The Easta Journal Law and Human Rights
Vol. 4, No. 03, June 2026, pp. 349 – 358
ISSN: 2985-7112, DOI: 10.58812/eslhr.v4i03

Challenges in Law Enforcement Against Online Phishing Fraud from a Positive Law Perspective

Siti Hardianti Rambing[1], Fenty U. Puluhulawa[2], Apripari[3]
[1,2,3] Faculty of Law, Gorontalo State University

Article Info

Article history:

Received May, 2026
Revised May, 2026
Accepted Jun, 2026

Keywords:

Cybercrime;
Cybersecurity;
Law Enforcement;
Phishing;
Positive Law

ABSTRACT

The development of information technology has fueled an increase in cybercrime, particularly online fraud through *phishing*, which poses serious challenges for law enforcement in Indonesia. This study aims to analyze the obstacles to law enforcement against *phishing* from a positive law perspective and to evaluate the effectiveness of existing regulations. The method used is normative legal research with a legislative and conceptual approach, through a literature review of primary, secondary, and tertiary legal materials. The results of the study indicate that the obstacles to law enforcement are multidimensional, including weaknesses in legal substance that have not adapted to technological developments, limitations in the capacity of law enforcement officials and supporting facilities, as well as low digital literacy among the public. Furthermore, the cross-border nature of the crime and the complexity of digital evidence exacerbate the challenges in law enforcement. This study concludes that an integrative approach is necessary through regulatory reform, institutional capacity building, and strengthened collaboration between the government, the private sector, and the public to achieve effective and responsive law enforcement against *phishing* crimes.

Corresponding Author:

Name: Siti Hardianti Rambing
Institution: Faculty of Law, Gorontalo State University
Email: sitihardiantirambing@gmail.com

1. INTRODUCTION

The development of information and communication technology has driven significant transformations in various aspects of society, including economic activities and digital transactions. Easy internet access and the increasing use of digital devices have created opportunities for *cybercrime*, one of which is online fraud through *phishing scams*. This method involves deceiving victims through electronic messages or fake websites that mimic official entities to obtain the victims' personal and financial data. This phenomenon indicates a shift in crime patterns from conventional crimes toward more complex, technology-based crimes that are difficult to trace [1].

Normatively, Indonesia has established various positive legal instruments to combat cybercrime, such as Law No. 11 of 2008 on Information and Electronic Transactions, as amended by Law No. 19 of 2016, as well as the Criminal Code (KUHP). However, the implementation of law enforcement against *phishing* crimes still

faces various obstacles, whether from the perspective of legal substance, the structure of law enforcement agencies, or the legal culture of society. This creates a gap between existing legal norms and the reality of law enforcement on the ground [2].

The main issue in this study lies in assessing the effectiveness of law enforcement against online fraud using *the phishing* method from the perspective of positive law in Indonesia, as well as identifying the factors that act as barriers in this process. *The* complexity of *phishing* crimes, which involve *borderless* technology, creates difficulties in the process of evidence gathering, tracking perpetrators, and coordination among law enforcement agencies. Additionally, the public's low digital literacy further exacerbates vulnerability to this crime.

Previous studies indicate that law enforcement efforts against cybercrime in Indonesia still face various structural and technical challenges. Research by several academics highlights that the shortage of human resources with expertise in digital forensics is a primary obstacle. Furthermore, existing regulations are deemed insufficient to fully accommodate the increasingly dynamic and innovative evolution of cybercrime methods [3]. Therefore, a more comprehensive study is needed to identify these barriers and formulate appropriate solutions.

This study aims to analyze the obstacles to law enforcement regarding online fraud involving *phishing schemes* from the perspective of positive law in Indonesia. Additionally, this study seeks to examine the effectiveness of existing regulations and provide recommendations for improving the law enforcement system to make it more adaptable to technological advancements. Thus, this study is expected to contribute both theoretically and practically to the development of cyber law in Indonesia.

