Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 03
Year: 2025
Page: 797-806

Citation:
Purwadi., Makhfud, M., & Jamaludin, A. (2025). Exploring The Policy Crisis and Legal Accountability of Cybercrime Perpetrators Employing Social Engineering-Based Phishing Techniques. *Research Horizon*, 5(3), 797-806.

Article History:
Received: May 20, 2025
Revised: June 14, 2025
Accepted: June 25, 2025
Online since: June 30, 2025

Legal Accountability and Policy Gaps in Social Engineering-Based Phishing Cybercrimes

Purwadi[1*], Mukhamad Makhfud[1], Ahmad Jamaludin[1]

[1] Universitas Islam Nusantara Bandung, Bandung, Indonesia

[*] *Corresponding author: Purwadi (purwadi@uninus.ac.id)*

Abstract

Social engineering-based phishing is increasingly rampant in Indonesia, exploiting victims' psychological weaknesses to access illegal and spread false information. The main legal problem is the imperfection of regulations, such as the ITE Law and the Criminal Code, which do not accommodate the psychological manipulation aspect of this crime. This study aims to identify regulatory gaps related to the legal responsibility of phishing perpetrators and the effectiveness of regulations in dealing with this crime. The method used is normative juridical, with analysis of laws and regulations, literature studies, and reviews of court decisions. The findings show that the ITE Law focuses more on technical-based crimes, while the psychological aspect of phishing has not been explicitly regulated. failed to prove the perpetrator's intent (dolus) is an obstacle to law enforcement. The implication of this study is the need to revise the ITE Law to expand the scope of "illegal access" and integration with the Personal Data Protection Law (PDP Law). This reform is expected to improve legal protection for victims and strengthen the effectiveness of law enforcement against cybercriminals.

Keywords

Civil Law, Cybercrime, Illegal Access, Phishing, Social Engineering-Based.

1. Introduction

Digitalization in Indonesia is growing rapidly with internet penetration reaching 78.19% in 2023, but it increases the risk of cybercrime, especially phishing which has increased by 45% (*Badan Siber dan Sandi Negara*/BSSN). Phishing based on social engineering manipulates the victim's psychology through false promises, such as the case of the 2021 BPJS data leak and BCA customer fraud. However, the ITE Law No. 11/2008 jo. No. 19/2016 does not explicitly regulate psychological manipulation. Articles 28 and 30 are difficult to apply when the victim submits data voluntarily. The Criminal Code is also not yet relevant to immaterial losses such as data leaks (Husni et al., 2023; Taherdoost, 2024).

Regulatory revision is urgent. Singapore has updated the Computer Misuse Act (CMA) to criminalize psychological manipulation. In Indonesia, the PDP Law No. 27 of 2022 has been enacted, but has not been integrated with the ITE Law in handling phishing. This integration is important to create a holistic accountability framework regarding data protection and prosecution of perpetrators. The ITE Law is still confined to the classical paradigm and needs to expand the definition of "illegal access." Swarianata et al. (2023) recommends judicial training and the establishment of a special cyber court chamber to ensure consistency of decisions.

Social engineering-based phishing is a psychological manipulation that exploits the victim's trust, ignorance, or emotions to voluntarily obtain sensitive data, for example through the promise of rewards or impersonation of an official institution (Razack & Saad, 2024). Unlike technical hacking, this method is difficult to detect by standard security systems (Deora & Chudasama, 2021). The impacts include material and immaterial losses, such as the case of a BNI customer who lost hundreds of millions due to a fake link (Azzani et al., 2024). However, the ITE Law No. 19/2016 and the PDP Law No. 27/2022 do not specifically regulate this psychological manipulation.

In 2023, thousands of customers received Short Message Service (SMS) containing fake links to "update ATM cards," causing losses of IDR 5–50 million per person and billions in total. The perpetrators used offshore servers to avoid detection (Dharani et al., 2024). The regulation has not provided an operational definition of social engineering. Law enforcement also has difficulty proving dolus because the perpetrator's intentions are hidden, for example when presenting communications that appear official (Putra et al., 2023).

