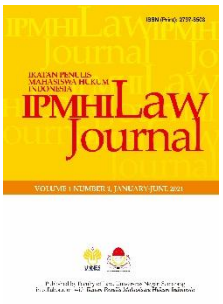
IKATAN PENULIS MAHASISWA HUKUM INDONESIA LAW JOURNAL



ISSN 2797-8508 (Print)
ISSN 2807-8330 (Online)
VOL.5 NO.2, JUNE-DECEMBER (2025)

Riwayat Artikel
History of Article
Diajukan: 10 Desember 2025
Submitted
Direvisi: 12 Desember 2025
Revised
Diterima: 25 Desember 2025
Accepted
Saran Perujukan
How to cite:
Abidah et.al. (2025). Criminal Policy of Indonesian Criminal Law in Combating the Crime of Phishing *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 5*(2), 297-314. https://doi.org/10.15294/ipmhi.v5i2.38656

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

Shofriya Qonitatin Abidah,[1] Sonny Saptoajie Wicaksono,[1] Muhammad Reza Faturahman,[1] ✉Nisrina Khoirunnisa,[1] Sri Wulandari[1]
[1] Faculty of Law, Universitas Negeri Semarang,

✉Email Korespondensi: rezafaturahman608@students.unnes.ac.id

Abstract Phishing is one of the forms of cybercrime that is increasingly widespread in Indonesia. However, to date, there is no legislation that explicitly defines phishing as an independent criminal offense. 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. Law enforcement against perpetrators still relies on general provisions in the Indonesian Penal Code (KUHP) and the Electronic Information and Transactions Law Number 1 Of 2024 Concerning The Second Amendment Of Law Number 11 Of 2008 On Information And Electronic Transactions. which are considered insufficient to fully address the complexity of phishing modus operandi. This results in suboptimal prosecution processes and inadequate legal protection for victims. In contrast to Indonesia, the United States has established more specific and comprehensive regulations concerning phishing, supported by integrated law enforcement agencies. Using Lawrence M. Friedman's legal system theory, it can be concluded that phishing regulations in Indonesia are still ineffective in terms of legal substance, institutional structure, and the public's legal culture. A

comprehensive legal reform is needed to appropriately respond to the evolving dynamics of digital crime.
Keywords Technology, Cybercrime, Phishing, Criminal Policy

Abstrak Phishing merupakan salah satu bentuk kejahatan siber yang semakin meluas di Indonesia. Namun hingga saat ini, belum ada peraturan perundang-undangan yang secara tegas mendefinisikan phishing sebagai tindak pidana yang berdiri sendiri. Di satu sisi, kemajuan teknologi memberikan kemudahan dan efisiensi; namun di sisi lain, hal ini menimbulkan tantangan baru yang tidak dapat diabaikan, salah satunya adalah kejahatan siber. Penegakan hukum terhadap pelaku masih bergantung pada ketentuan umum dalam Kitab Undang-Undang Hukum Pidana (KUHP) serta Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang dinilai belum mampu sepenuhnya menjangkau kompleksitas modus operandi phishing. Kondisi ini menyebabkan proses penegakan hukum menjadi kurang optimal dan perlindungan hukum bagi korban belum memadai. Berbeda dengan Indonesia, Amerika Serikat telah memiliki regulasi yang lebih spesifik dan komprehensif terkait phishing, serta didukung oleh lembaga penegakan hukum yang terintegrasi. Berdasarkan teori sistem hukum Lawrence M. Friedman, dapat disimpulkan bahwa pengaturan mengenai phishing di Indonesia masih belum efektif, baik dari segi substansi hukum, struktur kelembagaan, maupun budaya hukum masyarakat. Oleh karena itu, diperlukan reformasi hukum yang menyeluruh untuk merespons secara tepat dinamika kejahatan digital yang terus berkembang.
Kata kunci Teknologi, Kejahatan Siber, Phising, Kebijakan Kriminal

A. 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: 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].

The Directorate of Special Criminal Investigation (Ditreskrimsus) of the Central Java Regional Police has stated that, in recent years, Indonesia has experienced a significant surge in cybercrime cases. This increase reflects the growing misuse of information technology alongside the expansion of digital services across various sectors. In addition, reports issued by the National Cyber and Crypto Agency (BSSN) indicate a sharp rise in cybercrime incidents, with an estimated increase of approximately 40% in 2022. During this period, thousands of cyberattacks were recorded and officially reported to the relevant authorities.

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

[1] "LAPORAN AKTIVITAS ABUSE DOMAIN .ID Indonesia Domain Abuse Data Exchange." n.d. www.pandi.id.
[2] PT. BPR Bank Jombang Perseroda. Bank Jombang. 2025. "Serangan Phishing Di Indonesia Terus Meningkat, Berikut Data Lengkapnya." PT. BPR Bank Jombang Perseroda. Bank Jombang. 2025.

