Criminal Policy of Indonesian Criminal Law in Combating the Crime of Phishing

Shofriya Qonitatin Abidah[1*], *Muhammad* Reza Faturrahman[1], *Nisrina* Khoirunnisa[1], *Sonny* Saptoadji Wicaksono[1] and *Sri* Wulandari[1]

[1]Universitas Negeri Semarang, Semarang, Indonesia

Abstract. Phishing has emerged as one of the fastest-growing forms of cybercrime in Indonesia, yet no legislation explicitly defines it as an independent criminal offense. This study aims to analyze the effectiveness of Indonesia's current legal framework in addressing phishing and to compare it with international practices. Employing a normative juridical approach complemented by empirical juridical insights, data were collected through document analysis of authentic legal sources and case records. The findings reveal that Indonesian law enforcement continues to rely on general provisions of the Penal Code (KUHP) and the Electronic Information and Transactions Law No. 1 of 2024, which leads to suboptimal prosecution and limited protection for victims. In contrast, the United States has adopted comprehensive anti-phishing regulations and integrated enforcement mechanisms that provide stronger safeguards. Using Lawrence M. Friedman's legal system theory, the study concludes that Indonesia's regulatory framework remains ineffective across the dimensions of legal substance, institutional structure, and legal culture. The results underscore the urgency for comprehensive legal reform, including the formulation of specific phishing-related offenses, capacity building for law enforcement, and public awareness initiatives to strengthen resilience against cybercrime in the digital era.
Keywords: Technology; Cybercrime; Phishing; Criminal Policy

1 Introduction

The rapid development of information technology over the past two decades has brought significant changes to human life. Almost all activities—from communication and financial transactions to public services—are now integrated into digital systems. On one hand, this progress offers convenience and efficiency; on the other hand, it gives rise to new challenges that cannot be ignored, one of which is cybercrime. Several common types of cybercrime include: joy computing, which refers to the unauthorized use of someone else's computer; hacking, which involves illegal access to terminals or systems; the trojan horse, where data or software is manipulated by altering instructions in a program; data leakage, the unauthorized disclosure of confidential computer data; data diddling, which is the act of unlawfully modifying legitimate data; and phishing, a form of deception involving fake emails or websites designed to trick users. Phishing itself can be classified into five types:

* Corresponding author: shofriyaabidah@mail.unnes.ac.id

Email Phishing, Spear Phishing, Whaling, Vishing, and Smishing. Phishing is one of the most rapidly growing cybercrimes. It is typically carried out by deceiving victims through emails, fake websites, or other electronic messages, with the goal of stealing personal data such as usernames, passwords, or bank account information. In many cases, victims are unaware that their personal information has been stolen and misused.

Indonesia does have several legal instruments that can be used to prosecute phishing perpetrators, although the term “phishing” is not explicitly mentioned. Generally, phishing activities can be prosecuted under Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). Additionally, phishing can be prosecuted under the Indonesian Criminal Code (KUHP), particularly Article 378 on fraud. According to the IDADX (Indonesia Domain Abuse Data Exchange) report, there were 2,470 phishing reports in the first quarter of 2025. Furthermore, the financial sector was the most targeted, accounting for 50.98% of the incidents. This number represents a significant increase from the 1,365 phishing reports recorded in the first quarter of 2024 [1] . The increase of 1,105 incidents highlights the seriousness of phishing as a cybercrime threat. [2]

From the data above, it is evident that the financial sector is the primary target of phishing attacks. The widespread occurrence of phishing in this sector can have severe consequences for Indonesia’s economy. As one of the 193 member states of the United Nations (UN), Indonesia is committed to achieving the Sustainable Development Goals (SDGs). These global goals aim to improve economic welfare, social quality of life, environmental preservation, and ensure justice and good governance to enhance the quality of life for current and future generations. Comprising 17 primary goals to be achieved by 2030, the SDGs have been adopted by numerous countries, including Indonesia. Through the National Development Planning Agency (Bappenas), Indonesia has aligned its national development priorities with the SDGs’ targets.

The rapid advancement of technology has greatly facilitated access to information, spurred cross-sector innovation, and enabled efficient digital transactions. Technological utilization also serves as a key driver of trade and national economic growth toward achieving societal prosperity. However, the increasing incidents of phishing in Indonesia’s financial sector now result in major economic losses that could hinder efforts to achieve the Sustainable Development Goals (SDGs), particularly those related to inclusive and sustainable economic growth, increasing productive employment, and ensuring decent work for all.