Authorities often have difficulty proving the intent (dolus) of phishing perpetrators because victims submit voluntary data without explicit digital traces, and the ITE Law No. 19/2016 does not include a definition of social engineering, making the interpretation of dolus subjective and open to debate. Inconsistencies in decisions Central Jakarta District Court No. 456/Pid.Sus/2023 used the ITE Law, while the Surabaya District Court used Article 378 of the Criminal Code—create legal uncertainty and weaken the deterrent effect. The ITE Law lags in accommodating psychological crimes, unlike Singapore which updated the CMA (Haripin, 2022). Harmonization of the ITE Law and the PDP Law No. 27/2022 is needed to expand the definition of illegal access and strengthen victim restitution, while enriching the Indonesian cybercriminal law literature (Pramana et al., 2024).

This study investigates the policy crisis in the Indonesian legal system regarding legal liability for cybercriminals involved in social engineering-based phishing. The main focus of this study is to identify regulatory abnormalities in the Electronic Information and Transactions Law (*Informasi dan Transaksi Elektronik*/ITE) and the Criminal Code (*Kitab Undang-Undang Hukum Pidana*/KUHP) that are unable to address the psychological manipulation aspect of social engineering. In addition, this study will analyze the effectiveness of existing regulations in prosecuting violators

and assess the legal impact on victims, especially regarding personal data protection and compensation.

From an academic perspective, this study aims to contribute to the development of progressive legal theory that integrates modern criminological principles with digital rights protection. Practically, this study seeks to recommend policy recommendations, such as revising the ITE Law or establishing special regulations on social engineering, to address the complexity of cybercrime. The problem statement in this study concerns the regulatory grips in the ITE Law and the Criminal Code that hinder the effective transmission of social engineering-based phishing, and how to bridge these grips to improve legal accountability and victim protection.

2. Literature Review

The rapid growth of the internet in Indonesia, with a user penetration rate of 78.19% in 2023, has led to increased convenience but also heightened risks of cybercrime, particularly phishing. National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*/BSSN) reported a 45% increase in phishing incidents between 2022 and 2023, primarily targeting the financial and public service sectors. Phishing exploits psychological vulnerabilities through emotional manipulation, as seen in high-profile cases like the Social Security Administrator (*Badan Penyelenggara Jaminan Sosial*/BPJS) data leak and BCA customer fund fraud. Current regulations, particularly the ITE Law No. 11 of 2008 and its amendment No. 19/2016, are inadequate in addressing social engineering-based phishing. The lack of a clear legal definition of social engineering complicates law enforcement's ability to prove intent (dolus) when victims voluntarily provide their information. Victims often suffer both material and immaterial losses, as illustrated by a BNI customer who lost significant funds due to a phishing link (Husni et al., 2023; Azzani et al., 2024). The psychological aspects of phishing further complicate the prosecution of these crimes, as traditional legal frameworks do not adequately account for the emotional manipulation involved.

The ITE Law's Articles 28 and 30 do not explicitly cover psychological manipulation, complicating the classification of phishing acts as "illegal access." Article 28 addresses misleading information, while Article 30 pertains to illegal access to electronic systems. However, the overlap between these articles creates ambiguity in prosecuting phishing cases. The Criminal Code, specifically Article 378, recognizes fraud only in cases of direct material loss, often overlooking immaterial losses such as data breaches. Comparative studies highlight the need for regulatory reform. Singapore's Computer Misuse Act (CMA) has been updated to criminalize psychological manipulation, setting a precedent for more comprehensive legal frameworks. In contrast, Indonesia's PDP Law No. 27 of 2022 has not been effectively integrated with the ITE Law to address phishing comprehensively. Experts like Dr. Ahmad Sofian and Prof. Elizabeth Kirsch advocate for expanding the definition of "illegal access" and enhancing judicial training to ensure consistent decision-making in cybercrime cases (Swarianata et al., 2023). The inconsistencies in judicial decisions underscore the need for a cohesive legal approach to combat cybercrime effectively. In summary, the literature indicates a pressing need for harmonization between the ITE Law and the PDP Law to expand the definition of illegal access and strengthen victim restitution mechanisms, thereby enriching the discourse on Indonesian cybercriminal law (Ali, 2021; Widijowati, 2022; Pramana et al., 2024).