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.

In the study titled "Legal Aspects of Phishing Crimes in Indonesian Law", Yazid Haikal Lokapala et al. 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. 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.

Based on the background issues raised, the research formulates the following problems:

1. What are the current legal provisions regarding phishing in Indonesia?
2. How effective are the legal provisions on phishing in Indonesia?

Accordingly, this discussion identifies several relevant studies that serve as both the urgency and the main focus of this research, particularly those related to the existing legal provisions, the effectiveness of law enforcement in addressing phishing crimes, and the need for criminal policy that is more responsive and adaptive to the evolving nature of cybercrime. These studies form the analytical foundation for assessing the extent to which Indonesian criminal law is capable of responding to the increasingly complex and dynamic practices of phishing.

B. Research Methods

This research employs a qualitative approach aimed at examining the modus operandi of phishing perpetrators in cybercrime and evaluating the relevance of existing legal policies. The study adopts a doctrinal or normative juridical method, which focuses on analyzing the effectiveness of Indonesia's current legal framework concerning phishing. The analysis encompasses various regulations related to

[3] Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. 2024. "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia." Indonesian Journal of Criminal Law and Criminology (IJCLC) 5 (1). https://doi.org/10.18196/ijclc.v5i1.19853.

phishing, including Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), the Indonesian Criminal Code (KUHP), and other relevant legal instruments. By applying a doctrinal method, this research concentrates on internal aspects of the law—such as legislation, legal principles, doctrines, and systematics—while also utilizing a normative legal approach that involves reviewing legal theories, concepts, and regulations pertinent to the issue.

Both primary and secondary data are utilized in this study. Primary data consists of original sources obtained directly by the researcher to answer the research questions, including statutory laws, legal documents, academic literature, journal articles, and relevant media reports. Meanwhile, secondary data includes expert opinions and interpretations derived from interviews and literature studies.

Data collection is carried out through the documentation method, which involves gathering and reviewing authentic legal and academic records. To ensure data accuracy, the triangulation technique is applied by cross-checking the consistency and reliability of information across multiple sources. Finally, the data is analyzed through a normative framework, where verified legal materials are examined and used as the basis for developing conclusions and solutions to the identified legal problems.

Observations and interviews conducted with the Directorate of Cyber Crime (Ditres Siber) of the Central Java Regional Police constitute an important source of empirical data in this research, as they provide direct insights into the practical challenges faced by law enforcement in handling cybercrime, particularly phishing-related offenses. These field findings reinforce the existence of normative and technical obstacles in the investigation, evidence gathering, and enforcement processes of cybercrime cases, thereby complementing the doctrinal and normative legal analysis employed in this study.

C. Discussion

1. Current 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 contemporary digital society, phishing has become one of the most prevalent cyber threats because it exploits not only weaknesses in technology but also vulnerabilities in human behavior. Phishing schemes are designed to manipulate victims psychologically, often by creating a sense of urgency, fear, or trust. For example, perpetrators may send emails that appear to come from legitimate banks, government institutions, or well-known companies, persuading users to click malicious links or disclose confidential credentials.

Phishing is particularly dangerous because it can affect anyone who participates in online communication and digital transactions. Victims often suffer significant losses, including financial theft, identity fraud, reputational damage, and emotional distress. In many cases, phishing serves as an entry point for broader cybercriminal operations, such as ransomware attacks, money laundering, and

organized digital fraud networks. The rapid expansion of e-commerce, online banking, and digital government services in Indonesia has increased the opportunities for phishing perpetrators to target individuals and institutions alike.

In Indonesia, phishing has not yet been explicitly regulated as a standalone criminal offense in any legislation. This absence of explicit criminalization creates a major challenge within the national legal system, as law enforcement authorities must rely on general provisions rather than a specific legal framework tailored to phishing. 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. These laws provide the normative foundation for cybercrime enforcement, yet their provisions remain broad and indirect, often failing to fully address the complexity and evolving nature of phishing attacks[4].

The lack of a dedicated phishing offense means that prosecutors must interpret phishing acts through categories such as fraud, illegal access, data manipulation, or dissemination of false information. While such interpretations allow some level of enforcement, they also create inconsistencies in judicial outcomes and uncertainty in legal practice. Moreover, because phishing is frequently transnational, anonymous, and technologically sophisticated, the reliance on conventional criminal provisions may weaken Indonesia's capacity to respond effectively.

