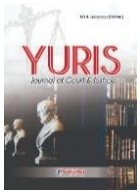

ISSN 2809-672X (Online)
**YURIS: Journal of Court and Justice**
https://journal.jfpublisher.com/index.php/jcj
Vol. 3 Issue 4 (2024)
doi.org/10.56943/jcj.v3i4.802

# Enforcement of Laws Against the Sale of Phishing Links for the Purpose of Personal Data Theft Based on the ITE Law

**Hollanda Putri Irawati[1]*, Kunarso[2],**
[1]hollandairawati@gmail.com, [2]kunarso@ubhara.ac.id
Universitas Bhayangkara Surabaya

*Corresponding Author: Hollanda Putri Irawati
Email: hollandairawati@gmail.com

## ABSTRACT

*The rapid growth of cybercrime poses significant threats to personal data security, with phishing emerging as one of the most common methods. Phishing involves tricking individuals into revealing confidential information, and a concerning development is the creation and sale of phishing links to facilitate personal data theft. This situation raises legal questions regarding the sufficiency of current regulations to address such acts. This study aims to examine the legal framework governing the buying and selling of phishing links and to assess law enforcement efforts in handling these activities. The research applies a normative juridical method, combining statutory and conceptual approaches, and relies on the analysis of legislation and relevant legal literature. The study finds that phishing link sellers may be prosecuted under Article 34 paragraph (1) letter a in conjunction with Article 50, as well as Article 35 in conjunction with Article 51 paragraph (1) of the ITE Law. Phishing link buyers can be charged under Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the ITE Law and Article 65 paragraph (1) in conjunction with Article 67 paragraph (1) of the Personal Data Protection Law. Nonetheless, these provisions remain insufficient, as they do not explicitly regulate the sale of phishing links and leave room for multiple interpretations. Law enforcement involves preventive actions through public and institutional collaboration and repressive measures through the imposition of criminal penalties.*

**Keywords:** *Buying and Selling, Law Enforcement, Personal Data, Phising*

## INTRODUCTION

Human civilization and technological development are inextricably linked. Humans use their intellect to solve problems. This is the root of technological development.[1] Humans continually innovate to make their lives easier. With the contributions of experts and industrialists, these innovations have led to rapid technological advancements.[2] One clear example of this is the impact we feel in our daily lives from the development of information and communication technology.

Information and communication technology has brought about numerous positive impacts on human life, including the emergence of cashless payment systems, electronic commerce (e-commerce), and the convenience of mobile banking, which allows banking transactions to be carried out via mobile phones.[3] These technologies have made transactions easier and more efficient, allowing for quick and secure purchases.[4] Other positive impacts include the easy dissemination of information, the development of learning facilities, and many more. However, it is crucial to be aware that technology also has the potential to cause negative impacts, and caution should be exercised.

The misuse of information and communication technology can be referred to as cybercrime. One form of cybercrime is the targeting of public data, resulting in data leaks. In line with this, there is a type of cybercrime known as phishing.[5]

Phishing is an activity to lure (obtain) information. The information targeted can be social media accounts, emails, personal data, and the like. Phishers (people who engage in phishing) will create a fake web page that resembles the original page as closely as possible.[6] One report states that 32% of data theft is carried out using phishing methods. In fact, at the beginning of 2020, the Anti-Phishing Working Group recorded 165,772 phishing sites, with the financial sector being the main target of these attacks.[7] This is what happened to Irwan Gema, a resident of

[1] Muhamad Ngafifi, "KEMAJUAN TEKNOLOGI DAN POLA HIDUP MANUSIA DALAM PERSPEKTIF SOSIAL BUDAYA," *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi* 2, no. 1 (June 2014).
[2] Pablo D'Este et al., "Inventors and Entrepreneurs in Academia: What Types of Skills and Experience Matter?," *SSRN Electronic Journal* (2011), http://www.ssrn.com/abstract=1951845.
[3] Llysselie Gay Querol Leiva, "Impact of Information and Communication Technologies on Everyday Life," *Management (Montevideo)* 3 (February 8, 2025): 130, https://managment.ageditor.uy/index.php/managment/article/view/130.
[4] Md Arif Hassan, Zarina Shukur, and Mohammad Kamrul Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," *Computers* 9, no. 3 (August 27, 2020): 66, https://www.mdpi.com/2073-431X/9/3/66.
[5] Adam Kavon Ghazi-Tehrani and Henry N. Pontell, "Phishing Evolves: Analyzing the Enduring Cybercrime," *Victims & Offenders* 16, no. 3 (April 3, 2021): 316–342, https://www.tandfonline.com/doi/full/10.1080/15564886.2020.1829224.
[6] Efvy Zam, *Phishing : Teknik Mudah Penyadapan Password Dan Pencegahannya* (Jakarta: Mediakita, 2014).
[7] Irfan Fanasafa, "Waspada Kejahatan Phising Mengintai Anda," *Website DJKN*.

