LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 5, 2024, pp. 1369-1377
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

Criminal Law Enforcement Against Cyber Phising Perpetrators (Study of decision Number 85/Pid.Sus/2022/PN Bjb)

Amalia Zahra Harahap[1], Zaid Alfauza Marpaung[2]

[1,2] Departement of Law, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia

Abstract: Cyber phishing crimes are the result of technological advances that allow attacks without physical interaction. This problem is getting worse and is a serious threat to public safety. This study examines the phenomenon of theft and hacking of personal data in a digital context, especially related to cyber phishing violations. This study also evaluates the criminal law framework in Indonesia that regulates these crimes. The methodology used is normative law with a conceptual approach, namely analyzing written laws from library materials, and collecting data from academic literature. The analysis in this study refers to the provisions of the applicable laws. This study aims to determine how criminal law applies to phishing perpetrators in decision No.85/Pid.Sus/2022/PN.Bjb and, explore the relationship between this problem and the Criminal Code, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions and the Personal Data Protection Law. The results of the study discuss how the criminal law system deals with cybercrimes such as phishing, to overcome this crime problem, it is important to increase public awareness, provide education, and strengthen personal data security.

Keywords: Cyber crime, Law enforcement, Phishing.

Correspondence:
Name Corespon Amalia Zahra Harahap
Email Corespon. Azraharahap2009@gmail.com

Received: date;
Revised: date;
Accepted: date;
Published: date;

1. Introduction

Information and communication technology has experienced rapid progress in its sophistication, making it easier for everyone to communicate, search for information, or socialize (Oksidelfa Yanto, 2021). With various increasingly sophisticated communication tools such as smartphones, laptops, or personal computers that are now present in the midst of society, they can make time and place more efficient because they are easily accessible anytime and anywhere (Munir, 2017).Currently, Period 5.0 encourages the people of the Republic of Indonesia to continue to follow the development of contemporary technology which is increasingly being used to accelerate all activities carried out by everyone (Munir, 2017).However, information technology is a useful tool for carrying out illicit activities (Syahrani & Habibullah, 2024). Many people use the internet to do anything, even to harm others, in order to pursue personal gain (Margianto & Syaefullah, 2012). This crime can also be recognized as cyber crime or digital crime which has the potential to trigger other crimes such as phishing (Sari & Sutabri, 2023).

Law enforcement is the process of implementing legal norms in community life to achieve justice and certainty (Hasaziduhu Moho, 2019). Criminal law enforcement can be interpreted as the implementation of law by law enforcement officers and by every person who has an interest in accordance with their respective authorities according to applicable legal regulations (Arief, 1991).

The phenomenon of phishing crimes has increased rapidly, 12,845 different phishing emails and 2,560 fake websites were used in phishing attempts in 2005. In 2022, there were 34,622 phishing cases recorded in Indonesia. As a result, more and more victims have had their m-banking hacked due to phishing crimes. Teddy A. Purwadi, Deputy Head of Administration of the Registry, Secretariat, Law, Government Relations, and Public Relations of Pandi, claims that identifying phishing can be difficult because URL links are usually sent via email that looks authentic and invites recipients to click on it. Teddy continued, "While related to phishing, every reported URL includes the name of a company, brand, or organization". However, in 2023 until now, phishing crimes have begun to spread using social media.

*Cybercrime*Phishing method is a general term for digital fraud crimes that occur during electronic transactions, most victims and law enforcement need additional capabilities to deal with this crime, this type of crime is worrying in various countries around the world (Rokhman & Liviani, 2020). Cyber crime perpetrators are called phishers, where the perpetrators most often utilize electronic media and trick internet users by sending fake links or websites that they send as if the link or website is an official website sent by an official party or company (Juniamalia & Fadlian, 2023). Common examples include the use of online bank accounts so that perpetrators can exploit them to make unlawful profits (Ardiyanti, 2016).

*Phishing*is a fraud strategy used in cybercrime that exploits people's low literacy levels to trick them into disclosing sensitive information such as credit card numbers, bank account numbers, user IDs, and PINs (Suharto & Kurniawan, 2020). Phishing crimes can cause major losses to victims, both material and non-material (Fadli et al., 2024) (Muhammad & Harefa, 2023). Victims can experience material losses such as loss of money, personal data, and identity. Victims can experience non-material losses such as stress, anxiety, and depression (Ma'ady et al., 2023).

*Phishing*generally done via email disguised as communication from a trusted institution such as a bank or company (Pardosi et al., 2024). Users receive emails asking them to provide personal information or click on links that lead to fake websites, which are exploited by criminals to obtain sensitive information. Personal digital data, such as credit card details, passwords, and OTP codes, are considered confidential personal information (Ma'ady et al., 2023).

