International Journal of Law and Society

E-ISSN: 3046-9562
P-ISSN: 3046-9619

Research Article

Criminal Liability for Phishing Perpetrators: A Normative Analysis of Indonesian Criminal Law

Prasetyo Wisnu Langgono[1*], Hartoyo[2], Fitri Ayuningtyas[3]

[1-2] Faculty of Law, Universitas Dr. Soetomo, Indonesia
* Corresponding Author: e-mail: prasetyowisnulanggono@gmail.com

Abstract: Phishing constitutes a form of cybercrime that continues to proliferate alongside the rapid advancement of information technology, causing significant impacts on data security and financial losses. This study aims to analyse the forms of criminal liability applicable to phishing perpetrators under Indonesian criminal law and to identify the challenges and solutions in its enforcement. The research employs a normative juridical approach utilising literature review methodology. The findings demonstrate that criminal liability for phishing perpetrators can be established through provisions in the Electronic Information and Transactions Law (ITE Law) as amended by Law Number 1 of 2024, the Indonesian Penal Code (KUHP), and related regulations. However, law enforcement faces numerous obstacles, including inadequate specific legal regulations, limited digital forensic technology, low public legal literacy, and cross-border jurisdictional barriers. In judicial proceedings, evidentiary processes are frequently hindered by the complexity of electronic evidence and the limited technical understanding among law enforcement officers. This study recommends regulatory reform, capacity building for human resources, international cooperation, and public education to strengthen the effectiveness of law enforcement against phishing crimes.

Keywords: Criminal Liability; Cybercrime; Evidence; Indonesian Law; Phishing

1. Introduction

The rapid development of information and communication technology has brought significant impacts across various aspects of human life. On one hand, this advancement provides convenience in interaction, transaction, and efficient access to information. However, on the other hand, technological progress has also created opportunities for the emergence of increasingly complex and difficult-to-detect forms of cybercrime. One prevalent form of cybercrime is phishing, which constitutes fraudulent conduct performed by deceiving victims into providing personal or confidential information through electronic media such as email, fake websites, or social media (Gulo et al., 2021).

Phishing represents a form of crime that exploits social engineering techniques to obtain sensitive data from victims, including usernames, passwords, identification numbers, and financial information (Wiranata et al., 2024). Data illegally obtained through such methods is subsequently used for criminal purposes, including identity theft, credit card fraud, or other financial crimes. The modus operandi of phishing is highly diverse, ranging from sending emails resembling official correspondence from financial institutions, creating fraudulent websites mimicking legitimate sites, to distributing text messages directing victims to malicious links. This phenomenon demonstrates that phishing is not merely a technological crime but also involves complex psychological and social dimensions.

In Indonesia, phishing offences have not been specifically regulated in legislation. However, phishing perpetrators can be prosecuted under provisions in the Indonesian Penal Code (KUHP), specifically Article 378 concerning fraud and Article 372 concerning embezzlement. Additionally, Law Number 11 of 2008 concerning Electronic Information

Received: July 28, 2025;
Revised: September 22, 2025;
Accepted: November 17, 2025;
Published: January 12, 2026;
Curr. Ver.: January 12, 2026

and Transactions (ITE Law), as amended by Law Number 1 of 2024, can also serve as a legal basis for prosecuting phishing perpetrators, particularly Article 28 paragraph (1) and Article 45 paragraph (1). Nevertheless, law enforcement against phishing crimes continues to face various challenges (Basthian & Sinaga, n.d.).

One of the primary challenges in law enforcement against phishing is the difficulty in identifying perpetrators who frequently use false identities and operate anonymously in cyberspace. Furthermore, the lack of coordination among law enforcement agencies and low public awareness in reporting phishing cases also constitute obstacles in the enforcement process. In several cases, phishing perpetrators receive relatively lenient sentences disproportionate to the losses suffered by victims. This research aims to analyse the legal aspects of criminal liability for phishing perpetrators according to the Indonesian criminal law system, as well as to identify challenges and solutions in its enforcement.