Kojen, Malang City. He lost Rp 549 million after clicking on a link to a PDF file that he received via WhatsApp.[8]

What is even more distressing is that there are individuals who abuse their skills in information and communication technology by creating phishing links for sale, which are then used to commit crimes by irresponsible individuals or groups.[9] On August 28, 2023, an individual who created and sold phishing links was apprehended in Sungai Raya Subdistrict, Kubu Raya Regency, West Kalimantan, by the Cybercrime Division of the Special Crimes Investigation Directorate of the Jakarta Metropolitan Police. The suspect, identified as AV alias ERR alias R, was 25 years old at the time. The suspect created a fake website mimicking one of the banks, which included a customer data entry form. The phishing links created by the suspect were sold at prices ranging from 100,000 to 500,000 rupiah. Since May 2023, the suspect has successfully sold 60 phishing links, earning profits ranging from 17 million to 20 million rupiah. The swift action of law enforcement has led to the apprehension of the suspect, ensuring the safety of the public.

These phenomena show that the development of crimes using information and communication technology is becoming increasingly diverse.[10] When discussing cybercrime cases, standardization and harmonization are needed in three areas, namely "legislation, criminal enforcement, and judicial review" as an effort to enforce the law and achieve justice.[11]

In Indonesia, crimes involving the use of ICT or cybercrime are regulated explicitly in the ITE Law. This law, which first came into effect in 2008, has shown its adaptability to changing technological landscapes through two amendments, the first in 2016 and the second in 2024. Meanwhile, regulations related to personal data are contained in Law No. 27 of 2022 on Personal Data Protection.

Despite the existence of regulations in Indonesian positive law regarding cybercrime that can endanger personal data, particularly related to phishing, such as Article 35 in conjunction with Article 51(1) of the ITE Law, which is often used to prosecute phishing offenders, the implementation of these regulations requires proper legal interpretation and reasoning. This is due to the lack of clear boundaries that can serve as a reference for prosecuting cybercriminals, underscoring the

[8] Muhammad Aminudin, "Lagi! Rekening Nasabah Bank Dibobol Rp 549 Juta Gegara Buka Link .PDF," *Detik Jatim*.
[9] SK Hasane Ahammad et al., "Phishing URL Detection Using Machine Learning Methods," *Advances in Engineering Software* 173 (November 2022): 103288, https://linkinghub.elsevier.com/retrieve/pii/S0965997822001892.
[10] Rapuluchukwu Ernest Nduka and Vinesh Basdeo, "The Need for Harmonised and Specialised Global Legislation to Address the Growing Spectre of Cybercrime," *Southern African Public Law* 36, no. 2 (January 28, 2022), https://unisapressjournals.co.za/index.php/SAPL/article/view/8112.
[11] Edmon Makari, "Informasi Hukum Untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem Dan Komunikasi Elektronik Global," *Jurnal Ketahanan Nasional* (2014): 77.

urgent need for legal reform.[12] This is also due to the evolving motives and models of cybercrime.

## LITERATURE REVIEW

### Legal Protection Theory

Philipus M. Hadjon contributed his thoughts on the theory of legal protection. He stated that, "Legal protection is the state's commitment to safeguarding the dignity and honor of individuals. It recognizes the human rights possessed by legal subjects based on legal provisions, thereby preventing arbitrariness and ensuring fairness. This guarantee, provided by the state, ensures that all parties can exercise their legal rights and interests in their capacity as legal subjects."[13]

Not only did he provide his opinion on the definition of legal protection, he also stated that legal protection can be divided into two types: preventive protection, which protects the community so that it can continue to contribute by actively providing input on every decision made by the government; and repressive protection, a crucial role of the state, which is provided to all its citizens ensuring they receive their rights as subjects of law, thereby fostering a sense of security and protection.[14]