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. This amendment was largely motivated by criticisms of over-criminalization and concerns regarding freedom of expression. It sought to clarify sanction mechanisms while maintaining legal instruments to combat cyber offenses. The second amendment was enacted through Law Number 1 of 2024, further modifying the ITE Law. The 2024 revision reflects Indonesia's continuing attempt to modernize its cyber legal framework amid increasing cyber threats and public demands for proportional criminal enforcement.

Nevertheless, despite the significance of the 2024 amendment as the most recent legal reform, it does not introduce explicit provisions that directly define or criminalize phishing as an independent offense. Instead, it largely maintains existing formulations, leaving phishing prosecutions dependent on broad interpretations of general cybercrime norms. This demonstrates that legislative reform remains incomplete and reactive rather than preventive.

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). Although Law No. 1 of 2024 maintains the substance of this

[4] Rangkuti, Putri Ramadhani, Muhammad Aldi Khoiri, Sumantri Ritonga, Putri Nabila, and Sitorus Pane. n.d. "Sanksi Pidana Terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia," no. 2: 291–305. https://doi.org/10.62383/konstitusi.v2i3.908.

provision from previous amendments, the revision reflects a broader legislative tendency toward proportionality and restraint in criminal enforcement.

This tendency is often associated with the promotion of restorative justice principles, which emphasize reconciliation, victim recovery, and reduced reliance on punitive imprisonment. Restorative justice may be appropriate for certain minor offenses, particularly those involving interpersonal disputes. However, in the context of phishing particularly large-scale or organized phishing targeting the financial sector such an approach risks reducing deterrent effects and may be counterproductive. Phishing typically involves deliberate deception, systematic targeting of vulnerable users, and repeated victimization. The economic harm caused by phishing is often extensive, affecting not only individual victims but also undermining trust in digital financial systems.

Furthermore, the application of Article 28(1) is often limited because phishing does not always involve "false information" in the conventional sense but rather fraudulent impersonation and manipulation. The absence of a clear distinction between misinformation offenses and cyber fraud schemes complicates enforcement, as phishing perpetrators may exploit loopholes in interpretation. Therefore, while Article 28(1) remains one of the available legal tools, it is not fully sufficient to address phishing comprehensively.

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. In phishing cases, this provision is relevant when perpetrators gain access to victims' accounts without authorization, such as online banking accounts, email services, or digital wallets.

   Unauthorized access constitutes a central element of many cybercrimes. However, phishing differs from traditional hacking because perpetrators often do not technically "break into" systems but instead trick victims into voluntarily providing access credentials. This raises important questions about whether access obtained through deception should be treated the same as access obtained through technical intrusion.

   The 2024 amendment does not provide further clarification on whether access obtained through social engineering techniques rather than technical system breaches falls squarely within the scope of this article, leaving room for interpretative uncertainty in enforcement. This ambiguity can weaken prosecution, as defense arguments may claim that victims consented by entering their information, even though such consent was obtained fraudulently. Consequently, clearer legislative guidance is needed to ensure that phishing-related unauthorized access is consistently criminalized.

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. This provision is particularly relevant because phishing schemes are primarily aimed at acquiring sensitive information, such as login credentials, personal identification numbers, financial account data, and verification codes.

While phishing frequently aims to obtain confidential electronic documents and information, the absence of explicit recognition of phishing methods in the 2024 amendment means that law enforcement must continue relying on broad interpretations. This reliance may weaken legal certainty and consistency in prosecution, as different courts may interpret "access" and "obtaining information" differently.

Moreover, phishing crimes evolve rapidly alongside technological innovation. Perpetrators now use advanced tactics such as AI-generated impersonation, fake mobile applications, and sophisticated website cloning. Without explicit legal recognition of phishing as a specific offense, enforcement remains dependent on outdated conceptual categories, making it difficult for the legal system to keep pace with cybercriminal developments.

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. This provision addresses more severe forms of cyber intrusion involving deliberate bypassing of technical security measures.

   Although applicable to technically sophisticated cyber intrusions, many phishing attacks do not involve direct system penetration but rather exploit human vulnerabilities. Perpetrators may bypass security indirectly by manipulating victims into sharing OTP codes or clicking malicious links. As a result, Article 30(3) may not effectively capture phishing cases that rely primarily on deception rather than technical hacking.

   This gap remains unaddressed in the 2024 amendment, demonstrating that Indonesian cybercrime regulation still focuses heavily on technical intrusion rather than the broader spectrum of cyber deception. Given that phishing is fundamentally based on fraudulent manipulation, a legal framework that emphasizes only system penetration may fail to address the most common cybercrime threats faced by society.

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. In phishing cases, this article becomes relevant when stolen personal or financial data is transferred, distributed, or sold to third parties.

