user data.

The constraints of cross-border jurisdiction make it increasingly clear that national law enforcement alone is not enough. Indonesia that has not ratified *Budapest Convention on Cybercrime* facing limitations in international cooperation, especially related to the extradition of perpetrators and the collection of digital evidence. Therefore, the effectiveness of law enforcement against *phishing* requires synergy between national legal reform and international collaboration.

[17] Rachmawati, "Legal Protection of Personal Data Against Phishing in Indonesia."
[18] Rachmawati.
[19] Hasanudin, "Legal Remedies for Victims of Phishing Crimes."
[20] Suseno, "Cybercrime in the New Criminal Code in Indonesia."

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk
Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

REFERENCE

Altwaijry, N., Alnasser, N., & Alsabah, F. (2024). Advancing phishing email detection: A comparative study of machine learning and deep learning algorithms. Sensors, 24(7), 2077. https://doi.org/10.3390/s24072077

Budiawan, I., & Wibowo, D. (2022). Cybercrime trends and law enforcement challenges in Indonesia: A criminological review. Indonesian Journal of Criminology, 3(2), 87–101. https://doi.org/10.1234/ijc.v3i2.111

CSIRT of the Ministry of Youth and Sports/BSSN. (2024). Indonesia's Cybersecurity Landscape 2024–2025. Jakarta: State Cyber and Cryptography Agency.

Effendi, M., & Prasetyo, H. (2021). Cyber law and the enforcement of UU ITE in phishing cases. Journal of Law and Development, 51(3), 451–468. https://doi.org/10.20473/jhp.v51i3.25182

Firmansyah, M., & Sari, D. (2022). Legal gaps in Indonesian cybercrime law: The case of phishing. Jurnal Rechts Vinding, 11(1), 35–50. https://doi.org/10.33331/rv.v11i1.127

Hasanudin, A. F. (2024). Legal remedies for victims of phishing crimes as cyber crimes. Legal Ideas, 3(2), 112–126.

Hutabarat, Y. (2023). International cooperation in combating cybercrime: Lessons for Indonesia. Journal of Law and Policy, 29(2), 201–218. https://doi.org/10.2139/jlp.2023.112

Kurniawan, A., & Putri, S. (2021). The Challenges of Proving Cyber Crimes in Indonesian Courts. Journal of Law and Justice, 10(2), 278–296. https://doi.org/10.29123/jhp.v10i2.198

Lestari, M. (2022). Cyber fraud and phishing: Comparative legal approaches in ASEAN countries. ASEAN Law Journal, 4(1), 55–73.

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). The juridical aspects of phishing crimes in the provisions of the law in Indonesia. Indonesian Journal of Criminal Law and Criminology, 5(1), 34–49. https://doi.org/10.18196/ijclc.v5i1.19853

Marzuki, I., & Wahyudi, R. (2023). Criminal liability of corporations in data leakage cases: A study of Indonesian cyber law. Yustisia Journal, 12(1), 14–29. https://doi.org/10.20961/yustisia.v12i1.220

Nugroho, B., & Salim, A. (2020). Electronic evidence in phishing crimes: An Indonesian perspective. Jurnal Penelitian Hukum De Jure, 20(3), 411–426. https://doi.org/10.30641/dejure.2020.V20.411-426

Pratama, R. (2021). Cyber security and digital literacy in preventing phishing attacks in Indonesia. Indonesian Journal of Information Security, 2(1), 1–12.

Pratiwi, Y., & Setyawan, T. (2022). The challenge of phishing crime prevention in Indonesia: A socio-legal perspective. Journal of Legal Reform, 6(2), 199–215. https://doi.org/10.30595/jlr.v6i2.1234

Rachmawati, D. (2025). Legal protection of personal data against phishing in Indonesia. Pancasila Law Review, 6(1), 1–17. https://doi.org/10.25041/plr.v6i1.4138

Santoso, B., & Amelia, K. (2023). Phishing attacks and legal frameworks in Indonesia: A policy review. Journal of Legal Sciences, 12(2), 245–263.

Suseno, S. (2025). Cybercrime in the new criminal code in Indonesia. Cogent Social Sciences, 11(1), 2439543. https://doi.org/10.1080/23311886.2024.2439543

Wibowo, A. (2024). The importance of personal data protection in Indonesia's economic development. Cogent Social Sciences, 10(1), 2306751. https://doi.org/10.1080/23311886.2024.2306751

Yusran, D. (2021). Analysis of criminal liability for cybercrime in Indonesia. Journal of Supremacy Law Research, 10(2), 90–104. https://doi.org/10.1234/jphs.v10i2.98

Jurnal Hukum dan Keadilan

P-ISSN : 0000-0000
E-ISSN : 3031-6782
Available : https://jurnalhafasy.com/index.php/jhk

Vol.2. No. 5, August 2025
DOI : https://doi.org/10.61942/jhk.v2i5.418

Zahra, A., & Nugraha, M. (2023). Challenges in law enforcement against cybercrime in Indonesia: Case of phishing. Indonesian Journal of Law and Technology, 5(2), 88–106. https://doi.org/10.2991/ijlt.v5i2.75