The approach used in this study is a normative legal approach, examining relevant laws and regulations, supported by literature reviews and case analyses. This approach was chosen to thoroughly examine the alignment between applicable legal norms and actual law enforcement practices in the field. Additionally, a conceptual approach is employed to understand the characteristics of *phishing* as a form of cybercrime with global dimensions.

The novelty of this study lies in its comprehensive analysis of the obstacles to law enforcement against online fraud using *the phishing* method, which is examined not only from a normative perspective but also from an implementational and contextual perspective. This study also offers an integrative perspective between positive law and the development of information technology, thereby aiming to provide more practical solutions in combating cybercrime.

Thus, this research is crucial given the rising number of online fraud cases that cause widespread harm to the public. Effective and responsive law enforcement that keeps pace with technological advancements is the key to fostering security and trust within the digital ecosystem. Consequently, this study is intended to serve as a reference for policymakers, law enforcement officials, and academics in developing more effective and sustainable strategies to combat *phishing* crimes.

2. LITERATURE REVIEW

2.1 The Concept of Law Enforcement in Positive Law

Law enforcement is a process of translating legal norms into reality through the actions of law enforcement officials. Law enforcement is influenced by several factors, namely the law itself, law enforcement officials, resources or facilities, society, and legal culture [4]. In the context of positive law in Indonesia, law enforcement is not only oriented toward *legal* certainty but also justice and utility [5]. This indicates that the effectiveness of law enforcement heavily depends on the balance between written norms and their implementation in practice.

Furthermore, from a criminal law perspective, law enforcement regarding information technology-based

crimes faces unique challenges due to their dynamic and complex nature. Muladi emphasizes that the criminal justice system must be able to adapt to the evolution of modern crime, including cybercrime [6]. Therefore, an integrated approach is required between adequate regulations and the capacity of law enforcement officials to address new forms of crime such as *phishing*.

2.2 *Cybercrime and Phishing Methods*

Cybercrime is a form of crime that utilizes information technology as both a means and a target. One of the most common forms is *phishing*, which involves attempting to obtain sensitive information such as passwords, credit card numbers, or other personal data by impersonating a trusted party. According to Wall, *phishing* is part of rapidly growing digital fraud-based crime, in tandem with the increasing use of the internet [7].

In the Indonesian context, *phishing* is implicitly regulated under the Electronic Information and Transactions Law (EIT Law), particularly regarding unauthorized access and electronic fraud. However, existing regulations still have limitations in addressing the various new modus operandi that continue to emerge [8]. Additionally, the public's low digital literacy also serves as a factor that increases the potential for *phishing* crimes [9].

2.3 *Challenges in Law Enforcement Against Online Fraud*

Challenges in law enforcement regarding online fraud, particularly *phishing*, can be classified into several aspects: legal substance, legal structure, and legal culture. From the perspective of legal substance, legislation often lags behind technological advancements, resulting in *legal gaps* [10]. From a structural perspective, the limited availability of human resources with expertise in digital forensics poses a major obstacle in the investigation and evidence-gathering processes [11].

Additionally, obstacles arise from the legal culture of society, which remains low in terms of awareness and caution regarding the use of digital technology. Legal culture is one of the key elements determining the success of law enforcement [12]. In this context, individuals who lack an understanding of *phishing* risks are more likely to become victims, making preventive efforts through education critically important. Thus, enforcing laws against online fraud requires not only robust regulations but also comprehensive support from various other aspects.

3. METHODS

This *study* is a normative legal study that focuses on the analysis of positive legal norms governing the enforcement of laws against online fraud committed through *phishing*. The research subjects include relevant legislation, such as the Criminal Code (KUHP) and the Electronic Information and Transactions Law (ITE Law), as well as court rulings related to cybercrime cases. The research subjects include law enforcement officials in a conceptual sense, legal doctrines, and academic literature relevant to the research topic. This research will be conducted during the period of 2025–2026, utilizing a *library-based research approach*, and is therefore not tied to a specific geographic location.

