West Science Law and Human Rights
Vol. 2, No. 03, July 2024, pp. 287~296

Legal Protection for Phishing Victims Reviewed from Indonesian Positive Law

Olivia Audriana Putri[1], E. Imma Indra Dewi Windajani[2]
[1,2]Atma Jaya Yogyakarta University

Article Info

Article history:

Received July, 2024
Revised July, 2024
Accepted July, 2024

Keywords:

phishing
legal protection
personal data
compensation
lawsuit

ABSTRACT

In this age of digitalization, phishing has become a crime that is close to human life. In phishing crimes, the perpetrator's identity is mostly unknown or anonymous. The perpetrator's identity is the primary key for processing a lawsuit in court. Victims who don't know the real identity of the phisher will not be able to file a lawsuit for compensation. This study aims to determine the legal protection the state provides to phishing victims, especially in terms of compensation. This research uses a juridical-normative method with data collection through a literature study. Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 regarding Electronic Information and Transactions (ITE Law), Law No. 27 of 2022 regarding Personal Data Protection (PDP Law), and other constitutional regulations are the primary legal materials in this research. The secondary legal materials are relevant research results, journals, and books. Based on the research conducted, it has been shown that it's necessary to establish the real identity of the perpetrator who can be responsible for compensating the victims of phishing. The difficulty of finding phishers who can hide their real identities and digital footprints are the main obstacle to compensating phishing victims.

Corresponding Author:

Name: Olivia Audriana Putri
Institution: Universitas Atma Jaya Yogyakarta
e-mail: oliviaaudr@gmail.com

1. INTRODUCTION

The development of science and technology has provided various conveniences for humans in their daily lives. One of them is the existence of the internet. Through the internet, everyone can easily find information, communicate, and even make buying and selling transactions easily without being limited by space and time [1]. With the development of science and technology, people are required to be able to adapt to the times.

Like a double-edged sword, technological developments also have positive and negative impacts. Technological developments can give rise to new crimes that endanger human life [2]. The threat of crime comes from the misuse of technology. Irresponsible parties use technological advances. With the times, perpetrators often create more complex cyber-attack strategies [3]. As a result, currently, there are forms of cybercrime that are increasingly common, one of which is phishing.

Phishing is a form of cybercrime in the form of fraud that aims to steal the victim's data by posing as a trusted or legitimate

organization [4]. The perpetrator creates tricks to trick victims with their disguise. Simply put, victims will be lured with traps or threats so that they will indirectly be deceived and provide their data to the perpetrator [5].

Many victims are deceived because the perpetrators use fake emails or websites that look like the real thing. Personal data targeted are full name, address, date of birth, username, password, PIN, credit card details, OTP (One-Time Password) code, and so on. If the victim's data has been successfully obtained, the perpetrator can directly utilize it by misusing the account, stealing the victim's account, and other things that benefit the perpetrator [6].

Anti-Phishing Data Exchange (IDADX), social engineering and technical subterfuge techniques are the common modus operandi used by perpetrator (phishers) [7]. Social engineering techniques are carried out by exploiting a person's weaknesses [7]. This is done by sending fraudulent messages in the form of fake links or documents to email addresses or social media, such as WhatsApp, Instagram, Facebook, and others. Through this method, the phishers can trick the victim and misuse the victim's data for irresponsible things. Furthermore, technical subterfuge is a technique of installing malware into the device to retrieve personal data belonging to the victim. Generally, the phishers create a website that looks like the original.

When the user (target) enters the username and password on the fake website that has been directed by the perpetrator, the phishers can reach the victim's data. As a result, many victims experience identity theft that leads to account breaches and other financial losses.

Ironically, phishing crimes are increasingly prevalent in Indonesia. According to the Badan Siber dan Sandi Negara (BSSN), in 2022 164.131 cases of phishing emails occurred in Indonesia [5]. Data on phishing case reports has also been received by the IDADX as many as 26,675 cases in 2023 [7]. Various sectors are targeted by phishing, such as the financial sector, trade, government, and technology, especially social media platforms. This shows that phishing has become a truly life-threatening problem.