Another legal expert, Satjipto Rahardjo, also has his own opinion regarding the definition of legal protection. He emphasizes that, "Legal protection refers to the provision of protection for human rights that have been violated. This protection is provided to the community, ensuring they can fully enjoy all the rights granted by law. The law's adaptability, a key feature that enables it to evolve and respond to changing circumstances, along with its flexibility, predictability, and anticipatory nature, makes it a relevant and effective tool in safeguarding human rights."[15][16]

### Legal Certainty Theory

Legal certainty is an axiological aspect that legal positivism strives for.[17] Based on formal sources of law, such as legislation, they believe that it is not impossible to achieve. The principle that underpins legal certainty is the principle

---

[12] Yazid Haikal Lokapala, Fuad Januar Nurfauzi, and Yeni Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (June 11, 2024), https://journal.umy.ac.id/index.php/ijclc/article/view/19853.

[13] Philipus M Hadjon, *Pengantar Hukum Administrasi Indonesia*, 10th ed. (Yogyakarta: Gadjah Mada University Press, 2008).

[14] "Teori-Teori Perlindungan Hukum Menurut Para Ahli," *Hukum Online*.

[15] Fokky Fuad, Istiqomah Istiqomah, and Suparji Achmad, "DIALEKTIKA PERLINDUNGAN HUKUM BAGI GURU DALAM MENDISIPLINKAN SISWA DI SEKOLAH," *Indonesian Journal of Law and Policy Studies* 1, no. 1 (May 2020): 55–64.

[16] Satjipto Rahardjo, *Ilmu Hukum*, 8th ed. (Bandung: PT Citra Aditya Bakti, 2014).

[17] Sukirno, Edy Lisdiyono, and Sri Mulyani, "Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website," *International Journal of Criminology and Sociology* 10 (April 26, 2021): 891–896, https://lifescienceglobal.com/pms/index.php/ijcs/article/view/7427.

of legality. Von Feuerbach formulated this principle in the adage: "No punishment without law, no punishment without crime, no crime without punishment (nulla poena sine lege, nulla poena sine crimine, nullum crimen sine poena)."[18]

Peter Mahmud expressed the opinion that legal certainty has two meanings. He stated that, "Legal certainty, with its dual meanings, is underpinned by the existence of general rules. These rules empower individuals, including law students and legal professionals, by clearly delineating permissible and impermissible actions. They also provide a sense of legal security, ensuring that individuals are protected from government arbitrariness. This understanding of legal certainty extends beyond the provisions in laws, encompassing the consistency in judicial decisions between one judge's ruling and another's on similar cases."[19]

**Law Enforcement Theory**

Regarding the theory of law enforcement, Jimly Asshiddiqie defines it as a process of upholding norms and maintaining social order. He states that, "Law enforcement is the process of enforcing or implementing legal norms as guidelines for behavior in traffic or legal relationships in social and state life."[20]

Unlike Jimly Asshiddiqie, Satjipto Rahardjo also has his definition of law enforcement. According to Satjipto Rahardjo, law enforcement is defined as: "Law enforcement is a series of processes that interpret values, ideas, and ideals, which are often abstract, and are the objectives of the law."[21]

**Sale and Purchase**

Buying and selling is a mutual agreement between a buyer and a seller. The seller is obligated to transfer ownership rights of the goods they own to the buyer, and the buyer is obligated to pay the seller the agreed-upon price for the goods.[22] Goods and price are the main elements in this mutual agreement of buying and selling.

**Phising**

The United States Computer Emergency Readiness Team (US-CERT) defines phishing as a form of social engineering that uses malicious emails or

[18] Shidarta, *Hukum Penalaran Dan Penalaran Hukum*, 1st ed. (Genta Publishing, 2013).
[19] Prof. Dr. Peter Mahmud Marzuki, *Pengantar Ilmu Hukum*, Revisi. (Jakarta: KENCANA, 2017).
[20] Laurensius Arliman, "MEWUJUDKAN PENEGAKAN HUKUM YANG BAIK UNTUK MEWUJUDKAN INDONESIA SEBAGAI NEGARA HUKUM," *Doctrinal* 2, no. 2 (June 2020): 509–532.
[21] Satjipto Rahardjo, *Penegakan Hukum: Suatu Tinjauan Sosiologis* (Yogyakarta: Genta Publishing, 2009).
[22] Yulvita Ratna and Gunawan Djajaputra, "LEGAL LIABILITY OF PROPERTY DEVELOPERS REGARDING THE FULFILLMENT OF OBLIGATIONS TO CONSUMERS IN SALE AND PURCHASE TRANSACTIONS USING THE BINDING SALE AND PURCHASE AGREEMENT," *Awang Long Law Review* 6, no. 2 (May 31, 2024): 453–459, https://ijsshr.in/v5i8/66.php.