2. Literature Review

Definition and characteristics of Phishing Crimes

The development of information technology has brought significant impacts across various aspects of life, including the emergence of new forms of crime that exploit technology. Phishing constitutes a form of cybercrime conducted by deceiving victims into providing personal or confidential information through electronic media. Information illegally obtained is subsequently used for criminal purposes such as identity theft, credit card fraud, or other financial crimes (Tabrani et al., 2024). According to Putra (2021), phishing is an act of deception performed by misleading targets with the intent to steal accounts by disseminating broadcasts, often through fake emails containing false information directing victims to fraudulent websites resembling legitimate sites.

The primary characteristics of phishing crimes include: utilisation of social engineering techniques to deceive victims; exploitation of electronic media such as email, fake websites, or social media; economic motivation as the primary objective; and difficulty in law enforcement due to anonymous and cross-border operations. Phishing can manifest in various forms, including email phishing, spear phishing, vishing (voice phishing), and smishing (SMS phishing). Email phishing represents the most common form where perpetrators send fake emails resembling official institutions to deceive victims.

Legal Framework for Phishing Crimes in Indonesia

In Indonesia, phishing crimes do not have specific regulations in legislation. However, perpetrators can be prosecuted under provisions in the Indonesian Penal Code (KUHP), specifically Article 378 concerning fraud and Article 372 concerning embezzlement. Additionally, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law Number 1 of 2024, can serve as a legal basis for prosecuting phishing perpetrators, particularly Article 28 paragraph (1) and Article 45 paragraph (1) (Lokapala et al., 2024). The absence of specific legal regulations concerning phishing in Indonesian legislation creates a legal vacuum that can impede law enforcement processes.

Principles of Criminal Liability

Criminal liability constitutes a legal mechanism for imposing consequences in the form of sanctions upon perpetrators who commit unlawful acts. In the Indonesian criminal law system, criminal liability can only be imposed upon someone who commits an unlawful act with fault and without justification or excuse. Several fundamental principles governing criminal liability include: the legality principle (nullum delictum nulla poena sine praevia lege), the culpability principle, the personal liability principle, and the proportionality principle. These principles serve as the foundation for determining whether a person can be held criminally liable for their conduct.

3. Research Methods

This research employs a normative juridical approach utilising secondary legal sources as primary data. The normative legal approach emphasises written legal materials, including legislation, doctrine, and expert opinions. In this research, the author analyses legal provisions governing phishing crimes and existing solutions in law enforcement against such crimes in Indonesia.

Primary legal materials include the Indonesian Penal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 27 of 2022 concerning Personal Data Protection. Secondary legal materials comprise literature, including books, scientific journals,

legal articles, and expert opinions relevant to criminal liability for phishing perpetrators. Tertiary legal materials include legal dictionaries and legal encyclopedias.

The collected data is analysed qualitatively using descriptive analysis methods. The author identifies and examines applicable legal provisions concerning phishing crimes, challenges encountered in law enforcement, and implementable solutions to enhance the effectiveness of law enforcement against phishing in Indonesia.

4. Results and Discussion

Forms of Criminal Liability for Phishing Perpetrators Under Indonesian Criminal Law

The development of information and communication technology has brought numerous benefits to society, including facilitating information access, financial transactions, and social interaction. However, this development also poses serious challenges in the form of cybercrime. One increasingly prevalent form of cybercrime is phishing. Phishing constitutes a form of fraud conducted using electronic media, particularly the internet, to illegally obtain personal data or victim information such as passwords, account numbers, or credit card data for personal gain.

In Indonesia, crimes such as phishing have caused substantial losses, both material and immaterial. Nevertheless, the regulation and law enforcement against these crimes still face various challenges. The primary legal instrument for prosecuting phishing perpetrators in Indonesia is Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024. In this Law, several relevant provisions for prosecuting phishing perpetrators include Article 28, paragraph 1, concerning the dissemination of false and misleading information, Article 35, concerning manipulation of electronic information, and Article 36 concerning acts causing losses to others.