In a phishing crime, the victim suffers material or even immaterial losses. Victims certainly expect compensation so that the money taken by the perpetrator can be returned. In addition, perpetrators often send deceptive messages using fake or even anonymous identities. The identity of the perpetrator is the main key for a lawsuit to be accepted and processed in court. The lawsuit filed by the victim cannot be processed if they do not know the identity of the perpetrator. Departing from these problems, this research aims to find out how legal protection is provided by the state to phishing victims, especially in terms of compensation.

2. LITERATURE REVIEW

According to Satjipto Raharjo also argues that legal protection should be able to protect the rights of victims who are harmed [8]. Legal protection is given so all people can feel the rights the law provides. The law functions to realize protection that is not only adaptive, but also anticipatory and predictive [9].

Legal instruments are needed to guide law enforcement officials in taking action against cybercrime perpetrators [10]. In dealing with existing cybercrimes, Indonesia has reformed the criminal law and created more specific regulations, as shown by the Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 regarding Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 regarding Personal Data Protection (PDP Law) However, punishing the perpetrators is not enough. Cybercrime victims suffer losses that require compensation as a form of legal protection.

In connection with the progressive legal theory initiated by Satjipto Rahardjo, the law should be able to keep up with the times [11]. It can be said that existing laws must be able to keep up with the times. As society evolves, the types of crimes may also evolve along with technological developments in the future. In addition, the law must be able to

respond to existing challenges and protect the community, including the handling of phishing cases.

3. METHODS

The method in this research uses the juridical-normative method. Juridical-normative research is carried out by collecting data through literature studies. The literature study was conducted by collecting materials in the form of laws and regulations, scientific journals, literature, and other sources relevant to this research. The legal sources used in this research are primary and secondary legal materials.

Primary legal materials consist of legislation and official records. Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 regarding Electronic Information and Transactions (ITE Law), Law No. 27 of 2022 regarding Personal Data Protection (PDP Law), and other constitutional regulations are the primary legal materials in this research. In addition, secondary legal materials used are scientific journals, literature, and other sources relevant to the issues raised in this research. The data analysis technique in this research uses qualitative analysis.

4. RESULTS AND DISCUSSION

4.1 *Regulations for Phishers in Indonesia*

In this age of digitalization, phishing is a crime that is very close to people's lives. This is because most people have used social media and other digital applications, including mobile banking services from banks. Perpetrators use these gaps to carry out their actions. Their phishing tricks can be directed to all social media and mobile banking users. This is because the main goal of the perpetrators is to take advantage, especially from the victim's account.

Under Indonesian law, several articles formulate criminal offenses related to phishing in the Criminal Code (KUHP). Some of these articles include Article 378 of the KUHP on fraud, Article 362 of the KUHP on theft, and Article 263 of the KUHP on forgery of letters that can be imposed on phishing crimes.

Phishing fulfills the elements of fraud in article 378 of the KUHP, namely the deliberate use of lies for one's own benefit. These lies are intended to deceive the victim through emails, links or fake websites that appear to be genuine. However, Article 378 of the KUHP does not cover the elements of cybercrime because it does not contain the element of electronic information. Phishing also fulfills the elements of theft in Article 362 of the KUHP, which is the unlawful taking of something that belongs to another person. However, there is a difference between phishing and ordinary theft, namely the object taken by the perpetrator. In the crime of phishing, the object taken is the electronic information (personal data) of the victims. This shows that phishing has more specific characteristics than ordinary theft.

The elements in Article 263 of the KUHP on mail forgery are also acts committed by phishers. First, the element of forgery. In phishing, the perpetrators mostly intentionally send messages via email or other social media that appear to come from genuine or legitimate parties. Messages received electronically are classified as electronic mail. Second, the use of the fake email/message causes harm. The fake message sent by the perpetrator tricks the victim into providing personal information. This information is then misused by the phishing perpetrator.