The case that occurred based on the Banjarbaru District Court decision Number 85/Pid.Sus/2022/PN.Bjb shows a phishing case in which the defendant Riswanda Noor Saputra was charged with creating and distributing phishing software. After a website called "16 Shop" was identified as a phishing kit targeting Apple, Amazon, PayPal, and American Express account users, INTERPOL and the US Embassy reported the case. The defendant is suspected of having a connection to the kit through account data and the use of Indonesian on the device.

Based on Article 51 and 35 of Law Number 19 of 2016 concerning Electronic Information and Transactions, and Article 3 of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, the prosecutor charged the defendant. The prosecutor charged the defendant with a prison sentence of 1 year and a fine of Rp.

200,000,000.00 (two hundred million thousand rupiah). If the fine is not paid, the fine will be replaced with imprisonment for 3 (three) months.

Law enforcement against phishers is very important because of their very detrimental impact, both financially and psychologically (Hasanudin & Babussalam, 2024). As phishing cases continue to increase from year to year, law enforcement and justice for victims are still not optimal. This raises questions about the readiness of the Indonesian legal system in facing the challenges of the digital era.

Based on the explanation above, the researcher is interested in conducting research on how to enforce criminal law against cyber phishing perpetrators (Case Study of Banjarbaru District Court Decision Number 85/Pid.Sus/2022/PN. Bjb).

2. Materials and Methods

This study uses normative legal research techniques which are commonly referred to as doctrinal legal research or library research. It is called doctrinal legal research because this research is only aimed at written regulations so that this research is very closely related to the library because it will require secondary data in the library (Muhammad Syahrum, 2022) (Ridho, 2021).

Based on the data used in this study, qualitative analysis was used with a statute approach, a conceptual approach, and a case approach.The type of data used in this study is secondary data, secondary data is a collection of previously existing information that is used to complete research data needs to obtain information or data needed to answer the formulation of research problems.

The data collection techniques and legal materials in this study include literature studies. The techniques and tools for collecting legal materials are by searching, collecting and reviewing laws and regulations, literature related to the main issues discussed. The purpose of this study is to determine how criminal law enforcement is carried out against cyber phishing perpetrators based on decision No. 85/Pid.Sus/2022/PN. Bjb.

3. Results and Discussion

1. Criminal law review of cyber phishing crimes

Cracking or cracker crime is one of the phishing crimes, which aims to gain personal gain by harming other parties. In the context of computer security, phishing is an electronic fraud that aims to steal sensitive information such as usernames, passwords, and credit card details of victims. This technique is done by disguising itself as an entity that appears official through electronic media such as email or a trusted website.

In dealing with phishing crimes, an approach is needed by the Indonesian government that includes prevention and enforcement strategies. The first effort is prevention with the criminal justice system, while the second effort involves law enforcement supported by the community. Handling phishing crimes requires the active role of the community to report criminal acts. Phishing victims should report to the cyber police to process the case legally and recognize the characteristics of phishing crimes so as not to become victims.

The frequency of phishing actions is increasing drastically, it is recorded globally that the number of frauds using the phishing method published on the official website of

the Anti-Phishing Working Group (APWG) in its monthly report reveals that phishing schemes from 2005 have increased to cover 42% of all reported actions (Gulo et al., 2020).

The author argues that phishing is a cybercrime in which the perpetrator impersonates a trusted entity to obtain sensitive information such as passwords and credit card numbers. In this case, the perpetrator meets the criminal elements such as "whoever", "with the intent to make a profit", and "unlawfully." Phishing is usually done via email, fake websites, text messages, or social media.

Law enforcement based on the provisions of statutory regulations to ensnare phishing perpetrators (phishers) can be reviewed from several relevant laws, namely:

a. Phishing Crimes According to the Criminal Code

In the Criminal Code, criminal provisions in cases of cyber crime in the form of phishing can be used based on Article 378 of the Criminal Code. Legal regulations for cyber crime in the form of phishing are regulated in Article 378 of the Criminal Code concerning fraud as it is known that phishing is generally an act of fraud. The fraud formulated in Article 378 of the Criminal Code is: Which states that:

"Anyone who, with the intention of benefiting himself or another person, goes against the rights, either by using a false name or a false condition, either by means of artifice and deceit, or by composing false words to persuade someone to give something, create a debt or write off a receivable , convicted of fraud, with a maximum prison sentence of four years" (Gunarto, 2012).