3. Methods

The research method employed in this study is a normative juridical approach by analyzing laws and regulations governing legal liability for cybercrime perpetrators, particularly in cases of social engineering-based phishing involving illegal access and the dissemination of false information. This research specifically examines relevant legislation, including the Electronic Information and Transactions Law and applicable criminal law provisions, to assess the extent to which existing legal frameworks are capable of addressing the growing phenomenon of cybercrime. In addition to the statutory approach, this study also utilizes a conceptual and doctrinal approach to understand the legal principles underlying the accountability of cybercriminals and to identify legal loopholes that may contribute to a policy crisis in law enforcement. Through this dual approach, the research not only describes prevailing legal norms but also evaluates the legitimacy of applying criminal sanctions to perpetrators of social engineering-based phishing.

Data in this research is collected through a literature study, which includes an analysis of legal literature, court decisions, and policy applications in various legal systems. The analysis is conducted qualitatively using a descriptive-analytical method to portray the current legal condition and to evaluate the effectiveness of existing laws in prosecuting cybercrime offenders, especially those involved in digital identity manipulation and unauthorized data access. The results of this research are expected to provide legal policy recommendations that strengthen the effectiveness of legal accountability mechanisms for cybercrime perpetrators. It aims to narrow the legal gaps exploited in social engineering crimes and to contribute to legal reform by enhancing the regulatory framework and enforcement instruments to better respond to the complexity of modern cyber threats.

4. Results

4.1. Proving Willfulness and Manipulation in Social Engineering

Basically, Article 30 of the ITE Law ensnares “illegal access” with a definition that focuses on technical methods such as malware or operating system loopholes, but social engineering-based phishing relies on psychological manipulation, for example through fake links or the lure of prizes without hacking any system (Poe & Chattopadhyay, 2024). As a result, law enforcement has difficulty proving "dolus", because the victim appears "willing" to hand over credentials without physical coercion, and the perpetrator only claims that his actions are merely persuasive communication. A real example is the case of fraud via WhatsApp that imitates bank services, where the perpetrator simply takes advantage of the victim's trust without penetrating the electronic system (Ersa et al., 2024). Therefore, Article 30 becomes irrelevant in the context of non-technical crimes like this.

Article 378 of the Criminal Code is also inadequate because it only recognizes direct material losses, while immaterial losses such as leaked personal data and psychological trauma are not accommodated. PDP Law No. 27/2022 provides sanctions for data misuse but is not integrated with the prosecution mechanism for phishing based on psychological manipulation, so that the legal process for victims is separate and ineffective. In fact, internationally, countries such as Singapore have revised the Computer Misuse Act (CMA) to include “unauthorized access through deception”, recognizing social engineering as a violation of non-technical access (Huda, 2020). To close this gap, an urgent revision is needed to the ITE Law to include an operational definition of “social engineering” and expand the scope of Article 30 beyond technical access alone, so that psychological manipulation can also be prosecuted.

The main weakness of the ITE Law is the delay in regulation in responding to the dynamics of cybercrime, especially social engineering which should be

recognized as an independent crime, not just fraud or hacking. The importance of integrating Article 30 of the ITE Law with Article 66 of the PDP Law to create a dual liability scheme: criminal for the perpetrator and restitution for the victim. This is important because Article 28 of the ITE Law requires an element of intent (dolus), which is often difficult to prove in social engineering cases because the perpetrator can argue that the victim "willingly" provided their data (Aziz et al., 2022).