Cybercrimes have been regulated in a more specific regulation, namely Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 regarding Electronic Information and Transactions (ITE Law). Phishing is one of the cybercrimes. There are several articles in the ITE Law that fulfill the elements of the crime of phishing. Based on Article 28 paragraph (1) of the ITE Law, there is a prohibition on spreading false and misleading messages that cause harm to consumers in electronic transactions. Anyone who violates this article will be punished with a maximum jail term of six years and/or a maximum fine of one billion rupiah. Phishers spread false information and mislead victims.

Based on Article 30 paragraph (2) jo. Article 46 paragraph (2) of the ITE Law, there is a prohibition of acts that unlawfully and illegally access a computer or electronic system for the purpose of obtaining electronic information. The perpetrator will be punished with a maximum jail term of seven years and/or a maximum fine of 700 million rupiah. In addition, Article 30 paragraph (3) jo. Article 46 paragraph (3) of the ITE Law states that accessing a computer or electronic system by violating or breaching the security system shall be punishable by a maximum of eight years imprisonment and/or a maximum fine of Rp 800 million.

For the act of transferring information or electronic documents belonging to the victim to other unauthorised persons, he may be charged under Article 32 paragraph (2) jo. Article 48 (2) of the ITE Law. The perpetrator will be sentenced to imprisonment for a maximum of nine years and/or a maximum fine of three billion rupiah. These are the usual actions taken by phishers. The perpetrator sends a message to the victim in the form of an email, a link or a forged document. In addition, the perpetrator intentionally breaches the security system to gain access to the electronic system and obtain the victim's personal information.

Article 35 jo. Article 51 paragraph (1) of the ITE Law also stipulates that every person is prohibited from manipulating, creating, altering, deleting, or damaging electronic information with the aim that the electronic information is perceived as real data. Any person who violates the provisions of this article shall be punished with imprisonment for a term not exceeding 12 years and/or a fine not exceeding Rp 12 billion. This means that the perpetrator of phishing has fulfilled the elements in the article. In a phishing crime, the perpetrator manipulates and creates fake links, websites or emails that are sent to victims. This is done to trick the victim into believing that the information they are receiving is genuine.

On January 4, 2024, President Joko Widodo signed Law No. 1 Year 2024 on the Second Amendment to Law No. 11 Year 2008 regarding Electronic Information and Transactions (ITE Law). However, until the signing of the second amendment to the ITE Law, there was no provision regarding compensation for victims of cybercrimes, especially phishing. The provisions of the ITE Law show that the form of legal protection and fulfillment of rights for victims is only in the form of case settlement in the form of criminal provisions. The legislator considers criminalization as the right step to deal with cybercrimes [12]. Sanctions in the form of imprisonment and fines are considered capable of resolving a criminal case by having a deterrent effect on the perpetrator.

The existing regulations have indeed formulated elements related to phishing crimes. However, none of the many existing articles regulates compensation for victims of cybercrimes. Existing regulations only provide for punishing perpetrators through imprisonment and fines. Imprisonment is a physical punishment for the perpetrator, while the perpetrator pays the fine to the state. In phishing, on the other hand, the victim suffers a material loss and therefore requires compensation. This shows that the criminal provisions in the ITE law are not yet able to provide legal protection and fulfillment of rights for phishing victims.

4.2 *Personal Data Protection Reviewed from Indonesian Positive Law*

Regarding personal data targeted by cybercriminals, such as phishing, Indonesian positive law has regulated personal data protection. This regulation is contained in Law No. 27 of 2022 regarding Personal Data Protection (PDP Law). The PDP Law is a regulation that provides certainty to the public's right to the protection of personal data, which is very crucial [13]. The government is responsible for protecting people's personal data.

Based on Article 5 of the PDP Law, every person has the right to obtain information about the clarity of identity, the purpose of using personal data, the basis of legal interests, and the accountability of the party requesting personal data. Article 12 of the PDP Law also affirms that the owner of

personal data has the right to claim compensation and request legal action if there is a violation in the processing of personal data. This means that the government needs to provide an effective personal data protection mechanism that guarantees that certain parties will not misuse personal data [14].