   Data transfer is often part of organized phishing networks, where perpetrators monetize stolen information through underground markets. Victims may suffer long-term consequences, including identity theft, financial fraud, and reputational harm. Nevertheless, Law No. 1 of 2024 does not introduce any specific aggravating circumstances for data misuse arising from phishing activities, despite their severe impact on victims and the financial system.

   The absence of aggravating provisions is particularly concerning because phishing often targets critical sectors such as banking, e-commerce, and public digital services. Without stronger legal recognition of the seriousness of phishing-related data crimes, deterrence remains limited.

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. However, its formulation is rooted in conventional fraud and does not adequately capture the technological complexity, anonymity, and transnational character of phishing crimes.
   Traditional fraud assumes direct interpersonal interaction, whereas phishing is typically remote, anonymous, and digitally mediated. The offender may operate from outside Indonesia, using fake identities and international infrastructure. As a result, applying Article 378 often requires interpretative stretching, which may reduce its effectiveness as a legal instrument against cyber-enabled fraud.

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. Its application to phishing cases is often indirect and limited, as phishing typically involves deceitful acquisition rather than prior lawful possession.
   Embezzlement provisions presuppose lawful possession before misappropriation, which rarely occurs in phishing. Therefore, reliance on Article 372 demonstrates the inadequacy of conventional criminal law provisions to address modern cybercrime phenomena.

Despite the availability of these provisions, the enactment of Law No. 1 of 2024 has not introduced substantive norms that specifically strengthen the regulation of phishing. Instead, the amendments largely preserve existing formulations without addressing evolving phishing techniques or clarifying the limits of restorative justice for serious cybercrimes.

This demonstrates that the reference to the 2024 amendment should not be viewed merely as procedural novelty, but as evidence that Indonesia's legal framework still lacks a targeted and comprehensive approach to combating phishing. Without explicit criminalization, clearer interpretative guidelines, and stronger institutional capacity, phishing will continue to pose a major threat to digital security, economic stability, and public trust in Indonesia's evolving digital ecosystem.

2. Effectiveness of Legal Provisions on Phishing in Indonesia

The effectiveness of criminal law regulation against phishing in Indonesia must be assessed not merely from the existence of normative provisions, but from the precision of their dogmatic construction in capturing the specific character of phishing as a form of cyber fraud based on data manipulation and social engineering. Although phishing is commonly subsumed under Article 378 of the Indonesian Criminal Code (KUHP) concerning fraud, doctrinal problems arise in fulfilling the legal elements of this provision. Article 378 requires that the perpetrator, by means of false names, false capacity, deceit, or a series of lies, induces another person to hand over goods, provide credit, or extinguish a debt. While the element of deceit can be satisfied through the use of fake websites or impersonation of legitimate institutions, the object of the offense in phishing is generally not a tangible "good" but rather digital credentials, personal data, or authentication information. Within the classical conception of property (goed) in the KUHP, such data do not always clearly

fall within the scope of "goods" or proprietary rights, thereby creating doctrinal uncertainty and evidentiary difficulties in qualifying phishing as conventional fraud.[5]

From the perspective of the Electronic Information and Transactions Law (ITE Law), a more appropriate dogmatic basis for phishing can be found in Article 35 in conjunction with Article 51 paragraph (1), which criminalizes the manipulation, creation, alteration, or deletion of Electronic Information or Electronic Documents with the intent that such data be considercffaed as authentic. The ratio legis of this provision is to safeguard the integrity and authenticity of electronic information systems. Phishing, which operates by engineering electronic interfaces, emails, and websites to appear legitimate in order to deceive users, essentially constitutes the creation of a false electronic reality that simulates authenticity. Nevertheless, law enforcement practice in Indonesia has tended to rely on more general provisions such as Articles 28 and 30 of the ITE Law, while Article 35—whose teleological orientation is most closely aligned with the modus operandi of phishing—has not been consistently utilized as the primary legal basis. This indicates a weakness in systematic and teleological interpretation rather than a complete absence of legal norms.[6]

The ineffectiveness of the application of material law, when further examined through the perspective of criminal policy as articulated by Barda Nawawi Arief, reveals a disjunction between the formulation policy (the legislative stage) and the application policy (the law enforcement stage). At the formulation level, although the ITE Law has undergone its second amendment through Law Number 1 of 2024, the orientation of criminalization remains fixated on the technical protection of electronic systems, failing to fully address the aspect of digital identity protection, which constitutes the primary target of phishing attacks. Consequently, at the application stage, law enforcement officials are compelled to employ extensive interpretation of conventional fraud provisions (Article 378 of the KUHP) to prosecute conduct that is inherently far more complex than merely inducing a person to deliver goods. This dogmatic challenge creates tangible legal uncertainty; on the one hand, society expects comprehensive protection, yet on the other, prosecutors and judges are constrained by the strict principle of legality, which demands precise correspondence between the elements of the offense and the facts of the conduct.