For these offences, perpetrators may be subject to criminal sanctions as provided in Article 45A and Article 51 of the ITE Law. Criminal penalties for perpetrators can reach 12 years imprisonment and fines of billions of rupiah, depending on the applicable provision. Additionally, phishing perpetrators can also be prosecuted under provisions in the KUHP, specifically Article 378 concerning fraud and Article 362 concerning theft. Thus, positive Indonesian law has recognised and provided legal instruments for prosecuting phishing perpetrators, although the term phishing is not explicitly mentioned in its formulation.

The most common form of criminal liability in phishing crimes is individual criminal liability. In this context, perpetrators bear full responsibility for actions they personally undertake or jointly commit with other perpetrators in the form of participation. Forms of participation such as joint participation (deelneming), instigating, or assisting in committing criminal acts can also be imposed as regulated in Articles 55 and 56 of the KUHP. Additionally, corporate criminal liability can be applied when phishing is conducted in the interest of a particular organisation. The Indonesian criminal law system has recognised corporate criminal liability as regulated in certain legislation.

Challenges and Solutions in Law Enforcement Against Phishing Crimes

Law enforcement against phishing crimes faces various challenges that are quite complex. Juridical challenges include the suboptimal specific regulations governing phishing, inconsistency between KUHP provisions and ITE Law, and overlapping authority among agencies handling cybercrime. On the technical side, challenges include limited human resources expertise in digital forensics, limited supporting equipment for cyber investigation, and the rapid technological development exploited by perpetrators.

Sociologically, low digital literacy among the public, an underdeveloped legal culture, and minimal awareness of reporting constitute serious obstacles. Internationally, limited jurisdiction, minimal inter-state cooperation, and Indonesia's non-membership in global conventions such as the Budapest Convention further complicate cross-border phishing eradication. In courts, evidentiary challenges also pose significant obstacles, ranging from the validity of electronic evidence, difficulty in proving perpetrator intent, to judges' limited understanding of digital technical aspects.

To address these challenges, several solutions can be implemented. First, regulatory reform and harmonisation related to cybercrime, including clarifying forms of criminal liability for individuals and corporations. Second, strengthening the capacity of law enforcement officers and digital forensic infrastructure through intensive training on cyber law, digital evidence, and phishing investigation techniques. Third, enhancing digital literacy and public legal awareness through massive and sustainable public education programs.

Fourth, developing more active and effective international cooperation, including Indonesia's accession to the Budapest Convention on Cybercrime. Fifth, reforming evidentiary procedures and developing cyber courtroom facilities.

5. Conclusion

Based on the research findings and discussion, two main conclusions can be drawn. First, phishing crimes constitute cybercrime containing elements of electronic fraud aimed at illegally obtaining personal information, important data, or financial benefits. In the Indonesian criminal law system, forms of criminal liability for phishing perpetrators can be applied through provisions in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), specifically Article 28 paragraph (1) jo. Article 45A paragraph (1), as well as other articles related to forgery, fraud, or illegal access to electronic systems. Additionally, criminal liability can also be imposed upon corporations when phishing is conducted in the interest of a particular organisation.

Second, law enforcement against phishing faces various challenges from juridical, technical, social, and international aspects. Juridical challenges include suboptimal specific regulations governing phishing, inconsistency between KUHP provisions and ITE Law, and overlapping authority among agencies handling cybercrime. Technical challenges include limited human resources expertise in digital forensics, limited supporting equipment for cyber investigation, and rapid technological development exploited by perpetrators. Sociologically, low digital literacy among the public, an underdeveloped legal culture, and minimal awareness of reporting constitute serious obstacles. Internationally, limited jurisdiction, minimal inter-state cooperation, and Indonesia's non-membership in global conventions further complicate cross-border phishing eradication.

This research recommends: regulatory reform and harmonisation related to cybercrime; strengthening the capacity of law enforcement officers and digital forensic infrastructure; enhancing digital literacy and public legal awareness; developing international cooperation, including accession to the Budapest Convention on Cybercrime; and reforming evidentiary procedures and digital judicial systems. A community-based approach through involvement of local communities, community leaders, and non-governmental organisations in prevention efforts will strengthen social control against cybercrime.