The research instruments used are document studies consisting of primary, secondary, and tertiary legal materials. Primary legal materials include legislation and court rulings, while secondary legal materials consist of books, scientific journals, and previous research relevant to the enforcement of laws against *phishing* crimes. Tertiary legal materials include legal dictionaries, encyclopedias, and online sources that support conceptual understanding. Sampling was conducted using *purposive sampling*, which involves selecting sources directly relevant to the research problem. Data collection was carried out through library research by cataloging,

reviewing, and classifying the obtained legal materials.

Data analysis in this study was conducted qualitatively using a descriptive-analytical approach. The collected data was then analyzed by interpreting applicable legal norms, examining the alignment between theory and practice, and identifying obstacles in the enforcement of laws against online fraud involving *phishing*. *A conceptual approach* and *a statutory approach* were employed to gain a comprehensive understanding of the issue under investigation. The results of the analysis were then systematically organized to provide conclusions and recommendations that are solution-oriented and practical from a positive law perspective.

4. RESULTS AND DISCUSSION

The research results indicate that online fraud using *phishing* has increased significantly alongside the development of digital technology and the rise in electronic transactions within society. This criminal pattern is no longer simple but has evolved into a more systematic and organized form. Perpetrators exploit digital security vulnerabilities and the public's low digital literacy in recognizing cyber threats. In this context, victims often do not realize they are being targeted by digital manipulation. This highlights a disparity between technological advancements and the public's readiness to address them [13]. This condition is one of the primary factors affecting the effectiveness of law enforcement.

From a positive law perspective, regulations regarding online fraud have actually been accommodated through various provisions in the Criminal Code (KUHP) and the Information and Electronic Transactions Law (UU ITE). However, research findings indicate that existing legal norms have not fully addressed the complexity of *phishing* methods. This is due to the dynamic and ever-evolving nature of the crime, which keeps pace with technological innovations. Additionally, there is a legal gap in specifically regulating the digital manipulation techniques used by perpetrators. Consequently, law enforcement officials often face difficulties in accurately classifying the perpetrators' actions [14]. This situation results in the weak effectiveness of law enforcement against such crimes.

From a substantive legal perspective, it has been found that there is a lack of alignment among several laws and regulations governing cybercrime. For example, there are differences in the interpretation of the elements of the criminal offense of fraud in the Criminal Code (KUHP) compared to the provisions in the ITE Law. This inconsistency leads to multiple interpretations in the application of the law in practice. Additionally, the absence of specific regulations comprehensively addressing *phishing* poses a distinct obstacle. This indicates that legal reform is urgently needed to align with the evolution of digital crimes [15]. Without such reforms, law enforcement will continue to face normative challenges.

From a legal structural perspective, this study found that the capacity of law enforcement officials remains the primary obstacle in handling *phishing* cases. The limited availability of human resources with expertise in information technology and digital forensics results in suboptimal investigative processes. Additionally, inadequate facilities and infrastructure also slow down the process of collecting digital evidence. In some cases, law enforcement officials also face difficulties in tracking perpetrators who use anonymous identities. These conditions highlight that institutional capacity building is an urgent necessity [16]. Without such support, law enforcement cannot operate effectively.

Furthermore, structural barriers are evident in the lack of coordination among law enforcement agencies. Handling *phishing* cases often involves various institutions, such as the police, the prosecutor's office, and other relevant agencies. However, suboptimal coordination leads to overlapping jurisdictions and delays in case processing. This results in a low-resolution rate for cybercrime cases. In this context, a

more integrated and systematic coordination mechanism is required. Synergy among agencies is key to enhancing the effectiveness of law enforcement [17].