Based on this article, the form of punishment for phishing perpetrators or called phiser is the provision on the crime of fraud, namely fraud against property because it includes directing the victim to access a fake website, where the phiser is sentenced to a maximum of 4 (four) years in prison or a maximum fine of up to Rp. 500,000,000 (five hundred million rupiah) (Muhammad & Harefa, 2023).

b. Phishing Crime According to UURI ITE 2024

Based on UURI ITE Number 1 of 2024, Article 35 in conjunction with Article 51 which regulates phishing crimes, which states: "Any person who intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered to be authentic data."

In addition, Article 28 paragraph (1) in conjunction with Article 45 paragraph (2) can also be applied because phishing deceives and misleads victims into visiting fake websites and entering personal data. Article 28 paragraph (1) states: "Any person who intentionally and without right spreads false and misleading news that results in consumer losses in Electronic Transactions".

Then the provisions of the threat according to Article 45 paragraph (2): "Any person who fulfills the elements as referred to in Article 28 paragraph (1) shall be punished with a maximum prison sentence of 6 years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah). The provisions in the article can be linked to the case*phishing*which occurred in accordance with decision No. 85/Pid.Sus/2022/PN.Bjb. The element, "every person" is a phisher who intentionally and illegally commits the crime of electronic manipulation and money laundering.

c. Phishing Crime According to UURI PDP

Guidelines for criminal acts of phishing according to UURI PDP No. 27 of 2022 are contained in Article 65 in paragraph (1) concerning personal data protection, which states: "Article (1): Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to the Personal Data Subject."

Regulations regarding the threat of criminal acts of phishing according to Article 67 Number (1) of Law Number 27 of 2022 concerning Protection of Personal Data, namely: "Article (1): Any person who intentionally and unlawfully obtains or collects Personal Data that is not his/hers with the intention of benefiting himself/herself or another person which may result in losses for the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah)"(Benjamin, 2024).

Phishing perpetrators can be subject to sanctions under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) if they obtain personal information belonging to other people through this crime, such as information and biometric data on other people's devices.(Malunsenge et al., 2022).

2. Criminal Law Enforcement against Cyber Phishing Perpetrators Based on Decision Number 85/Pid.Sus/2022/PN.Bjb

a. Case Chronology

The author explains the phishing crime case that occurred in the Banjarbaru area in decision No. 85/Pid.Sus/2022/PN Bjb with the defendant named Riswanda Noor Saputra, a 22-year-old student, committing fraud through phishing methods by producing and selling software called "16 shop" which resembles official PayPal, Apple, Amazon products. He was arrested on November 19, 2021, and began detention on November 20, 2021. Where the public prosecutor, the Chief Justice of the District Court, and the Chief Justice of the High Court repeatedly extended his detention. In accordance with Article 51 of the ITE Law No. 19 of 2016 and Article 3 of the Money Laundering Law No. 8 of 2010, Riswanda was found guilty of the crimes of electronic manipulation and money laundering.

b. Public prosecutor's indictment

The Public Prosecutor charged Riswanda Noor Saputra with the crime of “Intentionally and without rights or against the law manipulating, creating, changing, removing, destroying Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as authentic data” and the crime of “placing, transferring, diverting, spending, paying, granting, depositing, taking abroad, changing the form, exchanging with currency or securities or other actions on Assets that he knows or should suspect are the result of a crime with the aim of hiding or disguising the origin of the Assets” as regulated and threatened with criminal penalties in Article 51 of the ITE Law No. 19 of 2016 in conjunction with Article 35 of the UTE Law No. 19 of 2016. The prosecutor charged Riswanda with a prison sentence of 1 (one) year and a fine of Rp200,000,000 (two hundred million rupiah). If he does not pay the fine, it will be replaced with 3 (three) months in prison. That the defendant Riswanda Noor

Saputra, intentionally and without rights or against the law, produced, sold, procured for use, imported, distributed, provided, or owned as referred to in Articles 27 to 33 computer hardware or software that was designed or specifically developed to facilitate the acts as referred to in Articles 27 to 33.

The way buyers cheat and steal other people's accounts is after buying a TOOL KIT named 16 defendant shops that resemble PayPAL, Apple, Amazon products, then spammers (application buyers) use email sending applications in large quantities by sending them to hundreds of thousands of victim user emails at once, then the victims receive an email and then click on the email containing the link and direct them to the TOOL KIT which closely resembles the appearance of the original PayPAL, Apple, Amazon account and the language according to the domicile of the victims' country, then the victims feel sure that the link is official, they are directed to fill in personal data and credit card data related to the use of PayPAL, Apple, Amazon products, which are then used by the perpetrators for personal needs such as shopping and/or commercial needs of the perpetrators.