Yazid Haikal Lokapala et al., in their study titled "Legal Aspects of Phishing Crimes in Indonesian Law", stated that there are still significant challenges and obstacles in enforcing the law against phishing in Indonesia, which include the need for involvement from law enforcement and the public [3]. In another study titled "Criminal Sanctions for Phishing Crimes under Indonesian Criminal Law", Putri Ramadhani Rangkuti et al. found that more responsive and adaptive legal reforms to technological advancements are needed to reduce the number of phishing victims in Indonesia [4]. In addition to building on previous research, the present study titled “Criminal Policy in Combating Phishing Crimes Under Indonesian Criminal Law” becomes crucial in identifying effective legal policies for tackling phishing cases in Indonesia. Moreover, this research is expected to serve as a meaningful contribution to community service efforts, particularly in supporting the achievement of SDGs goals related to the creation of decent jobs and promoting economic growth both nationally and globally.

2 Methods

The research adopts a qualitative approach, which, in this context, aims to explore the modus operandi of phishing perpetrators in cybercrime and assess the relevance of existing

policies. The type of research employed is doctrinal or normative juridical research, focusing on the effectiveness of legal provisions related to phishing in Indonesia. The analysis is planned to cover all regulations relevant to phishing, such as Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), the Indonesian Criminal Code (KUHP), and others. By using doctrinal research, this study focuses on the internal aspects of law, namely legislation, legal principles, legal doctrines, and the systematics of law, as well as employing a normative legal approach, which examines theories, concepts, and regulations related to legal issues.

In this study, both primary and secondary data are used. Primary data refers to original information obtained directly by the researcher to address the research questions. Sources of primary data include relevant legislation, legal documents, academic books, journal articles, news reports, and similar materials. Additionally, this research also incorporates secondary data derived from the views or opinions of legal experts, gathered through interviews or literature reviews.

Beyond normative juridical research, this study also adopts an empirical juridical approach, which seeks to complement doctrinal findings with field-based insights. Empirical data will be collected directly from stakeholders involved in phishing cases, including law enforcement officials, policymakers, and victims, in order to capture their perspectives, experiences, and challenges in combating phishing crimes. This approach allows the research to bridge the gap between legal norms and their practical implementation, providing a more comprehensive understanding of both the theoretical and applied dimensions of criminal policy on phishing in Indonesia.

Data collection is conducted using the documentation study method, which involves collecting and recording various authentic documents. Once the data has been gathered, the next step is to validate the data using the triangulation method—by comparing the contents of one document with others to ensure accuracy. Subsequently, the data is analyzed using a normative approach, in which validated legal sources are examined and utilized as a foundation for formulating solutions to the issues under study.

3 Results and Discussions

3.1 Legal Provisions Regarding Phishing in Indonesia

Cybercrime in the form of phishing is a type of fraud carried out through emails or fake websites with the intent of deceiving users, where the perpetrators typically impersonate trusted organizations. In Indonesia, phishing has not yet been explicitly regulated as a standalone criminal offense in any legislation. However, Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), along with the Indonesian Criminal Code (KUHP), currently serve as the legal basis for prosecuting phishing-related offenses.

Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) has undergone two amendments. The first amendment was introduced through Law Number 19 of 2016, which revised certain provisions of the original ITE Law. The second amendment was enacted through Law Number 1 of 2024, further modifying the ITE Law.

Several articles within the ITE Law can be used to prosecute phishing perpetrators, including:

1) Article 28(1) Jo. Article 45(2), which regulates the dissemination of false information causing harm in electronic transactions, punishable by up to six (6) years of imprisonment and/or a fine of up to IDR 1,000,000,000 (one billion rupiah). In the first amendment (Law No. 19/2016), Article 45(2) was amended and became Article 45A(1) with the same penalties. In the second amendment (Law No. 1/2024), these provisions

were updated again to refer to Article 28(1) and Article 45A(1);
2) Article 30(1) Jo. Article 46(1), concerning unauthorized access to another person's or the public's computer systems or electronic systems, punishable by up to six (6) years of imprisonment and/or a fine of up to IDR 600,000,000;
3) Article 30(2) Jo. Article 46(2), which addresses unauthorized access to obtain information or electronic documents, punishable by up to seven (7) years of imprisonment and/or a fine of up to IDR 700,000,000;
4) Article 30(3) Jo. Article 46(3), which pertains to unauthorized access with the intent to bypass security systems, punishable by up to eight (8) years of imprisonment and/or a fine of up to IDR 800,000,000;
5) Article 32(2) Jo. Article 48(2), concerning the illegal transfer of electronic information and/or documents to another person's electronic system, punishable by up to nine (9) years of imprisonment and/or a fine of up to IDR 3,000,000,000;

The Indonesian Criminal Code (KUHP) also includes provisions that may be applied to phishing cases:
1) Article 378 of the KUHP, which regulates the crime of fraud, punishable by up to four (4) years of imprisonment;
2) Article 372 of the KUHP, which governs the crime of embezzlement, punishable by up to four (4) years of imprisonment and/or a fine of up to IDR 900,000.