From a legal culture perspective, this study indicates that public awareness of *phishing* threats remains relatively low. Many people do not understand how these schemes operate, making them easy targets. Additionally, the culture of carelessly sharing personal information further increases the risk of online fraud. A lack of education and digital literacy are the primary factors contributing to this situation. From a legal perspective, the public's legal culture plays a crucial role in supporting the effectiveness of law enforcement. Therefore, raising public awareness is a strategic step that must be taken [18].

Research findings also indicate that the evidentiary process in *phishing* cases presents a high level of difficulty. This is due to the nature of digital evidence, which is easily manipulated and deleted. Furthermore, digital traces scattered across various systems and jurisdictions pose a unique challenge during the investigative process. Law enforcement officials must possess adequate technical capabilities to identify and secure digital evidence. Without such capabilities, the evidentiary process will be weak and could potentially lead to the dismissal of cases in court. This underscores the importance of strengthening digital forensic capabilities [19].

In practice, many *phishing* cases are not reported by victims to law enforcement. This is due to various factors, such as shame, lack of knowledge, and a lack of trust in the legal system. Consequently, data on *phishing* crimes becomes inaccurate and difficult to analyze comprehensively. This low reporting rate also makes it difficult to identify crime patterns comprehensively. In this context, efforts are needed to increase public trust in law enforcement. Transparency and accountability are key factors in building that trust [20].

This study also found that *phishers* often exploit security vulnerabilities in digital platforms. This indicates that technology plays a crucial role in preventing cybercrime. Digital service providers need to enhance their security systems to protect user data. Furthermore, collaboration between the government and the private sector is essential in creating a secure digital ecosystem. This collaborative approach can strengthen prevention and law enforcement efforts. Thus, addressing *phishing* is not solely the responsibility of law enforcement agencies [21].

From a comparative perspective, several countries have developed specific regulations to address *phishing* crimes. These regulations include clear definitions, effective law enforcement mechanisms, and strong international cooperation. This indicates that Indonesia needs to learn from best practices implemented in other countries. Legal harmonization is a crucial step in addressing cross-border cybercrime. Without international cooperation, law enforcement will face jurisdictional limitations. Therefore, a global approach is essential [22].

Furthermore, research findings indicate that the use of *artificial intelligence* technology can assist in detecting and preventing *phishing* attacks. This technology is capable of identifying attack patterns and providing early warnings to users. However, the implementation of such technology remains limited in Indonesia. This is due to cost factors and infrastructure limitations. Therefore, greater investment is needed in the development of digital security technology. Technological innovation can serve as a solution to address the limitations of conventional law enforcement [23].

In relation to the research objectives, it can be concluded that the obstacles to law enforcement against *phishing* are multidimensional. These obstacles stem not only from legal aspects but also from technological and social aspects. Therefore, the approach used in addressing this crime must be holistic. Integration between regulations, law enforcement capacity, and public awareness is the key to success. Without a comprehensive approach, law enforcement efforts will continue to face

obstacles. This underscores the importance of ongoing legal reform.

This study also reveals that the criminal justice system is not yet fully prepared to address the challenges of cybercrime. Conventional judicial processes often fail to accommodate the requirements of digital evidence. Additionally, the lack of judges with a deep understanding of information technology poses a challenge during trials. This has the potential to affect the quality of court rulings. Therefore, enhancing the capacity of judicial officials is an urgent need. Specialized education and training must be provided to improve these competencies [24].

From a policy perspective, the government has undertaken various efforts to improve cybersecurity, such as establishing specialized agencies and formulating a national cybersecurity strategy. However, the implementation of these policies remains suboptimal. This is due to a lack of coordination and limited resources. Furthermore, existing policies have not been fully integrated into the law enforcement system. Therefore, an evaluation of existing policies is necessary. Policy improvements are a crucial step in enhancing the effectiveness of law enforcement [25].

Research findings also indicate that public education is one of the most effective preventive measures in reducing *phishing* incidents. Digital literacy programs need to be enhanced to provide the public with an understanding of the risks and methods of preventing cybercrime. Additionally, public awareness campaigns can be utilized to raise public awareness. This preventive approach can reduce the burden on law enforcement agencies. Thus, the handling of crime is not merely repressive but also preventive. This aligns with modern legal principles that prioritize prevention.