websites to request personal information from individuals or companies by posing as a trusted organization or entity.[23]

**Personal Data Theft**

The negative impact of technological advances is the rise in cases of personal data theft. Personal data theft can be defined as the illegal act of accessing or obtaining another person's personal data.[24] Cases of personal data theft that attract public attention and cause significant losses to victims are those involving electronic systems.[25] The losses caused by personal data theft are generally not minor. This is because the illegally obtained personal data can be used to commit a wide range of other crimes, such as bank account hacking, applying for online loans that are not paid back, human trafficking, extortion, and more, highlighting the severity and complexity of the issue.

## RESEARCH METHODOLOGY

To complete the writing of this thesis, researchers employed normative juridical research, which involves examining or studying the implementation of rules or norms in positive law[26], especially those related to buying and selling phishing links for personal data theft. The approach used is a statutory approach and a conceptual approach. The process of collecting legal materials for this research is carried out meticulously, leaving no stone unturned, by examining all relevant legislation and legal literature related to buying and selling phishing links for personal data theft.

## RESULT AND DISCUSSION

**Legal Instruments for Selling Phishing Links for Personal Data Theft Modes**

To ensnare phishers, law enforcement officials use articles in the ITE Law as lex specialis. The article often used by law enforcement officials to ensnare phishers is Article 35, Jo Article 51, paragraph (1) of the ITE Law. This article is also one of the articles used by the police to ensnare AV (phishing link seller).

The seller of phishing links fulfills the elements in Article 35 of the ITE Law; however, the fulfillment of these elements is limited to the act of creating phishing links, and Article 35 of the ITE Law has not yet addressed the act of selling phishing links. Meanwhile, the buyer of the phishing link certainly does not fulfill the

[23] Zainab Alkhalil et al., "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science* 3 (March 2021): 563060.
[24] Yury A. Kuzmin, "IDENTITY THEFT (CRIMINOLOGICAL ASPECT)," *Oeconomia et Jus*, no. 3 (September 28, 2020): 48–57, http://oecomia-et-jus.ru/en/en-singlenum/.
[25] Ekaterina Ryazanova, "Responsibility for the Dissemination of Personal Data as a Way to Counteract Offenses in the Field of Information and Communication Technologies," *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia* 2022, no. 3 (October 3, 2022): 118–123, http://vestnikspbmvd.ru/en/nauka/article/48998/view.
[26] Dr. Johnny Ibrahim, *Teori & Metodologi Penelitian Hukum Normatif* (Bayu Media, 2013).

elements in Article 35 of the ITE Law because they do not participate in creating the link; instead, they directly buy it from the phishing link maker, thereby exposing themselves to the serious legal consequences of their actions.

Article 35 of the ITE Law, which only covers the act of creating phishing links, does not extend to their sale. This necessitates the need for additional legal norms to ensnare the seller of phishing links, specifically Article 34 paragraph (1) letter a of the ITE Law, which explicitly mentions the act of selling. The question then arises: can the object being sold (phishing link) be deemed to fulfill the elements in letter a, specifically, can the phishing link be considered as software?.

Of the several types of software, some are related to links, namely internet software and one type is the Web Browser which is used to access or display various websites while links are access to the web.[27] So, phishing links that connect to the web indirectly can be categorized as software.

According to this description, phishing link sellers can be charged with Article 34, paragraph (1), letter a, of the ITE Law and Article 35, paragraph (1), of the ITE Law, even though the articles do not explicitly regulate the act of selling phishing links. The article contains elements that can lead to multiple interpretations. It is crucial to thoroughly examine whether the phishing link maker, after selling the link, truly cannot or does not access everything related to the link.[28] This examination is of utmost importance as it can significantly impact the legal implications. There is a possibility that he can access and utilize the information obtained from the link, adding another layer of complexity to the legal analysis.[29]

In the case of buying and selling phishing links, not only can the seller be subject to criminal sanctions, but the buyer may also be held liable. Link buyers must also be held accountable for their actions. Buyers of phishing links can be charged with Article 28, paragraph (1), Article 45A, paragraph (1), of Law No. 19 of 2016, concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, and Article 65, paragraph (1), of the Jo—article 67 paragraph (1) of Law No. 27 of 2022 concerning Personal Data Protection. In addition, it does not rule out the possibility that buyers of phishing links can be charged with other articles. This is because personal data obtained from phishing links can be used to commit other crimes, such as extortion.