Despite the availability of various legal articles that can be used to prosecute phishing perpetrators, the number of reported phishing incidents in Indonesia remains high. This raises concerns about the overall effectiveness of existing legal provisions in combating phishing crimes in the country.

3.2 Effectiveness of Legal Provisions on Phishing in Indonesia

In Indonesia, phishing has not yet been specifically regulated as an independent criminal offense within the legislation. Nevertheless, such acts can still be subject to criminal sanctions under several existing legal provisions. Generally, phishing is categorized as a form of fraud under Article 378 of the Indonesian Criminal Code (KUHP) or embezzlement under Article 372 of the KUHP. In addition to the Criminal Code, phishing-related offenses may also be prosecuted under Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was amended by Law Number 19 of 2016. In 2024, the ITE Law was further amended through Law Number 1 of 2024, which introduced several provisions that could be applied to phishing offenses.

One of the major shortcomings of the ITE Law in addressing phishing lies in the absence of explicit provisions that directly criminalize this type of cyber fraud. The existing articles, particularly Articles 27 to 37, are drafted in broad and general terms, which makes it difficult for law enforcement officials to apply them specifically to phishing cases. This lack of clarity leads to multiple interpretations, resulting in legal uncertainty and inconsistent enforcement. Perpetrators are often able to exploit these loopholes to evade responsibility. Furthermore, the ITE Law has not adequately anticipated the emergence of new forms of cybercrime, such as phishing, spamming, doxing, and cybersquatting, which continue to evolve alongside technological advancements. The failure to explicitly regulate these offenses demonstrates that the current legal framework is reactive rather than preventive, leaving significant gaps in protection for society and making law enforcement less effective in combating increasingly sophisticated cyber threats. [5]

This lack of specific regulation creates challenges in law enforcement practice. Many phishing cases cannot be thoroughly pursued because they do not align with the elements outlined in existing criminal provisions. For example, phishing conducted via fake websites using social engineering techniques often cannot be processed under fraud provisions, as it

may not fulfill the specific elements of fraud as defined in Article 378 of the KUHP. Likewise, certain provisions within the ITE Law—while addressing the dissemination of false electronic information or unauthorized access to systems—are insufficient to cover all the rapidly evolving forms and methods of phishing. This demonstrates that Indonesia's current positive law has not fully kept pace with the development of new forms of phishing crimes, leaving law enforcement officials frequently challenged in classifying the offender's actions and proving phishing offenses in court. [6]

The United States, on the other hand, is one of the countries that has developed a comprehensive cyber law system, including specific measures to combat phishing. Unlike Indonesia, which still relies on general provisions in the ITE Law and the KUHP, the United States has detailed and specific regulations addressing phishing through various legal instruments. One such law is the Computer Fraud and Abuse Act (CFAA), which directly targets computer-based crimes, including unauthorized access and digital fraud. Additionally, the U.S. criminal justice system reinforces its regulation through U.S. Code Title 18, such as Section 1028A on aggravated identity theft and Section 1030 on fraud and unauthorized access to computers. These laws encompass various forms of cybercrime commonly found in phishing practices. The American legal system is also supported by dedicated law enforcement agencies like the FBI and the Cybersecurity and Infrastructure Security Agency (CISA), which are structurally and technically equipped to handle cybercrimes in a coordinated manner. [7]

When compared to the U.S. legal system through the lens of Lawrence M. Friedman's Legal System Theory, the weaknesses of Indonesia's phishing regulations become apparent across three dimensions: substance, structure, and legal culture. First, in terms of substance, Indonesian law does not define phishing as a distinct crime, making it less responsive to the evolving modes of cybercrime. Second, structurally, Indonesia lacks dedicated agencies like the FBI or CISA, as well as standardized digital forensic units. Third, in terms of legal culture, low digital literacy and public distrust in legal processes result in underreporting by victims, while law enforcement officials often lack sufficient digital forensic capabilities. [8]

To strengthen Indonesia's ability to combat phishing, concrete strategies are needed beyond legal reform. Public awareness campaigns should be systematically implemented to improve digital literacy, particularly regarding safe online behavior and early detection of phishing attempts. At the same time, capacity building for law enforcement is essential through regular training in digital forensics, cyber investigation techniques, and cross-sector collaboration with financial institutions and internet service providers. These efforts will not only enhance the competence of law enforcement officers but also foster greater public trust and participation in reporting phishing crimes.