Processing of personal data must be with the valid consent of the owner of the personal data as referred to in Article 20 paragraph (2) of the PDP Law. Article 24 of PDP Law also explains that the personal data controller, as the party conducting personal data processing, must be able to prove that it has obtained the consent of the personal data owner. It can be interpreted that proof of consent is important to ensure that data processing is carried out legally and by existing provisions [15].

Data security breaches that result in the intentional or unauthorized loss, disclosure, alteration, or access of personal data are considered a failure to protect personal data [15]. According to Article 47 of the PDP Law, the personal data controller is responsible for the processing of personal data and must comply with the principles of personal data protection. If the personal data owner suffers a loss, the personal data controller must prove that the data processing was conducted according to the principles of personal data protection.

Article 65 of the PDP Law also emphasizes the prohibition for any person to unlawfully obtain, disclose, and use another person's data. In addition, Article 66 of the PDP Law states that any person is prohibited from falsifying personal data to obtain personal benefits to the detriment of others. A person who violates Article 65 of the PDP Law shall be sentenced to a maximum of 4-5 years imprisonment and/or a maximum fine of 4-5 billion rupiah. In addition, a violation of Article 66 of the PDP Law shall be punishable by a maximum term of imprisonment of six years and/or a maximum fine of six billion rupiah. The perpetrator may also be subject to additional punishment in the form of payment of compensation and confiscation of proceeds of crime. Anyone who misuses personal information will be punished under the PDP Law, including phishers.

4.3 Legal Protection for Phishing Victims

Victims of phishing crimes indeed suffer losses, especially material losses. This shows that victims have the right to compensation. Based on Article 1246 of the Civil Code (KUHPerdata), the compensation elements are costs incurred, losses, and expected profits. In phishing cases, a person has to incur expenses to deal with the case, losses due to the loss of money in the account, and needs or activities that should have been carried out are delayed. These rights must be fulfilled as a form of legal protection for victims. Based on the applicable law in Indonesia, there are generally several ways for victims to obtain compensation. These include merger of compensation claims in criminal cases, unlawful act lawsuits, and restitution claims [12].

First, through the merger of compensation claims in criminal cases. The merger of compensation claims in criminal cases is the examination of compensation claims (which are civil) against criminal cases that are being processed in court [16]. The compensation claim is filed because the criminal act committed by the perpetrator causes damage to the victim. In this case, phishing has caused losses to the victim, so the victim has the right to file a compensation lawsuit.

Based on Article 98 of the Criminal Procedure Code (KUHAP), the victim may request the judge to merger the compensation claims for the crimes that caused the victim's loss. According to Article 98 paragraph (2) of the KUHAP, this request shall be made at the latest before the prosecutor files the indictment. If the public prosecutor is absent, the application for compensation is submitted before the judge issues the verdict.

The charges against the accused/suspect must first be investigated and proven as the primary (criminal) case. If the perpetrator is proven to have committed a crime, this becomes the basis for granting the compensation claim. This is because the

compensation claim is only an addition to "hitchhikes" in the main case. Conversely, if it is not proven that the suspect has committed a crime, the compensation claim cannot be granted.

In practice, the merger of compensation claims in criminal cases still causes problems [17]. The rules regarding the merger of cases contained in the KUHAP have weaknesses. One of them is that it is facultative. This means that it is up to the victim to decide whether or not to apply for the merger of compensation. However, not all victims are aware that they have the right to submit a request and that it should be submitted at the latest before the public prosecutor files charges. In addition, law enforcement officers often do not inform victims because the KUHAP does not require them to do so.