In the context of legal enforcement theory, the findings of this study align with Soerjono Soekanto's view that the effectiveness of the law is influenced by five main factors. These five factors are interrelated and inseparable. In the case *of phishing*, these five factors clearly influence the success of law enforcement. Therefore, the approach used must consider all these factors. A partial analysis will not be able to provide a comprehensive solution. This highlights the importance of a multidisciplinary approach in legal research [26].

This study also compares its findings with previous research, revealing commonalities in the challenges of enforcing laws against cybercrime. However, this study offers a new perspective by emphasizing the integration of law and technology. This approach provides a more comprehensive understanding of the existing issues. Furthermore, this study highlights the importance of international cooperation in addressing *phishing* crimes. This serves as a significant addition compared to previous research. Thus, this study makes a substantial contribution to the development of legal science.

Furthermore, this study finds that legal reform is an inevitable step in addressing the evolution of cybercrime. Regulatory updates are necessary to align with technological advancements. Additionally, existing regulations need to be simplified to ensure they are easily understood and implemented. Legal reform must also be accompanied by capacity building for law enforcement officials. Without comprehensive reform, law enforcement will continue to face obstacles. This underscores the importance of the government's commitment to legal reform.

In terms of implementation, research findings indicate that law enforcement regarding *phishing* remains reactive. Law enforcement agencies tend to act only after a crime has occurred. This approach is considered ineffective in addressing rapidly evolving cybercrimes. Therefore, a proactive approach capable of preventing crimes is necessary. This can be achieved through regular monitoring of digital systems. Consequently, law enforcement can be carried out more effectively.

This study also highlights the importance of the private sector's role in

addressing *phishing* crimes. Technology companies play a strategic role in protecting user data. Additionally, they can assist law enforcement agencies in the investigative process. Collaboration between the public and private sectors is key to achieving cybersecurity. Without such collaboration, law enforcement efforts will be limited. Therefore, collaboration is of utmost importance.

From a human rights perspective, law enforcement regarding *phishing* must also prioritize the protection of users' privacy rights. The use of technology in investigations must be proportional and in accordance with legal provisions. This is crucial to prevent human rights violations. Law enforcement that disregards this aspect may create new problems. Therefore, a balance between security and privacy must be maintained. This presents a unique challenge in the digital age.

Research findings also indicate that globalization influences the patterns of *phishing* crimes. Perpetrators can operate across national borders without geographical constraints. This complicates law enforcement processes, which remain based on national jurisdictions. Therefore, international cooperation is crucial in addressing this crime. International agreements and cooperation between nations can assist in extradition and information-sharing processes. Without such cooperation, it would be difficult to apprehend perpetrators. This underscores the importance of a global approach.

In terms of evidence, the use of electronic evidence is crucial in *phishing* cases. However, the validity and admissibility of such evidence are often debated in court. This is due to a lack of understanding of digital technology. Therefore, clear guidelines regarding the use of electronic evidence are needed. These guidelines can assist judges in making decisions. Consequently, the judicial process can proceed more effectively.

This study also found that training and education for law enforcement officials are essential. This is to enhance their ability to handle cybercrimes. Additionally, the legal education curriculum must be updated to include material related to cyber law. Consequently, future generations of law enforcement officials will possess adequate competencies. This represents a long-term investment in law enforcement. Without adequate education, law enforcement will fall behind.

Furthermore, this study indicates that a multidisciplinary approach is essential in addressing *phishing* crimes. Law cannot stand alone without the support of other disciplines such as information technology and criminology. Therefore, interdisciplinary collaboration is crucial. This approach can provide more comprehensive solutions. Moreover, interdisciplinary research can enrich legal studies. This underscores the importance of integrating knowledge across disciplines.