Author Contributions: Conceptualisation, P.W.L. and H.; Methodology, P.W.L.; Validation, H. and F.A.; Formal Analysis, P.W.L.; Writing – Original Draft, P.W.L.; Writing – Review & Editing, H. and F.A.; Supervision, H.

Funding: This research received no external funding.

Data Availability Statement: All data generated or analysed during this study are included in this published article

Acknowledgements: The authors would like to express gratitude to the Faculty of Law, Universitas Dr. Soetomo, for support in completing this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

Anjheli, D. (2025). Digital privacy and phishing crimes in Indonesia: Critical evaluation of the effectiveness of ITE law and PDP law. *Staatsrecht: Jurnal Hukum Ketatanegaraan dan Politik Islam, 4*(1), 165–189. https://doi.org/10.14421/990epf27

Arifin, H., & Sabri, M. (2023). Perlindungan hukum terhadap korban kejahatan siber melalui regulasi di Indonesia. *Jurnal Hukum dan Keadilan, 15*(2), 215–227.

Az-Zahra, I., & Labib, Z. M. (2024). Perlindungan hukum bagi nasabah dalam kasus phishing dan siber perbankan di Indonesia. *Yurisprudentia: Jurnal Hukum Ekonomi, 10*(2), 1–15. https://doi.org/10.24952/yurisprudentia.v10i2.13952

Dinda, A. L. S. (2024). Effectiveness of law enforcement against cybercrime in Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum, 2*(2), 69–77. https://doi.org/10.24952/yurisprudentia.v10i2.13952

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber crime in the form of phishing based on the electronic information and transactions law. *PAMPAS: Journal of Criminal Law, 1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Hidayat, N., & Fauzi, F. (2024). Cybercrime dan perlindungan data pribadi dalam perspektif hukum Indonesia. *Jurnal Hukum dan Teknologi, 5*(1), 45–60.

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Juridical aspects of phishing crimes in Indonesian legal provisions. *Indonesian Journal of Criminal Law and Criminology, 5*(1). https://doi.org/10.18196/ijclc.v5i1.19853

Mulyani, R., & Kurniawan, A. (2023). Efektivitas penegakan hukum terhadap cybercrime di Indonesia: Kasus phishing dan pemalsuan data. *Jurnal Kriminologi Indonesia, 8*(3), 123–137.

Priyadi, A., Trisno, A., Banjarnahor, H., & Sugianto, F. (2025). Building digital trust through personal data protection law enforcement. *Syntax Literate: Jurnal Ilmiah Indonesia, 10*(5), 5309–5320. https://doi.org/10.36418/syntax-literate.v10i5.59613

Putra, Y. V. F. (2021). Modus operandi of phishing crimes according to ITE law. *Jurist-Diction, 4*(6), 2525. https://doi.org/10.20473/jd.v4i6.31857

Rangkuti, P. R., Khoiri, M. A., Ritonga, S., Pane, P. N S. (2025). Sanksi pidana terhadap kejahatan phishing menurut hukum pidana Indonesia. *Konstitusi: Jurnal Ilmu Hukum dan HAM*.

Sari, R. M. P. (2025). An analysis of phishing crimes in Indonesia. *Jurnal Hukum Kriminal (JHK), 2*(5). https://doi.org/10.61942/jhk.v2i5.418

Syah, M., & Putra, F. D. (2024). Tinjauan hukum terhadap pelanggaran privasi dan pencurian data pribadi dalam dunia maya di Indonesia. *Jurnal Hukum dan Informasi, 4*(4), 312–325.

Tabrani, S., Safitri, V., Nayla, P. A. P., & Hosnah, A. U. (2024). Phishing crimes viewed from a legal perspective and cybercrime. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan.*

Widyasari, T., & Harahap, S. (2024). Pengaruh undang-undang perlindungan data pribadi terhadap pengendalian kejahatan siber di Indonesia. *Jurnal Cyber Law Indonesia, 6*(1), 89–102.