The actions of the defendant Riswanda Noor Saputra are regulated and threatened with criminal penalties under Article 51 in conjunction with Article 35 of Law no. 1 of 2024 concerning the second amendment to Law no. 19 of 2016 concerning Electronic Information and Transactions.

From the Defendant's actions, the Defendant obtained benefits from his actions in the form of assets, namely money amounting to +/- Rp.1,702,383,118 (one billion seven hundred two million three hundred eighty three thousand one hundred eighteen rupiah) That the Defendant with the aim of hiding or disguising the origin of the money, the Defendant has placed the proceeds of the crime into a BITCOIN wallet account at PT. INDODAX with Wallet Address 1NyjuDCFpwEuzuWWAZWqt94maZSuTddx3P with the account erenes007@gmail.com and email devilscream and then the Defendant put it back into the BCA Bank account 7895461296 in the name of RISWANDA NOOR SAPUTRA belonging to the Defendant.

That for the defendant's actions in placing, transferring, spending, paying or carrying out other actions on the Assets as intended to hide or disguise the origin of the Assets, the defendant's actions are regulated and are subject to criminal penalties in violation of Article 3 of Law of the Republic of Indonesia Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering.

c. Judge's Consideration

The judge stated that the Defendant Riswanda Noor Saputra was proven legally guilty of committing a crime by intentionally without rights or unlawfully producing computer software that was designed or specifically developed to facilitate acts as referred to in Article 32 paragraph (2) and the crime of placing and transferring currency or securities or other acts that he knew or could reasonably suspect were the result of a crime with the aim of hiding or disguising the origin of the assets as charged by the Public Prosecutor, sentencing the defendant to imprisonment for 2 (two) years and 6 (six) months and a fine of Rp. 500,000,000 (five hundred million rupiah) which if not paid will be replaced with imprisonment for 3 (three) months, and ordering the defendant to pay court costs of Rp. 5,000 (five thousand rupiah).

d. Decision Analysis

The panel of judges has confirmed that the decision 85/Pid.Sus/2022/PN.Bjb has met the requirements for law enforcement. These requirements are the act of transferring, diverting, and hiding assets that are known or suspected to originate from criminal acts, including in this category, namely phishing. The judge sentenced him to 2 (two) years and 6 (six) months in prison and a fine of Rp. 500,000,000 because the law enforcement was considered in accordance with the principles of criminalization.

Based on the author's analysis, there are weaknesses in law enforcement, namely the mismatch between the penalties imposed and the provisions in the relevant laws, where cybercrime is still considered light and disproportionate to the losses suffered by the victim. Given the losses suffered by the victim, a longer prison sentence, for example between 3 to 5 years and a higher fine, for example IDR 1,000,000,000, can be imposed to reflect the victim's losses considered more appropriate to provide a deterrent effect. However, it is important to remember that criminal law enforcement has two main objectives, namely combating crime and ensuring that the government acts in accordance with the law, therefore based on the description above, things that need to be considered regarding Cyber Crime phishing methods based on the law are, among others:

1) Law Enforcement Officer
   Law enforcement officers need to play an active role in handling cybercrime, because this crime is always present in society. Punishment is not only intended to provide a deterrent effect to the perpetrators, but also as an effort by the state to maintain justice. Therefore, the quality and ability of law enforcement officers are very important in law enforcement. To increase public trust, it is necessary to strengthen the function of law enforcement officers individually and organizationally, as well as build a community that focuses on handling cybercrime.
2) Improvement of Facilities and Infrastructure
   Effective cyber law enforcement in Indonesia is highly dependent on the availability of adequate facilities and infrastructure. Strong legal standards need to be supported by tools such as phishing identification systems to ensure law enforcement officers can carry out their duties optimally, and the importance of public and government understanding of personal data protection.
3) Special Law Regarding Cyber Law In Indonesia
   Phishing victims need to fulfill material losses, and the Witness and Victim Protection Law (UUPSK) provides protection through compensation, restitution, and assistance. However, the effectiveness of the ITE Law in enforcing the law for phishing victims is still questionable because the rights of victims have not been explicitly regulated. Better implementation of Law No. 27 of 2022 is also needed to guarantee individual privacy rights.

Therefore, criminal law enforcement is not solely aimed at punishment, but must also consider how effective it is in reducing crime, and prosecutors must pay attention to Law Number 27 of 2022 concerning Personal Data Protection and Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 19 of 2016 concerning Data Protection Guidelines. In this case, various provisions regulate the

rights of the public to protect personal data, although Law Number 19 of 2016 does not include a clear definition of "personal data".