This study also identified that one of the main obstacles is the slow pace of the legislative process in responding to technological developments. The lengthy process of drafting laws often results in regulations lagging behind. This creates opportunities for criminals to exploit legal loopholes. Therefore, a more responsive legislative mechanism is needed. Legal updates must be implemented quickly and accurately. This poses a challenge for policymakers.

From an economic perspective, *phishing* crimes cause significant losses to society and the state. These losses are not only material but also impact trust in digital systems. Low trust can hinder the development of the digital economy. Therefore, effective law enforcement is crucial. This is to maintain the stability of the digital economy. Thus, law enforcement plays a strategic role in economic development.

This study also indicates that the media plays a vital role in raising public awareness about *phishing* crimes. Information disseminated through the media can help the public understand existing risks. Additionally, the media can serve as an effective educational tool. Consequently,

collaboration between the government and the media must be strengthened. Mass public awareness campaigns can be conducted to enhance public awareness. This forms part of preventive efforts.

From a philosophical perspective, law enforcement against *phishing* reflects the state's efforts to protect the public from the threat of digital crime. This aligns with the state's function as a protector of its citizens. However, such protection must be carried out fairly and proportionally. Excessive law enforcement can lead to rights violations. Therefore, balance is crucial. This highlights the complexity of law enforcement in the digital age.

Overall, the results of this study indicate that the obstacles to law enforcement against online fraud via *phishing* are complex and multidimensional. Therefore, a comprehensive and integrated approach is required. Legal reform, capacity building for law enforcement officials, and increased public awareness are the primary steps that must be taken. Additionally, international cooperation is also a key factor. Thus, law enforcement can operate more effectively.

Finally, this study emphasizes that law enforcement against *phishing* crimes cannot be carried out in isolation. Synergy among various parties is required to create an effective system. The approach used must be adaptive to technological developments. Thus, the law can remain relevant in facing the challenges of the times. It is hoped that this study can contribute to the development of cyber law in Indonesia.

5. CONCLUSION

Based on the research findings and discussion, it can be concluded that law enforcement against online fraud using *phishing* methods, from the perspective of positive law in Indonesia, still faces various multidimensional obstacles, encompassing legal substance, law enforcement structure, and the legal culture of society. From a substantive perspective, existing regulations have not fully accommodated the dynamic and technology-based evolution of *phishing* crime methods, leading to legal gaps and ambiguity in legal norms. From a structural perspective, limitations in human resources, infrastructure, and weak coordination among law enforcement agencies constitute major obstacles in the investigative and evidentiary processes. Meanwhile, from the legal culture perspective, low digital literacy and public awareness of cybercrime risks further increase the potential for *phishing* offenses. Thus, the research objective to identify barriers and analyze the effectiveness of law enforcement has been addressed: law enforcement against *phishing* is not yet functioning optimally and requires a more comprehensive, integrative, and adaptive approach to advancements in information technology.

Based on the findings of this study, the following recommendations can be made: there is a need for responsive legal reform through regulatory updates that specifically address *phishing* crimes, as well as harmonization among relevant laws and regulations. Additionally, there is a need to enhance the capacity of law enforcement officials through education and training in information technology and digital forensics, as well as strengthening the infrastructure and resources supporting law enforcement. The government must also improve public digital literacy through systematic and sustainable educational programs to foster a stronger legal culture. On the other hand, strengthening cooperation between the government, the private sector, and the international community is a strategic step in addressing the cross-border nature of *phishing* crimes. With the implementation of these measures, it is hoped that law enforcement against online fraud can be more effective, providing optimal legal protection for the public, and supporting the creation of a safe and trustworthy digital ecosystem.

REFERENCES

[1] D. Anjheli, "Digital Privacy and Phishing Crimes in Indonesia: A Critical Evaluation of the Effectiveness of the ITE Law and the PDP Law," *Staatsr. J. Const. Law Islam. Polit.*, vol. 4, no. 1, pp. 165–189, 2024, doi: 10.14421/990epf27.