Another weakness is that merger of compensation claims in criminal cases are only ancillary. The decision on compensation depends heavily on the main (criminal) case. If the victims did not appeal the criminal case, the victims cannot appeal the compensation. The compensation can't be filed for immaterial losses either. Another problem that arises is the relative competence of the court [18]. The merger of compensation claims in criminal cases is based on the place where the crime was committed, while a lawsuit must be filed with the court where the defendant is domiciled. This means that the merger of compensation claims in criminal cases cannot be done with a difference in jurisdiction. In the case of phishing, the crime takes place in cyberspace and the perpetrator's domicile is often unknown. Therefore, the merger of compensation claims in criminal cases is inappropriate for cybercrimes such as phishing.

Second, through an unlawful act lawsuit. In terms of civil law, compensation can come from unlawful acts. This is based on Article 1365 of the Civil Code (KUHPerdata), which states that all unlawful acts that cause damage to others obligate the perpetrator to pay compensation. An unlawful act lawsuit must satisfy the elements of the unlawful act itself, the existence of damage, the existence of a fault, and a causal relationship between the unlawful act of the perpetrator and the damage [19].

Phishing is against the law, especially against the ITE Law and the PDP Law. The mistake made by the phishing perpetrator is to intentionally send a fake link or website to the victim for profit. In phishing cases, the victims have suffered material or even immaterial losses. The unlawful act committed by the perpetrator has caused damage to the victim. There is a causal relationship between the unlawful act and the loss suffered by the victim. This means that phishing can be classified as an unlawful act. Therefore, phishing victims can ask for compensation through an unlawful act lawsuit.

An unlawful act lawsuit is filed in the district court where the defendant is located. Victims can also file criminal charges against the perpetrator first. Then, after the perpetrator has been criminally proven to have committed a crime and has received an *inkracht* verdict, the verdict can be used as evidence in a civil lawsuit. Criminal judgments that have been *inkracht* have substantial evidentiary value in civil lawsuits. This is because the perpetrator (convicted) has been proven guilty and has caused harm to the victim.

Third, compensation can be made through restitution. Compensation given to victims or their families by perpetrators or third parties is called restitution. This has been regulated in Article 1 point 11 of Law No. 31 of 2014 Amendments to Law No. 13 of 2006 regarding Witness and Victim Protection. Article 1, point 8 of the Law No. 31 of 2014 also explains that protection is all efforts to fulfill rights and provide assistance to provide security to witnesses and/or victims. In this case, restitution is a form of fulfillment of rights for victims.

The rules related to restitution in the Law on Witness and Victim Protection still have weaknesses. There is no further explanation regarding what criminal offenses restitution can be applied for. Victims do not

always get their rights in terms of applying for restitution. This is because there are no rules regarding the type of criminal offense as a condition for applying for restitution. In addition, the existing rules are still facultative. The fulfillment of witness and victim rights depends on the decision of the Lembaga Perlindungan Saksi dan Korban (LPSK).

In general, there are still obstacles to the implementation of compensation. The facts in the field show that these obstacles come from the side of the perpetrator/defendant. When compensation claims are granted, perpetrators are often unwilling or unable to pay compensation due to economic difficulties [18]. Perpetrators also feel that a prison sentence or fine is sufficient. They feel burdened by having to pay compensation to the victim. This is the perpetrator's obligation because they have harmed the victim.

Victims of phishing should not only know how to obtain compensation, but also who is responsible for their losses. The victim's bank account has become the primary target in phishing cases. In this regard, victims need to know how banks are liable for losses incurred by customers who are victims of phishing.

According to Article 19 of Law No. 8 of 1999 regarding Consumer Protection, banks, as business actors, are responsible for losses customers suffer. With a note, the loss sustained by the customer is the bank's negligence. In addition, according to Article 15 paragraph (2) of the ITE Law, banks, as providers of electronic systems, are responsible for users of electronic systems. This provision does not apply if force majeure, fault, or negligence of the electronic system user can be proven.

Article 10 paragraph (2) of Financial Services Authority Regulation No. 22 of 2023 regarding Consumer and Community Protection in the Financial Services Sector also regulates a similar matter. The article states that the bank cannot be held liable if the bank can prove that there is negligence on the part of the customer. This means that banks can only be held responsible for losses incurred by customers if the losses are due to the fault or negligence of the bank.