[27] Fayyad-Kazan Hasan et al., "Forensic Analysis of Private Browsing Mechanisms: Tracing Internet Activities," *Journal of Forensic Science and Research* 5, no. 1 (March 8, 2021): 012–019, https://www.forensicscijournal.com/articles/jfsr-aid1022.php.
[28] Tommy Chin, Kaiqi Xiong, and Chengbin Hu, "Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking," *IEEE Access* 6 (2018): 42516–42531, https://ieeexplore.ieee.org/document/8387883/.
[29] Emma J Williams and Adam N Joinson, "Developing a Measure of Information Seeking about Phishing," *Journal of Cybersecurity* 6, no. 1 (January 1, 2020), https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyaa001/5748294.

**Law Enforcement on the Case of Buying and Selling Phishing Links for Personal Data Theft Mode**

In Dutch, law enforcement or "law enforecement" has a synonym, namely "*rechts handhaving*". In the Netherlands, *rechts handhaving* consists of preventive (administrative measures with appeals, corrections, and so on) and repressive measures.[30]

In the law enforcement process related to cases of buying and selling phishing links, the Police have the authority to take preventive actions. These actions include: collaborating with relevant stakeholders such as Kominfo and OJK; conducting cyber patrols; being up to date to provide appeals to the public regarding phishing crimes through social media, television, radio, and newspapers; and conducting socialization to the public as a means of education regarding phishing, empowering them to take preventive measures.

In addition to the Police, BSSN can play an active role in enhancing cybersecurity by increasing cybersecurity literacy among all elements, especially in the digital economy, and by building capacity across various sectors to be always ready to face cyber attacks.[31]

Preventive efforts also need to be carried out by the legislative body as the compiler of laws and regulations to form a regulation to establish prohibitions and sanctions (criminal threats).[32] In the case of buying and selling phishing links, there are laws and regulations that can be used in law enforcement efforts, including the ITE Law and the PDP Law. Furthermore, it is imperative that the drafter of laws and regulations continuously monitors the development of related cases, given the rapid development of technology and the potential for crime modes that are also growing rapidly.

Preventing the crime of buying and selling phishing links requires a cautious and thoughtful approach. Always read every message, especially electronic messages, carefully. Be cautious when opening links sent by others, especially from unknown individuals. Do not send sensitive information if you receive a request via email or other platforms before confirming its authenticity. It is crucial to verify requests before sharing sensitive information. Contact the call center of a related agency if there is a suspicious request. Use an antivirus software program, especially one with anti-phishing features. Moreover, do not fill in the username and password request fields at suspicious web addresses.

In terms of law enforcement, some efforts can be made after a criminal offense, also known as repressive efforts. In the realm of criminal law, repressive

[30] Prof. Dr. Romli Atmasasmita, *Hukum Kejahatan Bisnis: Teori & Praktik Di Era Globalisasi*, 1st ed. (Jakarta: KENCANA, 2014).
[31] Akbar Evandio, "Serangan Phising Meningkat, Ini Cara Antisipasinya," *BISNIS TEKNO*.
[32] Shereen Khan et al., "A Systematic Literature Review on Cybercrime Legislation," *F1000Research* 11 (August 23, 2022): 971, https://f1000research.com/articles/11-971/v1.

efforts are carried out through penal means, namely the application of criminal law with criminal sanctions.

The seller of phishing links can be charged with multiple articles, namely Article 34 paragraph (1) letter a Jo Article 50 of the ITE Law and Article 35 Jo 51 paragraph (1) of the ITE Law. The provisions of criminal sanctions in these articles both impose imprisonment and/or fines, so the determination of the maximum punishment is based on Article 65 of the Criminal Code. The way to calculate the maximum punishment is by adding one-third of the heaviest punishment to the heaviest punishment, resulting in a severe consequence that should be approached with utmost caution.[33]

In Article 34 paragraph (1) letter a Jo Article 50 of ITE Law, the criminal sanction imposed is imprisonment for a maximum of 10 years and/or a maximum fine of ten billion rupiah while the criminal sanction contained in Article 35 Jo 51 paragraph (1) of ITE Law is imprisonment for a maximum of 12 years and/or a maximum fine of twelve billion rupiah, so it can be determined that the heaviest criminal sanction is imprisonment for a maximum of 12 years and/or a maximum fine of twelve billion rupiah. Then, the punishment is significantly increased by 1/3 of each of the most severe punishments. The imprisonment that can be charged is 12 years plus (1/3 x 12 years) = 16 years, while the fine that can be charged is Rp 16,000,000,000.00 (sixteen billion rupiah).