[2] M. D. Saifullah and A. Pramono, "Law Enforcement of Online Fraud Crimes: A Study on the Implementation of the ITE Law in Indonesia," *J. Magister Huk. Perspekt.*, vol. 16, no. 2, pp. 130–140, 2025, [Online]. Available: https://magister.wisnuwardhana.ac.id/index.php/Perspektif/article/download/127/110

[3] E. Satoto and F. Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption," *Greenation Int. J. Law Soc. Sci.*, vol. 3, no. 2, pp. 309–317, 2025, doi: 10.38035/gijlss.v3i2.425.

[4] O. Puhi, R. M. Moonti, Y. Kadir, and S. Pakaya, "The Application of Article 22 of the Regulation of the Head of the Indonesian National Police Force Number 14 of 2011 Concerning the Code of Ethics of the Indonesian National Police Profession," *IBLAM Law Rev.*, vol. 3, no. 2, pp. 89–108, 2023, doi: 10.52249/ilr.v3i2.131.

[5] Y. Yahman, "Understanding Law Enforcement in the Perspective of Expediency and Justice," *IUS POSITUM J. Law Theory Law Enforc.*, vol. 3, no. 1, pp. 26–34, 2024, doi: 10.56943/jlte.v3i1.468.

[6] A. Wisnubroto and H. Tegnan, "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States," *J. Hum. Rights, Cult. Leg. Syst.*, vol. 5, no. 2, pp. 630–658, 2025, doi: 10.53955/jhcls.v5i2.606.

[7] M. N. Trisolvena and N. H. Saputra, "Phishing cyber security threats," *J. Improsci*, vol. 2, no. 1, pp. 38–48, 2024, doi: 10.62885/improsci.v2i1.440.

[8] R. M. P. Sari, "Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia," *J. Huk. dan Keadilan*, vol. 2, no. 5, pp. 49–55, 2025, doi: 10.61942/jhk.v2i5.418.

[9] R. of I. Ministry of Communication and Information Technology and K. I. Center, "Status Literasi Digital Indonesia 2022," 2022. [Online]. Available: https://data.komdigi.go.id/opendata/dataset/indeks-literasi-digital-indonesia-tahun-2021-2022

[10] Purwadi, M. Makhfud, and A. Jamaludin, "Legal Accountability and Policy Gaps in Social Engineering-Based Phishing Cybercrimes," *Res. Horiz.*, vol. 5, no. 3, pp. 797–806, 2025, doi: 10.54518/rh.5.3.2025.580.

[11] H. N. Fakhouri, M. A. AlSharaiah, M. Alkalaileh, and F. F. Dweikat, "Overview of challenges faced by digital forensics," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, 2024, pp. 1–8. doi: 10.1109/ICCR61006.2024.10532850.

[12] M. Candrasari and A. Adhari, "The Urgency of Developing an Ideal Model for Law Enforcement Against Copyright Infringement in the Digital Age," *Kertha Semaya J. Leg. Sci.*, vol. 13, no. 9, pp. 2071–2087, 2025, [Online]. Available: https://ejournal3.unud.ac.id/index.php/kerthasemaya/article/download/1416/573

[13] I. Yurita, M. K. Ramadhan, and M. Candra, "The Impact of Technological Advancements on the Development of Cybercrime (A Case Study of Phishing as a Digital Security Threat)," *J. Huk. Leg.*, vol. 5, no. 2, pp. 143–155, 2023, [Online]. Available: https://jurnal.umko.ac.id/index.php/legalita/article/download/995/407

[14] F. E. Muhammad and B. Harefa, "Criminal Regulations for Perpetrators of Web-Based Phishing Fraud," *USM Law Rev. J.*, vol. 6, no. 1, pp. 226–241, 2023, doi: 10.26623/julr.v6i1.6649.