In the case of phishing, there is an element of negligence on the part of the customer (victim) [20]. In fact, from the point of view of good faith, the victim's actions show that he is acting as an honest person, and there is an element of ignorance in him. This means that the actions of phishing victims are not entirely due to negligence, but there is an element of ignorance on the victim's part. As a result of his ignorance, the victim is deceived by the link or website provided by the phisher and thinks that the link or website is genuine. This happened in the case of personal data leakage experienced by several customers of Bank Tabungan Pensiunan Nasional (BPTN) Jenius [21].

In the BTPN Jenius case, several customers received phone calls in the name of Jenius. The customer did not feel suspicious because the caller's words were convincing, such as providing genuine information. The customers (victims) who received the call then clicked on the link provided by the caller. Moments later, the customer's Jenius application was logged out and inaccessible. Upon further investigation, the hundreds of millions in the victim's account had disappeared and been transferred to another party.

In this case, the victim suffered a material loss, but the bank cannot be held responsible. The bank cannot be held responsible in this case because, after further investigation, it was proven that the victim committed an element of negligence. The negligence consists of filling out a link outside of BTPN Jenius provided by the phisher. The first step is to prove that the phishing victim was negligent. If it is proven that the victim was not at fault and the fault lies with the bank, the victim is entitled to compensation. This compensation is a form of legal protection for the victim.

On the other hand, there are forms of liability that the banks have. As a financial services business actor, banks must have and implement policies and procedures regarding consumer protection for customers who

become victims of digital banking services. This is regulated in Article 8 of the Financial Services Authority Regulation No. 22 of 2023.

Article 21 of Financial Services Authority Regulation No. 21 of 2023 regarding Digital Services of Commercial Banks also regulates the legal protection of customers. Customers who become victims while using digital banking services are entitled to protection and legal certainty [22]. Banks must apply the principle of security control of transactions and data used by customers in the bank's digital services. In addition, Article 26 of the Financial Services Authority Regulation No. 21 of 2023 states that banks must follow up on customer complaints by operating 24 hours a day. Customer complaints will be confirmed, and then the bank will examine and investigate the cause of the loss. The bank will examine and investigate whether the customer's loss was caused by phishing, which is the victim's negligence or by the bank's security system.

It can be interpreted that the bank's responsibility to the customers who have suffered losses is to examine and investigate the causes of phishing. In addition, banks can provide facilities in the form of complaint services for customers that operate 24 hours a day. If it is proven that the loss suffered by the victim is due to the bank's negligence, then the bank must be fully responsible for compensation.

If phishing is proven to involve elements of negligence on the victim's part, the bank can at least help secure the victim's account. This must be done as part of the bank's efforts to protect the consumer, ensuring the customer's data and funds remain after a phishing incident. This is what BTPN Jenius did when one of its customers became a victim of phishing.

The phishing incidents experienced by some of BTPN Jenius's customers were caused by negligence by customers who clicked on phishing links. In this case, BTPN Jenius did not provide liability in compensation. The form of responsibility that BTPN Jenius takes is to support the complaint process through review and investigation and to assist customers in reporting the phishing incident to the police [23].

Another form of responsibility from BTPN Jenius is maintaining the Jenius application to support the customer's security in the future [23]. BTPN Jenius disables access to Jenius via the website to reduce the risk of phishing attempts. To protect customers' Jenius accounts, BTPN Jenius has implemented a single-connected device policy. This allows customers to access and transact with only one verified device.

Another problem is that perpetrators often send phishing messages under false or anonymous identities. Perpetrators use this strategy to avoid legal liability. Perpetrators take great care to maintain anonymity and hide their digital footprints. They use social media accounts with fake names that are difficult to trace and use VPNs or other techniques to obscure their digital footprint [24].

In a study conducted by Purwandari, it was also mentioned that Subdit V Siber POLDA Daerah Istimewa Yogyakarta experienced obstacles in catching phishing perpetrators because the perpetrators had expertise in hiding their identity and digital footprint [25]. Identifying the perpetrator becomes more complicated when the perpetrator uses multiple accounts and e-wallets to store phishing funds. The use of various accounts or e-wallets makes it more difficult to track transactions and the identity of the perpetrator.