Furthermore, buyers of phishing links can be charged with Article 28 paragraph (1) Jo Article 45A paragraph (1) of the ITE Law and Article 65 paragraph (1) Jo Article 67 paragraph (1) of Law No. 27 of 2022 on Personal Data Protection. The provisions of criminal sanctions in these articles both impose imprisonment and/or fines, so the determination of the maximum penalty is also based on Article 65 of the Criminal Code. The calculation of the maximum punishment is the maximum amount that is threatened for each of the acts, but it may not be more severe than the most severe punishment plus one-third.[34]

The criminal sanction imposed under Article 28, paragraph (1), and Article 45A, paragraph (1), of the ITE Law is a serious imprisonment for a maximum of 6 years and/or a significant fine of one billion rupiah. Similarly, the criminal sanction imposed under Article 65, paragraph (1), and Article 67, paragraph (1), of the PDP Law is a grave imprisonment for a maximum of 5 years and/or a substantial fine of five billion rupiah. These penalties carry significant weight. Based on these provisions, the maximum imprisonment that can be charged is 6 years + (1/3 x 6 years) = 8 years, while the fine that can be charged is Rp. 5,000,000,000.00 + (1/3 x Rp. 5,000,000,000.00) = Rp. 5,000,000,000.00 + (1/3 x Rp. 5,000,000,000.00) = Rp. 6,666,666. 666.66 (six billion six hundred sixty-six million six hundred sixty-six rupiah).

[33] Andi Hamzah;, *Asas-Asas Hukum Pidana / Andi Hamzah* (Jakarta: Rineka Cipta, 2008).
[34] Ibid.

According to this description, sellers of phishing links can be sentenced to a maximum imprisonment of 16 years and/or a maximum financial penalty of sixteen billion rupiah. Buyers of phishing links, on the other hand, can face a maximum imprisonment of 8 years and/or a maximum financial penalty of six billion six hundred sixty-six million six hundred sixty-six rupiah. These significant financial penalties underscore the financial impact of the crime.

The act of selling phishing links for the purpose of personal data theft presents unique legal challenges because current regulations under the ITE Law only explicitly address the creation of phishing links rather than their sale. Sellers can be prosecuted under Article 34 paragraph (1) letter a in conjunction with Article 50, as well as Article 35 in conjunction with Article 51 paragraph (1) of the ITE Law. These provisions are applied because phishing links can be interpreted as software that facilitates unlawful access to personal data. Meanwhile, buyers of phishing links may also face legal consequences under Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the ITE Law and Article 65 paragraph (1) in conjunction with Article 67 paragraph (1) of the Personal Data Protection Law, as their actions directly contribute to the misuse of stolen data. However, the absence of explicit regulation regarding the buying and selling of phishing links creates room for multiple interpretations, potentially complicating law enforcement efforts.[35]

Law enforcement in these cases requires a combination of preventive and repressive measures. Preventive measures involve cooperation between government agencies such as the Police, Kominfo, OJK, and BSSN, alongside public awareness efforts including cyber patrols, socialization, and the promotion of cybersecurity literacy.[36] Repressive measures are applied when offenses occur, imposing criminal sanctions on both sellers and buyers. Under current law, phishing link sellers face a maximum of sixteen years of imprisonment and a fine of sixteen billion rupiah, while buyers face a maximum of eight years of imprisonment and a fine of approximately six point six billion rupiah. These penalties reflect the state's commitment to deterring cybercrime while highlighting the urgent need for clearer and more comprehensive legal provisions to address emerging cybercrime patterns.

[35] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."
[36] Anna Makuch, "Raising Public and Private User Awareness of the Threats and Risks Related to Cyberspace Security," *Cybersecurity and Law* 8, no. 2 (December 6, 2022): 44–55, http://www.cybersecurityandlaw.com/Raising-public-and-private-user-awareness-of-the-threats-and-risks-related-to-cyberspace,157123,0,2.html.