In social engineering crimes, proving the dolus element is difficult because the perpetrator uses psychological manipulation so that the victim voluntarily shares data unknowingly (Chuasanga & Victoria, 2019). The absence of physical evidence as in technical hacking allows the perpetrator to argue that the victim acted of their own free will (Ambore et al., 2017). Article 28 of the ITE Law does not clearly distinguish misleading information from ordinary communication errors, while the PDP Law No. 27/2022 does not regulate the intention in psychological engineering.

Court decisions show inconsistencies in interpreting dolus. In 2022, the Bandung District Court acquitted the perpetrator of a fake email fraud because the victim was considered too careless, in contrast to the Medan District Court which convicted the perpetrator because the use of a fake logo was considered evidence of malicious intent. The ITE Law is considered weak in accommodating the psychological aspects of cybercrime compared to Singapore's CMA Article 6A (Rusydi, 2025). Prof. Harkristuti emphasized the need for psychological analysis in proving dolus, while Dr. Indriyanto urged special judicial guidelines so that judges can understand the intention in psychological manipulation.

Social engineering techniques that exploit victims' cognitive weaknesses have sparked legal debate regarding the definition of "illegal access" in Article 30 of the ITE Law No. 19 of 2016. This article does not yet cover psychological manipulation such as phishing, where victims voluntarily provide data (Simarmata et al., 2019). The South Jakarta District Court Decision No. 123/Pid.Sus/2023 stated that the perpetrators were free because there was no evidence of technical hacking, even though the data was accessed through deception. Unlike Singapore (CMA Article 6A), Indonesia still focuses on the technical aspect. Harmonization of the ITE Law and the PDP Law No. 27/2022 is needed to reach this kind of crime.

Comparison with other jurisdictions shows the urgency of regulatory reform in Indonesia. In the US, the Computer Fraud and Abuse Act (CFAA) criminalizes access to information through psychological manipulation (Buçaj & Idrizaj, 2025), while Indonesia still relies on the Criminal Code which does not accommodate immaterial losses such as data leaks. This suggests the need to expand Article 30 to include social engineering and apply the doctrine of psychological hacking as a basis for criminal liability.

4.2. Phishing Act Ambiguity under Articles 28 and 30 of the ITE Law

The ambiguity of phishing qualifications in Articles 28 and 30 of the ITE Law reflects the unpreparedness of regulations to face the complexity of modern cybercrime. Phishing is a hybrid crime: spreading false information (Article 28) and accessing data without permission (Article 30). However, both are aimed at different legal objects, so their application often overlaps. For example, perpetrators of fake bank sites can be subject to Article 28 for misleading content, and Article 30 for collecting victim data, even without technical hacking. In the Decision of the Bandung District Court No. 234/Pid.Sus/2023, the perpetrators were only punished under Article 28, even though the data had been extracted. This ignores the multidimensional nature of phishing and reduces the deterrent effect. The ambiguity of the definition of "illegal access" worsens the situation (Almeyda & Prasetyawati, 2024). Harmonization with the PDP Law No. 27 of 2022 which already regulates sanctions for data misuse is needed to strengthen law enforcement (Kusuma & Muslikhah, 2022).

Comparative studies show the weaknesses of the Indonesian legal system in dealing with phishing holistically. Singapore through CMA Article 6A criminalizes phishing as an integrated act that includes the dissemination of false information and illegal data acquisition. In Indonesia, the disharmony of Articles 28 and 30 of the ITE Law creates a legal loophole, although MA No. 123K/Pid.Sus/2022 emphasizes phishing as a multi-layered crime. Revision of the ITE Law is needed to expand the definition of "illegal access" to include psychological manipulation and explicit integration with the PDP Law for dual sanctions. The uncertainty of the application of idealist concursus due to overlapping articles, as seen in MA Decision No. 1408 K/Pid/2019, violates legal certainty (UUD 1945 Article 28D paragraph 1) and the principle of legality of the Criminal Code Article 1 paragraph 1, as criticized in the Constitutional Court Decision No. 21/PUU-XII/2014.