4 Conclusion

Based on the above explanation, it can be concluded that although Indonesia already has several legal provisions that can be used to prosecute perpetrators of phishing crimes—both in the Criminal Code (KUHP) and the Electronic Information and Transactions Law (ITE Law), including its amendments up to 2024—these regulations are still neither specific nor comprehensive. The existing provisions are generally formulated and do not explicitly recognize phishing as a distinct criminal offense, which complicates the process of identification, evidence gathering, and law enforcement. This is reflected in the persistently high number of phishing cases and the low rate of case resolution. This ineffectiveness becomes even more evident when compared to the criminal law system in the United States, which has established specific legal instruments such as the Computer Fraud and Abuse Act (CFAA) and the U.S. Code Title 18, supported by competent and well-structured cybersecurity enforcement agencies. Using Lawrence M. Friedman's legal system theory, Indonesia's weaknesses in addressing phishing can be seen in three dimensions: the

substance of the law, which has yet to accommodate developments in digital crime; the legal structure, which is not yet institutionally and technically equipped; and the legal culture, which is still affected by low digital literacy and limited public trust. Therefore, substantive legal reform, strengthening of law enforcement structures, and raising public awareness are urgently needed for Indonesia to effectively and sustainably address the challenges posed by phishing crimes. In conclusion, while Indonesia has a legal foundation to address phishing through the Criminal Code and the ITE Law, the absence of a specific and comprehensive regulation continues to hinder effective enforcement. Therefore, beyond legal reform, practical strategies are urgently needed. These include systematic public awareness campaigns to strengthen digital literacy and proactive capacity building for law enforcement officers through training in digital forensics and cybercrime investigation. Such efforts will not only improve the effectiveness of phishing countermeasures but also enhance public trust and participation in combating cybercrime. [9–12]

References

1. Laporan Aktivitas Abuse Domain.Id Indonesia Domain Abuse Data Exchange, n.d.
2. PT. BPR Bank Jombang Perseroda. Bank Jombang, *Serangan Phishing Di Indonesia Terus Meningkat, Berikut Data Lengkapnya*, (unpublished).
3. Y. H. Lokapala, F. J. Nurfauzi, and Y. Widowaty, Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia, Indonesian Journal of Criminal Law and Criminology (IJCLC), **5**, (2024).
4. P. R. Rangkuti, M. A. Khoiri, S. Ritonga, P. Nabila, and S. Pane, Sanksi Pidana terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia, **291** (n.d.). https://doi.org/10.62383/konstitusi.v2i3.908
5. A. Mulyana Hadi, Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice, Jolsic Journal of Law, Society, and Islamic Civilization, **53** (2024). https://doi.org/10.18196/ijclc.v5i1.19853
6. N. Darmawan and W. Saraswati, Efektivitas Penegakan Hukum Terhadap Tindak Pidana Phishing di Indonesia, Jurnal Penegakan Hukum Dan Keadilan 15 (2023).
7. P. Aditama, E. A. Sinaga, and C. A. Putri, Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya dalam Penegakan Hukum antara Indonesia dan Amerika, Jurnal Kompilasi Hukum, **60** (2025).
8. Rahmat and Wahyuni, Analisis Efektivitas Sistem Hukum Indonesia Berdasarkan Teori Lawrence M. Friedman, Jurnal Ilmu Hukum 45 (2020).
9. A. Sahfitri, Penipuan Digital Melalui Tautan Phishing, Jurnal Dialektika Hukum, **6**, (2024).
10. Arabel, E. Y. Sekar, and I. Musofiana, Studi Perbandingan Hukum Pidana dalam Penanganan Kejahatan Siber: Perspektif Indonesia dan Amerika Serikat, Causa Jurnal Hukum Dan Kewarganegaraan, **6**, 1 (2024).
11. Cahyaningsih, D. Rohmah, A. Fauzan, S. Hasbi, and A. Winanti, Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang- Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia, Abdurrauf Science and Society, **1**, 800 (2025).
12. Matondang, M. Aulia, and Andryan, Kebijakan Hukum Pidana Terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia Dan Thailand Dalam Perspektif Hukum Internasional, Rewang Rencang : Jurnal Hukum Lex Generalis **6**, 1 (2025).