## CONCLUSION

Sellers of phishing links can be charged with Article 34 paragraph (1) letter a, Article 50 of the ITE Law, and Article 35 Jo 51 paragraph (1) of the ITE Law. In contrast, buyers of phishing links can be charged under Article 28, paragraph (1), Article 45A, paragraph (1), of the Law on Electronic Information and Transactions, and Article 65, paragraph (1), of the Law. Article 67 paragraph (1) of Law No. 27 of 2022 concerning Protection of Personal Data. In addition, it does not rule out the possibility that buyers and sellers of phishing links can be charged with other articles. This is because personal data obtained from other people using phishing links can be used to commit other crimes, such as extortion.

Law enforcement in tackling cases of buying and selling phishing links can be carried out with preventive efforts carried out by state government agencies such as the Police, Kominfo, OJK, and BSSN. However, it is crucial to emphasize that preventive efforts must also start from each community, underscoring the importance of their involvement. Meanwhile, repressive efforts can be carried out by imposing criminal sanctions on the perpetrators. The maximum imprisonment for sellers of phishing links is 16 years and/or a maximum fine of Rp. 16,000,000,000.00 (sixteen billion rupiah) while the maximum imprisonment for buyers of phishing links is 16 years and/or a maximum fine of Rp. 6,666,666,666.66 (six billion six hundred sixty-six million six hundred sixty-six rupiah).

## REFERENCES

Ahammad, SK Hasane, Sunil D. Kale, Gopal D. Upadhye, Sandeep Dwarkanath Pande, E Venkatesh Babu, Amol V. Dhumane, and Mr. Dilip Kumar Jang Bahadur. "Phishing URL Detection Using Machine Learning Methods." *Advances in Engineering Software* 173 (November 2022): 103288. https://linkinghub.elsevier.com/retrieve/pii/S0965997822001892.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy." *Frontiers in Computer Science* 3 (March 2021): 563060.

Aminudin, Muhammad. "Lagi! Rekening Nasabah Bank Dibobol Rp 549 Juta Gegara Buka Link .PDF." *Detik Jatim*.

Arliman, Laurensius. "MEWUJUDKAN PENEGAKAN HUKUM YANG BAIK UNTUK MEWUJUDKAN INDONESIA SEBAGAI NEGARA HUKUM." *Doctrinal* 2, no. 2 (June 2020): 509–532.

Atmasasmita, Prof. Dr. Romli. *Hukum Kejahatan Bisnis: Teori & Praktik Di Era Globalisasi*. 1st ed. Jakarta: KENCANA, 2014.

Chin, Tommy, Kaiqi Xiong, and Chengbin Hu. "Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking." *IEEE Access* 6 (2018): 42516–42531. https://ieeexplore.ieee.org/document/8387883/.

D'Este, Pablo, Surya Mahdi, Andy D. Neely, and Francesco Rentocchini. "Inventors and Entrepreneurs in Academia: What Types of Skills and

Experience Matter?" *SSRN Electronic Journal* (2011). http://www.ssrn.com/abstract=1951845.

Evandio, Akbar. "Serangan Phising Meningkat, Ini Cara Antisipasinya." *BISNIS TEKNO*.

Fanasafa, Irfan. "Waspada Kejahatan Phising Mengintai Anda." *Website DJKN*.

Fuad, Fokky, Istiqomah Istiqomah, and Suparji Achmad. "DIALEKTIKA PERLINDUNGAN HUKUM BAGI GURU DALAM MENDISIPLINKAN SISWA DI SEKOLAH." *Indonesian Journal of Law and Policy Studies* 1, no. 1 (May 2020): 55–64.

Ghazi-Tehrani, Adam Kavon, and Henry N. Pontell. "Phishing Evolves: Analyzing the Enduring Cybercrime." *Victims & Offenders* 16, no. 3 (April 3, 2021): 316–342. https://www.tandfonline.com/doi/full/10.1080/15564886.2020.1829224.

Hadjon, Philipus M. *Pengantar Hukum Administrasi Indonesia*. 10th ed. Yogyakarta: Gadjah Mada University Press, 2008.

Hamzah;, Andi. *Asas-Asas Hukum Pidana / Andi Hamzah*. Jakarta: Rineka Cipta, 2008.

Hasan, Fayyad-Kazan, Kassem-Moussa Sondos, Hejase Hussin J, and Hejase Ale J. "Forensic Analysis of Private Browsing Mechanisms: Tracing Internet Activities." *Journal of Forensic Science and Research* 5, no. 1 (March 8, 2021): 012–019. https://www.forensicscijournal.com/articles/jfsr-aid1022.php.