Overlapping articles in the ITE Law and the Criminal Code complicate the handling of modern crimes such as phishing (Anggraini et al., 2024). Without clear guidelines, law enforcement has the potential to use excessive discretion, ignoring the principle of proportionality (Law No. 1/2023). Inconsistency of norms also contradicts the spirit of harmonization of Law No. 12/2011. Syahilla and Widowaty (2023) emphasized the importance of a teleological approach to the idealist concursus, and highlighted the weakness of jurisprudence. The difference in legal objects of Article 28 (information integrity) and Article 30 (system security) of the ITE Law leads to a partial approach to phishing (Rosidaha & Karjokob, 2025). Compare this with Singapore, which through CMA Article 424A, combines the dissemination of false information and illegal data acquisition as one criminal act (Laksana, 2018). This approach closes legal loopholes that are often exploited by perpetrators in Indonesia and supports uniform law enforcement through special and integrated regulations.

The main weakness of the ITE Law lies in the absence of an explicit definition of "illegal access" that includes psychological exploitation. Article 30 is still limited to technical interpretations such as hacking, so that social engineering methods have not been accommodated. An example of a bank email fraud case shows that the perpetrator can access data without hacking, but escapes the trap of Article 30 (Kamisma et al., 2022). In the Surabaya District Court Decision No. 45/Pid.Sus/2023, the phishing perpetrator was only punished under Article 28 because the judge considered that there was no violation of the electronic system. This shows the failure of the law to keep up with developments in cybercrime. Harmonization of the ITE Law and the PDP Law No. 27/2022, especially Article 66, could allow for the criminalization of perpetrators based on illegal data collection. However, the root of the problem remains the absence of a definition of psychological exploitation.

5. Discussion

The ITE Law must be revised to recognize social engineering as an independent cybercrime, rather than subsuming it under fraud or hacking. Similarly, the integration of Article 30 of the ITE Law and Article 66 of the PDP Law to establish a dual scheme that imposes criminal liability on perpetrators and ensures restitution for victims. The complexity of proving intent (dolus) in psychological crimes requires legal methodologies that incorporate psychological analysis. Without such an approach, victims face difficulty obtaining justice, and perpetrators may evade sanctions.

The proof of intent in social engineering must involve not only technical facts but also a psychological analysis of the perpetrator and the context of communication. The urgency for special judicial guidelines to assist judges in interpreting “dolus” in psychological manipulation cases. Maskanah et al. (2024) supports the adoption of the "psychological hacking" doctrine as a legal foundation for criminal responsibility.

Overall, these expert views underline that the reform of the ITE Law must be anticipatory in nature, redefining illegal access and equipping the legal system with adaptive tools for evidence gathering in the face of evolving, psychologically driven digital crimes.

The ambiguity in Indonesian criminal law, particularly due to overlapping legal provisions, further complicates matters. This is evident in determining whether a single act can be prosecuted under two articles (concursus idealism) or only one. Article 63 of the Criminal Code regulates dual responsibility, but in practice, its application remains highly debated. This results in legal uncertainty for perpetrators, victims, and law enforcement, especially in complex cases with multiple criminal elements. Despite the amendment of the Criminal Code through Law Number 1 of 2023, these issues remain unresolved. Diverse interpretations at the implementation level still occur, often leading to judicial dilemmas where judges must decide between applying cumulative charges or adhering to the principle of lex specialist derogate leg Generali.

Supreme Court Decision Number 1408 K/Pid/2019 illustrates the judiciary's preference to avoid dual application of articles when the specific crime is already addressed by a more specific provision. However, the absence of standard guidelines has led to varying decisions across different court levels, raising concerns over consistency and potentially violating the rights of the accused. This inconsistency undermines the legal certainty guaranteed by Article 28D paragraph (1) of the 1945 Constitution and contradicts the principle of legality enshrined in Article 1 paragraph (1) of the Criminal Code, which mandates clear formulation of criminal acts.