Analyzed through Lawrence M. Friedman's legal system theory, the issue of effectiveness also involves structural and cultural dimensions. Structurally, Indonesia cannot be said to lack specialized cyber institutions, as the National Police have established the Directorate of Cyber Crime (Dittipidsiber) within the Criminal Investigation Agency (Bareskrim), and the state has formed the BSSN to oversee national cybersecurity. Therefore, the core structural problem lies not in institutional absence but in the limitations of inter-agency coordination, the technical capacity of

[5] Wahyudi, Thea Farina, and Claudia Yuni Pramita. n.d. "EFEKTIFITAS PASAL 378 KUHP PADA TRANSAKSI JUAL BELI ONLINE." Jurnal Dinamika Hukum dan Masyarakat, 113–21.

[6] Gusti, I, Ayu Tiary Cayani, I Made, and Wirya Darma. n.d. "Kekuatan Pembuktian Alat Bukti Elektronik Dalam Perkara Pidana Pencemaran Nama Baik Melalui Media Sosial." https://doi.org/10.61104/alz.v3i5.2255.

digital forensic investigators, and the speed of response in dismantling phishing infrastructures that are often transnational and highly adaptive.[7]

Based on the results of an interview with Mr. Dwi Susilo, S.E., an investigator at the Cyber Crime Directorate (Ditressiber) of the Central Java Regional Police, it was found that the available facilities and infrastructure are still inadequate to handle phishing crimes that are increasingly complex and technology-based. These limitations constitute a significant obstacle in the investigation and prosecution process, resulting in the suboptimal implementation of the criminal justice system in addressing phishing offenses.

This fact becomes increasingly crucial when examined through the lens of Lawrence M. Friedman's legal system theory, particularly concerning the aspect of legal structure. Legal structure encompasses not merely the existence of police or prosecutorial institutions, but also the technical capacity and system integration within them. Drawing upon realities found in interviews with investigators from the Ditressiber of the Central Java Regional Police, the structural obstacles encountered are not simply matters of personnel shortages, but rather a velocity gap between the criminal *modus operandi* and law enforcement procedures. Phishing perpetrators operate within seconds, utilizing technological automation to disseminate thousands of fake links, whereas the law enforcement structure continues to operate under a bureaucratic procedural logic that requires days merely to trace a single IP address. This disparity confirms that the current legal structure is not designed to respond to high-speed crime, rendering it unsurprising that the case clearance rate remains suboptimal relative to the number of reports received.

Supporting the statement of Mr. Dwi Susilo, S.E., and as reported by the Ditressiber of the Central Java Regional Police, Indonesia has experienced a significant surge in cybercrime cases in recent years. This phenomenon is consistent with reports from the BSSN, which indicate that the number of cybercrime incidents increased sharply in 2022, with thousands of cyberattacks recorded and reported to the relevant authorities. The most prevalent types of cybercrime include phishing, ransomware, and malware, which predominantly target the financial sector and digital service users. Furthermore, BSSN's annual report notes that in 2025 there was an approximate 40% increase in cybercrime complaints compared to previous years. This escalation demonstrates that cybercrime, particularly phishing, has evolved into a serious threat that not only causes individual financial losses but also poses risks to the stability of the national financial system and digital security. These conditions underscore the significant challenges faced by law enforcement agencies in preventing and combating cybercrime effectively, especially in light of regulatory limitations, as current legal frameworks have yet to specifically and comprehensively regulate phishing as an independent criminal offense.

When analyzed using Soerjono Soekanto's legal system theory, this condition indicates that the facilities and infrastructure factor—one of the key determinants of effective law enforcement—has not been adequately fulfilled. According to Soerjono Soekanto, the effectiveness of law enforcement is influenced by five factors: legal substance, law enforcement officials, facilities and infrastructure, society, and legal culture. The failure to fulfill one of these factors undermines the overall effectiveness

[7] Disemadi, Hari Sutra, and Cindy Kang. 2021. "Tantangan Penegakan Hukum Hak Kekayaan Intelektual Dalam Pengembangan Ekonomi Kreatif Di Era Revolusi Industri 4.0" 7 (1).https://ejournal.undiksha.ac.id/index.php/jkh.

of law enforcement. Therefore, the inadequacy of law enforcement facilities and infrastructure in handling phishing crimes reflects a structural constraint within the criminal justice system, which in turn negatively affects the effectiveness of law enforcement against phishing offenses.