4. Conclusions

Cyber phishing fraud is becoming increasingly rampant and causing losses to its victims. According to this study, perpetrators of cybercrime, including phishing, can be subject to the provisions of Article 378 of the Criminal Code which regulates fraud. In addition, they can be prosecuted under Law Number 1 of 2024, concerning the second amendment to Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE), especially Article 35 in conjunction with Article 51 which regulates illegal access and data theft, and Article 67 paragraph (1) of Law of the Republic of Indonesia Number 27 of 2022 concerning personal data. Banjarbaru District Court Decision Number 85/Pid.Sus/2022/PN Bjb, the defendant was sentenced to 2 (two) years and 6 (six) months in prison and a fine of IDR 500,000,000.00. If the fine is not paid, the defendant will serve an additional 3 (three) months in prison. However, law enforcement against victims has not fulfilled the justice that it should. The rights of victims in the legal process are regulated in Law Number 27 of 2022 concerning Protection of Personal Data and the Criminal Procedure Code (KUHAP). To achieve balanced justice, law enforcement against perpetrators and adequate protection for victims are needed.

References

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *… Dinamika Masalah Politik Dalam Negeri Dan …*.

Arief, B. N. (1991). Upaya Non Penal Dalam Kebijakan Penanggulangan Kejahatan. In *… : Makalah disampaikan dalam Seminar Kriminologi VI*.

Benyamin, B. (2024). *ANALISIS YURIDIS TINDAK PIDANA CYBER CRIME PHISING DALAM KETENTUAN HUKUM POSITIF INDONESIA*. repository.unhas.ac.id.

Fadli, M., Widijowati, D., & Andayani, D. (2024). Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi. *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan*, *14*(12).

Gulo, A. S., Lasmadi, S., & ... (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of …*.

Gunarto, M. P. (2012). Asas Keseimbangan Dalam Konsep Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana. *Mimbar Hukum-Fakultas Hukum Universitas Gadjah …*.

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. *Jurnal Gagasan Hukum*, *6*(01), 16–29.

Hasaziduhu Moho. (2019). Penegakan Hukum di Indonesia Menurut Aspek Kepastian Hukum, Keadilan, dan Kemanfaatan. *Jurnal Warta*, *13*(1), 138–149.

Juniamalia, A., & Fadlian, A. (2023). PERSPEKTIF UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP CYBER CRIME DALAM BENTUK PHISING: Bentuk Pemidanaan Terhadap Pelaku Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia. *De Juncto Delicti: Journal of Law*, *3*(1), 30–46.

Ma'ady, M. N. P., Zahra, A. N., Darmawan, M. Z., & ... (2023). Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet). *Seminar Nasional …*.

Malunsenge, L., Massie, C., & Rorie, R. (2022). Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia. *Lex Crimen*.

Margianto, J. H., & Syaefullah, A. (2012). Media online: Pembaca, laba, dan etika. *Jakarta: Aliansi Jurnalis Independen Indonesia*.

Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. *Jurnal USM Law Review*.

Muhammad Syahrum, S. T. (2022). *Pengantar Metodologi Penelitian Hukum: Kajian Penelitian Normatif, Empiris, Penulisan Proposal,*

Laporan Skripsi dan Tesis. CV. Dotplus Publisher.

Munir, N. (2017). Pengantar Hukum Siber Indonesia Edisi Ketiga. In *PT Raja Grafindo Persada, Depok*.

Oksidelfa Yanto, S. H. (2021). *Pemidanaan atas kejahatan yang berhubungan dengan teknologi informasi*. Samudra Biru.

Pardosi, V. B. A., Kom, S., Karim, A., Ti, M., Ilham, R., Kom, M., Hamuda, H., Dotulong, F. V, Arfianto, A. Z., & Septiani, S. (2024). *Sistem Keamanan Komputer*. CV Rey Media Grafika.

Ridho, M. N. (2021). Pengenaan Pajak Pertambahan Nilai (PPN) Pada Transaksi E-Commerce. *JISIP (Jurnal Ilmu Sosial dan Pendidikan)*, *5*(1).

Rokhman, M., & Liviani, H. I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. In *Jurnal Pemikiran dan Pembaharuan Hukum Islam*.

Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*.

Suharto, B., & Kurniawan, A. B. (2020). Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising). *JHP*.

Syahrani, R., & Habibullah, H. (2024). Peran Teknologi Informasi Komunikasi dalam Manajemen Rantai Pasok: Systematic Literatur Review. *Journal of Business Management*, *2*(1), 1–10.