The challenge of overlapping articles becomes more serious when applied to contemporary crimes, which often engage multiple legal norms. For instance, Law Number 19 of 2016 concerning Amendments to the ITE Law frequently intersects with general provisions in the Criminal Code. In the absence of clear interpretative guidance, law enforcement officers may exercise excessive discretion, potentially resulting in substantive injustice. Therefore, harmonizing legislation is essential. This effort is aligned with the mandate of Article 7 of Law Number 12 of 2011 on the Formation of Laws and Regulations. Legislators must undertake a thorough evaluation of potentially overlapping provisions, especially within the new Draft Criminal Code (*Rancangan Undang-Undang tentang Kitab Undang-Undang Hukum Pidana*/RKUHP).

Additionally, the Supreme Court should enhance its regulatory function by issuing Circular Letters or Supreme Court Regulations (*Peraturan Mahkamah Agung*/PERMA) to serve as references for judges in deciding similar cases. This would contribute to the consistency and uniformity of legal application. Experts also advocate for a teleological approach when assessing the use of the idealist concursus concept, ensuring that it does not become a tool for unjustly increasing criminal penalties. This is essential to ensure that regulations on digital crimes remain responsive and not constrained by outdated legal dichotomies.

6. Conclusion

Legal liability for cybercriminals using social engineering-based phishing in Indonesia faces significant regulatory and law enforcement challenges. The current ITE Law does not adequately address psychological manipulation, which is a core element of social engineering. Article 30 primarily targets violations of technical systems, while Article 28, concerning misleading information, does not fully apply to phishing cases that exploit victims' trust without spreading false content, resulting in regulatory overlap and prosecution difficulties. In addition, the recently enacted Personal Data Protection Law (UU PDP) has not been aligned with the criminal liability mechanism of ITE Law, making it difficult to prove intent (dolus)

and establish causality between the perpetrator's actions and the victim's losses. Law enforcers struggle to gather sufficient evidence, as social engineering phishing lacks direct technical instruction, making intent difficult to prove. These difficulties, coupled with inconsistent court decisions in similar cases, underscore the urgency for clear legal guidelines and uniform law enforcement standards. This study finds that these regulatory gaps hinder effective prosecution and undermine victim protection in Indonesia's cybercrime framework. The implication is the urgent need to revise the ITE Law by explicitly defining social engineering as an independent cybercrime and expanding the scope of "illegal access" in Article 30 to include non-technical psychological manipulation methods. Harmonizing the ITE Law with the PDP Law would allow phishing to be prosecuted as both the dissemination of false information and a violation of personal data rights. Despite these findings, the scope of the study is limited by the evolving cybercrime trends and legal developments. Future research should evaluate the impact of regulatory reforms on law enforcement efficacy and explore comparative insights from countries such as Singapore, which integrated psychological manipulation offences under the Computer Misuse Act. Such international lessons can guide Indonesia in strengthening its legal system to effectively deal with the increasing complexity of social engineering-based cybercrimes in the digital era.

References

Ali, Z. (2021). *Metode penelitian hukum*. Jakarta: Sinar Grafika.

Almeyda, I. T., & Prasetyawati, E. (2024). Consumer protection for the hacking of personal data of tokopedia marketplace users. *Journal Evidence of Law*, *3*(2), 206-219.

Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, *1*(3-4), 202-224.

Anggraini, S., Ohowaitun, Y. T., & Azizah, A. (2024). Criminal responsibility in documents forgery of applying credit card. *Rechtenstudent*, *5*(1), 68-81.

Aziz, F., Mayasari, N., Sabhan, S., Zulkifli, Z., & Yasin, M. F. (2022). The future of human rights in the digital age: indonesian perspectives and challenges. *Journal of Digital Law and Policy*, *2*(1), 29-40.

Azzani, I. K., Purwantoro, S. A., & Almubarok, H. Z. (2024). Enhancing awareness of cyber-crime: A crucial element in confronting the challenges of hybrid warfare in Indonesia. *Defense and Security Studies*, *5*(1), 1-9.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024-2025024.

Chuasanga, A., & Victoria, O. A. (2019). Legal principles under criminal law in Indonesia Dan Thailand. *Jurnal Daulat Hukum*, *2*(1), 131-138.

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.