Furthermore, Soerjono Soekanto's theory regarding facilities and infrastructure as determinants of legal effectiveness finds its strongest relevance in this case. In the context of cybercrime, facilities can no longer be interpreted merely as office buildings or operational vehicles, but rather as the availability of capable digital forensic laboratories down to the regional level and up-to-date tracking software. The absence of these facilities at the resort police (Polres) level often causes a case backlog at the Regional Police (Polda) or National Police Headquarters, which ultimately creates a bottleneck in the investigation process. This directly implicates the loss of digital evidence, which is highly volatile and easily altered or deleted by perpetrators. Thus, the ineffectiveness of phishing countermeasures in Indonesia can be seen as a logical consequence of the failure to meet the minimum facility requirements needed to enforce cyber law ideally.

Beyond the aspects of structure and facilities, the aspect of legal culture plays an equally important role in determining whether a regulation is effective. In the phishing crime ecosystem, the legal culture of society often becomes the weakest link exploited by perpetrators. Low digital literacy among the public, unaccompanied by a prudent attitude in interacting within the cyber space, creates massive opportunities for victimization. Many victims unknowingly surrender their personal data because they are deceived by social engineering—a method that attacks the victim's psychology rather than hacking the device's security system. This phenomenon demonstrates that the law cannot operate alone in a vacuum; it requires cultural support in the form of public legal awareness to protect their own personal data as a form of primary prevention.

Comparatively, the experience of the United States demonstrates that the effectiveness of phishing prosecution is not solely derived from the existence of specific statutes such as the Computer Fraud and Abuse Act (CFAA), but from a clear formulation of the actus reus as unauthorized access and misuse of electronic identity for unlawful gain. The focus is placed on the core conduct of manipulating computer systems and digital identities rather than on the formal label of the offense. Conceptually, this approach can be accommodated within the Indonesian civil law system by strengthening the construction of electronic data manipulation and identity misuse in the ITE Law and the new Criminal Code, without adopting the common law model in a purely textual manner.[8]

The comparison with law enforcement in the United States, reveals significant differences in approach. While in Indonesia the emphasis remains heavily on the repressive aspect (post-incident crackdown) using general provisions, the United States, through the Computer Fraud and Abuse Act (CFAA), has moved toward a more specific approach by explicitly criminalizing 'unauthorized access' and 'identity theft.' Effectiveness there is supported by a more integrated reporting culture and the role of institutions like the Federal Trade Commission (FTC), which actively carries out preventive-administrative actions. This provides a valuable lesson that to

[8] Aditama, Prigel, Elisabeth Aprilia Sinaga, and Citra Anjelika Putri. 2025. "Perbandingan Hukum Pidana Cyber Crime Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika." Journal Kompilasi Hukum 10 (1): 58–76. https://doi.org/10.29303/jkh.v10i1.202.

make the law against phishing effective in Indonesia, it is not enough to rely solely on the KUHP or the ITE Law; rather, there is a need for harmonization between criminal law, administrative law, and systematic public education.

In terms of criminal policy, the strengthening of the legal response to phishing should not be limited to general recommendations such as public education and capacity building, but must be directed toward more operational measures. These include the development of judicial and prosecutorial guidelines that recognize digital credentials and electronic identities as protected legal objects equivalent to property in modern fraud, the systematic application of Article 35 of the ITE Law as the central offense for phishing based on document and data manipulation, and the integration of reporting and rapid takedown mechanisms between financial institutions, internet service providers, Dittipidsiber Polri, and BSSN. Such measures reflect a penal policy that combines doctrinal refinement, institutional coordination, and preventive-administrative action in order to ensure that the criminal law framework is capable of responding effectively to the evolving dynamics of phishing as a contemporary form of cybercrime.[9]

As a synthesis of the various obstacles outlined above, it can be concluded that the ineffectiveness of the law in combating phishing in Indonesia is a systemic, multidimensional problem. This issue cannot be resolved partially by merely revising one or two articles in the legislation. A comprehensive criminal policy reform is required, encompassing the renewal of legal substance to be more adaptive to identity theft offenses, the strengthening of legal structure through the equitable modernization of investigation facilities, and the engineering of legal culture to build a resilient and legally aware digital society. Without simultaneous measures on these three elements of the legal system, law enforcement efforts against phishing will only be sporadic and fail to provide the expected deterrent effect, leaving Indonesia's cyber space as fertile ground for the growth of digital financial crimes.

D. Conclusion

Based on the discussion, it can be concluded that Indonesia’s criminal policy in combating phishing crimes remains ineffective and insufficiently comprehensive. Although existing positive law both under the KUHP and the ITE Law, including its latest amendment through Law Number 1 of 2024 can be used as a legal basis for prosecuting phishing-related offenses, these regulations are still formulated in general terms and do not explicitly recognize phishing as an independent criminal offense. This condition creates significant challenges in legal qualification, evidentiary processes, and the proportional application of criminal sanctions in response to increasingly sophisticated phishing modus.