[15] H. W. Ong, W. Afdal, and Tantimin, "A Comparison of Sanctions for Artificial Intelligence-Based Online Fraud: Indonesia vs. the United States," *to-ra Law J. Law to Regul. Prot. Soc.*, vol. 11, no. 2, pp. 448–464, 2025, doi: 10.55809/tora.v11i2.579.

[16] A. L. Sariani, "The Effectiveness of Law Enforcement Against Cybercrime in Indonesia," *AL-DALIL J. Soc. Polit. Leg. Sci.*, vol. 3, no. 1, pp. 54–62, 2025, [Online]. Available: https://ejournal.indrainstitute.id/index.php/al-dalil/article/download/824/655

[17] A. M. Matondang, "Criminal Law Policies on Cybercrime: A Comparative Study Between Indonesia and Thailand from an International Law Perspective," *Lex Gen. Law J.*, vol. 6, no. 1, 2025, [Online]. Available: https://ojs.rewangrencang.com/index.php/JHLG/article/download/994/520

[18] B. D. Hartanto, T. A. Nugraha, B. R. Ramadhan, M. A. Pratama, and R. P. Alamsyah, "Digital Security Education to Enhance Public Awareness of Phishing Links," *J. Soc. Serv.*, vol. 2, no. 9, pp. 4341–4346, 2025, [Online]. Available: https://ejournal.jurnalpengabdiansosial.com/index.php/jps/article/download/875/741

[19] N. Allah Rakha, "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations," *Mex. Law Rev.*, vol. 16, no. 2, pp. 23–54, 2024, doi: 10.22201/iij.24485306e.2024.2.18892.

[20] Y. Kwak, S. Lee, A. Damiano, and A. Vishwanath, "Why do users not report spear phishing emails?," *Telemat. Informatics*, vol. 48, p. 101343, 2020, doi: 10.1016/j.tele.2020.101343.

[21] F. A. Permana and A. Jamaludin, "Personal data vulnerability in the digital era: A study of modus operandi and mechanisms to prevent phishing crimes," *Al-Hakim J. Student Sci. Journal, Sharia Stud. Law, Philanthr.*, vol. 5, no. 2, pp. 201–216, 2023, doi: 10.22515/jurnalalhakim.v5i2.7074.

[22] M. T. Rusydi, "Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats," *J. Progress. Law Leg. Stud.*, vol. 3, no. 01, pp. 69–85, 2025, doi: 10.59653/jplls.v3i01.1365.

[23] Y. Y. Santika, R. Rianto, and E. I. H. Ujianto, "A Comprehensive Study on Cybersecurity: A Comparison of AI Technology with Non-AI Systems in Threat Detection and Prevention," *J. Komtika (Computing Informatics)*, vol. 9, no. 1, pp. 45–64, 2025, doi: 10.31603/komtika.v9i1.13149.

[24] R. S. Billah and H. Saragih, "The Application of Electronic Evidence in Cybercrimes (Case Study of Judgment No. 616/Pid. Sus/2023/Pn Jkt. Sel)," *Arus J. Soc. Sci. Humanit.*, vol. 5, no. 2, pp. 2739–2747, 2025, [Online]. Available: https://jurnal.ardenjaya.com/index.php/ajsh/article/download/1543/1011

[25] E. Winarno *et al.*, "Cybersecurity Education for Students to Create a Digital Safe School at SMP Muhammadiyah Tahfizh Salatiga," *J. Community Serv.*, vol. 5, no. 1, pp. 661–671, 2026, [Online]. Available: https://jurnaluniv45sby.ac.id/index.php/ABDIMAS45/article/download/6193/4636

[26] H. Haeril, R. Renggong, and Y. A. Hasan, "Implementation of the Functions of the South Sulawesi Regional Water Police Directorate in the Enforcement of Illegal Fishing Crimes in the Waters of South Sulawesi," *Indones. J. Leg. Law*, vol. 5, no. 2, pp. 454–461, 2023, doi: 10.35965/ijlf.v5i2.2623.