Hassan, Md Arif, Zarina Shukur, and Mohammad Kamrul Hasan. "An Efficient Secure Electronic Payment System for E-Commerce." *Computers* 9, no. 3 (August 27, 2020): 66. https://www.mdpi.com/2073-431X/9/3/66.

Ibrahim, Dr. Johnny. *Teori & Metodologi Penelitian Hukum Normatif*. Bayu Media, 2013.

Khan, Shereen, Tajneen Saleh, Magiswary Dorasamy, Nasreen Khan, Olivia Tan Swee Leng, and Rossanne Gale Vergara. "A Systematic Literature Review on Cybercrime Legislation." *F1000Research* 11 (August 23, 2022): 971. https://f1000research.com/articles/11-971/v1.

Kuzmin, Yury A. "IDENTITY THEFT (CRIMINOLOGICAL ASPECT)." *Oeconomia et Jus*, no. 3 (September 28, 2020): 48–57. http://oecomia-et-jus.ru/en/en-singlenum/.

Leiva, Llysselie Gay Querol. "Impact of Information and Communication Technologies on Everyday Life." *Management (Montevideo)* 3 (February 8, 2025): 130. https://managment.ageditor.uy/index.php/managment/article/view/130.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (June 11, 2024). https://journal.umy.ac.id/index.php/ijclc/article/view/19853.

Makari, Edmon. "Informasi Hukum Untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem Dan Komunikasi Elektronik Global." *Jurnal Ketahanan Nasional* (2014): 77.

Makuch, Anna. "Raising Public and Private User Awareness of the Threats and Risks Related to Cyberspace Security." *Cybersecurity and Law* 8, no. 2 (December 6, 2022): 44–55. http://www.cybersecurityandlaw.com/Raising-

public-and-private-user-awareness-of-the-threats-and-risks-related-to-cyberspace,157123,0,2.html.

Marzuki, Prof. Dr. Peter Mahmud. *Pengantar Ilmu Hukum*. Revisi. Jakarta: KENCANA, 2017.

Nduka, Rapuluchukwu Ernest, and Vinesh Basdeo. "The Need for Harmonised and Specialised Global Legislation to Address the Growing Spectre of Cybercrime." *Southern African Public Law* 36, no. 2 (January 28, 2022). https://unisapressjournals.co.za/index.php/SAPL/article/view/8112.

Ngafifi, Muhamad. "KEMAJUAN TEKNOLOGI DAN POLA HIDUP MANUSIA DALAM PERSPEKTIF SOSIAL BUDAYA." *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi* 2, no. 1 (June 2014).

Rahardjo, Satjipto. *Ilmu Hukum*. 8th ed. Bandung: PT Citra Aditya Bakti, 2014.

———. *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing, 2009.

Ratna, Yulvita, and Gunawan Djajaputra. "LEGAL LIABILITY OF PROPERTY DEVELOPERS REGARDING THE FULFILLMENT OF OBLIGATIONS TO CONSUMERS IN SALE AND PURCHASE TRANSACTIONS USING THE BINDING SALE AND PURCHASE AGREEMENT." *Awang Long Law Review* 6, no. 2 (May 31, 2024): 453–459. https://ijsshr.in/v5i8/66.php.

Ryazanova, Ekaterina. "Responsibility for the Dissemination of Personal Data as a Way to Counteract Offenses in the Field of Information and Communication Technologies." *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia* 2022, no. 3 (October 3, 2022): 118–123. http://vestnikspbmvd.ru/en/nauka/article/48998/view.

Shidarta. *Hukum Penalaran Dan Penalaran Hukum*. 1st ed. Genta Publishing, 2013.

Sukirno, Edy Lisdiyono, and Sri Mulyani. "Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website." *International Journal of Criminology and Sociology* 10 (April 26, 2021): 891–896. https://lifescienceglobal.com/pms/index.php/ijcs/article/view/7427.

Williams, Emma J, and Adam N Joinson. "Developing a Measure of Information Seeking about Phishing." *Journal of Cybersecurity* 6, no. 1 (January 1, 2020). https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyaa001/5748294.

Zam, Efvy. *Phishing : Teknik Mudah Penyadapan Password Dan Pencegahannya*. Jakarta: Mediakita, 2014.

"Teori-Teori Perlindungan Hukum Menurut Para Ahli." *Hukum Online*.