In practice, law enforcement authorities are often compelled to interpret phishing acts through broader categories such as fraud, unauthorized access, or dissemination of misleading information, which may not fully reflect the unique characteristics of phishing as a cyber-enabled deception crime. Consequently, the absence of a specific legal framework weakens legal certainty and contributes to

[9] Indriani Berlian Mewengkang, Robert N. Warong, and S.H., M.H. Michael Kuntag. 2021. “KAJIAN YURIDIS CYBER CRIME PENANGGULANGAN DAN PENEGAKAN HUKUMNYA.” Lex Crimen 10 (5): 26–35.

inconsistencies in prosecution and judicial decisions. Moreover, phishing crimes frequently involve transnational elements, anonymous perpetrators, and rapidly evolving digital techniques, requiring legal provisions that are more adaptive and technologically responsive than the current framework provides.

This ineffectiveness is reflected in the continuous increase in phishing cases reported by the Ditreskrimsus and BSSN. The rising number of cybercrime reports demonstrates not only the escalation of digital threats but also exposes weaknesses within Indonesia's law enforcement system. Phishing has become one of the most dominant cybercrime threats targeting Indonesian society, particularly within the financial and digital transaction sectors. The persistence of such cases suggests that the existing criminal policy approach has not yet achieved its deterrent function, nor has it provided effective protection for victims.

Phishing continues to expand in scope, targeting not only individual consumers but also major institutions such as banks, e-commerce platforms, and government-related digital services. The growing complexity of phishing methods ranging from email impersonation and fake websites to smishing and AI-generated fraud highlights the inadequacy of relying solely on conventional penal provisions that were not originally designed to address technologically mediated crimes.

According to Mr. Dwi Susilo, S.E., one of the contributing factors to the high incidence of phishing crimes is the limited availability of facilities, technological infrastructure, and supporting resources within the Directorate of Cyber Crime Investigation. These limitations affect the speed and effectiveness of investigations, digital tracing, and preventive measures, such as the rapid takedown of phishing websites. Cybercrime investigations require advanced forensic tools, specialized investigators, and real-time monitoring systems, especially since perpetrators often operate through encrypted networks and foreign-based servers. When institutional capacity is insufficient, law enforcement may struggle to respond promptly, allowing phishing infrastructures to remain active and continue victimizing the public. This demonstrates that criminal policy must include institutional readiness and technological capability, not merely legal drafting.

From a criminal policy perspective, phishing cannot be effectively addressed through a purely normative and repressive penal approach. Concrete and measurable policy measures are urgently required. First, from the perspective of legal substance, it is necessary to strengthen and expand judicial interpretation of concepts such as "data manipulation" and "electronic fraud" through judicial instruments, including a Supreme Court Circular Letter (Surat Edaran Mahkamah Agung/SEMA). Such guidance would provide clearer standards for judges and prosecutors in classifying phishing offenses without forcing them into conventional fraud provisions. A SEMA could also clarify that credentials obtained through social engineering constitute unlawful electronic deception, even when victims appear to provide information voluntarily under fraudulent circumstances.

Second, from a structural and administrative perspective, an integrated phishing reporting system particularly within the banking and digital financial sectors should be directly connected to the Cyber Patrol Unit of the Indonesian National Police. This integration would enable swift administrative actions, such as blocking or takedown of phishing websites before broader harm occurs. Currently, reporting mechanisms remain fragmented, often delaying response. A centralized framework linking financial institutions, cybersecurity authorities, and cyber police units would strengthen early detection and rapid intervention. This reflects the understanding that cybercrime prevention requires proactive disruption, not only prosecution after losses occur.

Third, enhancing the facilities and technical capacities of the Directorate of Cyber Crime Investigation must be positioned as part of a national criminal policy supported by a clear legal basis and adequate budget allocation. The fight against phishing demands investment in forensic laboratories, surveillance technology, specialized training, and inter-agency cooperation mechanisms. Without institutional strengthening, even comprehensive legal reforms will remain ineffective in practice. Enforcement capacity is inseparable from legal substance.

In addition, Indonesia may consider adopting comparative approaches from jurisdictions such as the United States, which has established specific legal instruments like the Computer Fraud and Abuse Act (CFAA) and specialized cyber enforcement agencies. While Indonesia's context differs, the comparative example demonstrates the importance of explicit criminalization, specialized institutional frameworks, and coordinated administrative enforcement in reducing cybercrime prevalence.