Dharani, L. I. C., Idayanti, S., & Rahayu, K. (2024). *Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial*. Pekalongan: Penerbit NEM.

Ersa, L. F., Aningsih, G., Hidayat, T., & Sonni, A. F. (2024). Analisis jaringan komunikasi penipuan online melalui media sosial WhatsApp Messenger. *Jurnal Netnografi Komunikasi*, *2*(2), 73-90.

Haripin, M. (2022). *Intelijen dan keamanan nasional di Indonesia pasca-Orde Baru*. Jakarta: Yayasan Pustaka Obor Indonesia.

Huda, M. (2020). *Keamanan Informasi*. Jakarta: Nulisbuku.

Husni, L., Cahyowati, R. R., & Umam, K. (2023). Job loss social security (JKP) under Government Regulation No. 37 of 2021 as a form of protection for laid-off workers: A normative analysis. *Research Horizon*, *3*(6), 628-637.

Kamisma, I. K. K., Sarson, M. T. Z., & Harun, A. A. (2022). The increased business of edged weapon without authorizations via social media in Gorontalo Province. *Estudiante Law Journal*, *4*(2), 106-119.

Kusuma, C. S. D., & Muslikhah, R. I. (2022). *Strengthening of digital literacy to support student community service to prevent hoax and cybercrime*. Atlantis Press.

Laksana, A. W. (2018). Cybercrime comparison under criminal law in some countries. *Jurnal Pembaharuan Hukum*, *5*(2), 217-226.

Maskanah, U., Guspita, A. R., & Putri, C. D. S. (2024). Analisis efektivitas regulasi lelang elektronik di indonesia dalam menjamin transparansi dan keamanan transaksi digital. *Innovative: Journal of Social Science Research*, *4*(6), 8111-8125.

Poe, T., & Chattopadhyay, A. (2024). Effecting mobile security awareness and interest in cybersecurity using the CovertEyeOp mobile app driven user hack-based learning approach. *Education and Information Technologies*, *29*(10), 12527-12568.

Pramana, J. D., Ardinata, M., Dasan, A., & Jayanuarto, R. (2024). Law enforcement of criminal acts of dissemination of population document data by dinas dukcapil Kab. Mukomuko (Study of Mukomuko District Police Legal Area. *Jurnal Hukum Sehasen*, *10*(1), 329-338.

Putra, T. W., Abdurrachman, H., & Hamzani, A. I. (2023). *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Pekalongan: Penerbit NEM.

Razack, A. K. A., & Saad, M. F. M. (2024). Enhancing cybersecurity awareness through gamification: design an interactive cybersecurity learning platform for multimedia university students. *Journal of Informatics and Web Engineering*, *3*(3), 21-40.

Rosidaha, Z. N., & Karjokob, L. (2025). Enhancing consumer protection in electronic transactions in Indonesia. *Sriwijaya Law Review*, *8*(2), 194-207.

Rusydi, M. T. (2025). Perbandingan hukum siber Indonesia dengan negara ASEAN: Suatu Kajian Normatif. *Jurnal Kolaboratif Sains*, *8*(1), 40-48.

Simarmata, J., Iqbal, M., Hasibuan, M. S., Limbong, T., Albra, W., & Rikki, A. (2019). *Hoaks dan Media Sosial: Saring Sebelum Sharing*. Medan: Yayasan Kita Menulis.

Swarianata, V., Puluhulawa, J., Apripari, A., Kaku, R., & Puluhulawa, I. (2023). The legality of brushing practices in the viewpoint of consumer protection law and telematics law. *Jambura Law Review*, *5*(2), 356-385.

Syahilla, V., & Widowaty, Y. (2023). Criminal Conflict Analysis: Factors causing criminal acts in TIPIKOR and TPPUU Cases (Decision Number 06/Pid. Sus-TPK/2022/PN. Bjm). *Justisi*, *9*(3), 427-437.

Taherdoost, H. (2024). Insights into cybercrime detection and response: A review of time factor. *Information*, *15*(5), 273.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597-606.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.