In conclusion, addressing phishing crimes in Indonesia requires an integrated criminal policy combining regulatory reform, institutional strengthening, and improvements in administrative and technological systems. The continuing reliance on general KUHP provisions and broad ITE Law norms, without explicit recognition of phishing as an independent cyber offense, has contributed to enforcement challenges and persistent case growth. Without concrete measures such as judicial interpretative expansion through SEMA, integrated reporting and takedown mechanisms connected to Cyber Patrol, and enhancement of cybercrime investigation infrastructure, phishing crimes will continue to threaten digital security, financial system stability, and public trust in Indonesia's criminal justice system. Therefore, a comprehensive, adaptive, and institutionally supported criminal policy is urgently necessary to respond effectively to phishing as one of the most serious cybercrime threats in the digital era.

E. Referensi

Adwi Mulyana Hadi. (2024). Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice. *Jolsic Journal of Law, Society, and Islamic Civilization*, 53–54.

Arabel, Yunita Sekar E., & Ida Musofiana. (2024). Studi Perbandingan Hukum Pidana dalam Penanganan Kejahatan Siber: Perspektif Indonesia dan Amerika Serikat. *Causa Jurnal Hukum Dan Kewarganegaraan* , *6*(11), 1–4.

Cahyaningsih, Rohmah D., Anis Fauzan, Saupi Hasbi, & Atik Winanti. (2025). , Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang- Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia. *Abdurrauf Science and Society* , *1*(4), 800–810.

Disemadi, H. S., & Kang, C. (2021). Tantangan Penegakan Hukum Hak Kekayaan Intelektual dalam Pengembangan Ekonomi Kreatif di Era Revolusi Industri 4.0. *JURNAL KOMUNIKASI HUKUM*, *7*(1), 54–71. https://ejournal.undiksha.ac.id/index.php/jkh

I Gusti Ayu Tiary Cayani, & I Made Wirya Darma. (2025). Kekuatan Pembuktian Alat Bukti Elektronik dalam Perkara Pidana Pencemaran Nama Baik melalui Media Sosial. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(5). https://doi.org/10.61104/alz.v3i5.2255

Indriani Berlian Mewengkang, Robert N. Warong, & Michael Kuntag, S. H. , M. H. (2021). KAJIAN YURIDIS CYBER CRIME PENANGGULANGAN DAN PENEGAKAN HUKUMNYA. *Lex Crimen*, *10*(5), 26–35.

LAPORAN AKTIVITAS ABUSE DOMAIN .ID Indonesia Domain Abuse Data Exchange. (n.d.). Retrieved www.pandi.id

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *5*(1). https://doi.org/10.18196/ijclc.v5i1.19853

Matondang, Aulia M., & Andryan. (2025). KEBIJAKAN HUKUM PIDANA TERHADAP KEJAHATAN CYBER STUDI PERBANDINGAN ANTARA INDONESIA DAN THAILAND DALAM PERSPEKTIF HUKUM INTERNASIONAL. *Rewang Rencang : Jurnal Hukum Lex Generalis*, *6*(1), 1–13.

Novan Darmawan, & Wiwi Saraswati. (2023). Efektivitas Penegakan Hukum Terhadap Tindak Pidana Phishing di Indonesia. *Jurnal Penegakan Hukum Dan Keadilan*, 15–23.

Prigel Aditama, Elisabeth Aprilia Sinaga, & Citra Anjelika Putri. (2025). Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya dalam Penegakan Hukum antara Indonesia dan Amerika. *Jurnal Kompilasi Hukum*, 60–76.

PT. BPR Bank Jombang Perseroda. Bank Jombang. (2025). *Serangan Phishing di Indonesia Terus Meningkat, Berikut Data Lengkapnya*. PT. BPR Bank Jombang Perseroda. Bank Jombang.

Rahmat, & Wahyuni. (2020). Analisis Efektivitas Sistem Hukum Indonesia Berdasarkan Teori Lawrence M. Friedman. *Jurnal Ilmu Hukum*, 45–60.

Rangkuti, P. R., Khoiri, M. A., Ritonga, S., Nabila, P., & Pane, S. (n.d.). *Sanksi Pidana terhadap Kejahatan Pishing Menurut Hukum Pidana Indonesia*. (2), 291–305. https://doi.org/10.62383/konstitusi.v2i3.908

Sahfitri, A. (2024). PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. *Jurnal Dialektika Hukum*, *6*(2). https://bankjombang.co.id/serangan-phishing-di-indonesia-terus

Wahyudi, Farina, T., & Pramita, C. Y. (n.d.). EFEKTIFITAS PASAL 378 KUHP PADA TRANSAKSI JUAL BELI ONLINE. *Jurnal Dinamika Hukum dan Masyarakat*, 113–121.

This page is intentionally left blank