When the investigative team learns the perpetrator's identity, it may not be the identity of the original perpetrator. Because many perpetrators falsify their identities, including names and addresses, tracing becomes difficult. Therefore, data and transaction lists (flow of funds) on the perpetrator's bank account or e-wallet account are essential in determining the true identity of the perpetrator. However, the investigating team often encounters obstacles to access to the bank [25]. This is because the bank authorization process takes a long time.

The real identity of the perpetrator is the primary key to the process of the lawsuit.

In a civil lawsuit, a lawsuit can be processed if the elements of the lawsuit are fulfilled, one of which is the identity of the parties (including the identity of the perpetrator) [26]. The next element that must be present in the lawsuit is the reason for the lawsuit *(fundamentum petendi)* and the demands *(petitum)* of the party filing the lawsuit. If the elements in the complaint are not fulfilled, the complaint is declared "NO" *(Niet Ontvankelijke Verklaard)* because it is considered to contain formal defects [27]. A lawsuit that has been declared "NO" can indeed be resubmitted if it has been corrected. In the new lawsuit, the victim must include the original identity of the perpetrator. The victim cannot file a lawsuit for compensation if the perpetrator's real identity is not found. In this case, tracking and finding the perpetrator is the primary key in handling phishing cases.

This is the problem that arises in law enforcement related to phishing. When the whereabouts or true identity of the perpetrator is not found, the victim cannot file a lawsuit for compensation. This means that the victim cannot get their money back and the case could potentially be closed or discontinued. In addition, the lack of human resources and technology is also an obstacle in handling phishing cases.

5. CONCLUSION

In today's digital age, the protection of personal information is becoming increasingly important. This is related to the rampant phishing cases that occur in Indonesia. Indonesian positive law has regulated the form of legal protection for phishing victims. In Indonesia, there are various provisions on criminal sanctions for phishers. However, criminal sanctions in the form of imprisonment or fines are not enough. Victims suffer losses so they need compensation. Efforts to enable victims to obtain compensation have also been regulated. However, in practice, compensation for phishing victims still faces obstacles. The difficulty of finding phishers who can hide their real identities and digital footprints are the main obstacle to compensating phishing victims. The lack of human resources and technology is also an obstacle in handling phishing cases.

Cooperation between various parties, including law enforcement officials, lawmakers, government organizations, banks, and the public, is necessary. Cooperation includes law enforcement, legislators, banks, government organizations, and the public. This must be done to provide legal protection for phishing victims, especially regarding compensation. There is a need to strengthen cybersecurity and improve the ability to track phishers. Another effort that can be made is to educate the public about the dangers of phishing. This education is necessary so that people can avoid phishers' actions. Another solution is to create or revise existing laws and regulations by regulating compensation for victims of cybercrimes, including phishing. If the rules for compensating victims of cybercrimes are regulated by law, the practice will be much clearer than it is now. This will provide legal certainty and protection for victims.

ACKNOWLEDGEMENTS

The author would like to thank God Almighty for all His grace so the authors can complete this research. Thanks to Atma Jaya Yogyakarta University, especially the Faculty of Law, the author's parents, and the author's friends.

REFERENCES

[1] T. Y. Rahmanto, "Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," *Jurnal Penelitian Hukum De Jure*, vol. 19, no. 1, p. 31, 2019, doi: 10.30641/dejure.2019.v19.31-52.

[2] A. W. Laksana, "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif," *Jurnal Hukum*, vol. 35, no. 1, p. 52, Jun. 2019, doi: 10.26532/jh.v35i1.11044.

[3] D. T. Rachmadie and Supanto, "Regulasi Penyimpangan Artificial Intelligence pada Tindak Pidana Malware berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016," *Deleted Journal*, vol. 9, no. 2, p. 128, May 2020, doi: 10.20961/recidive.v9i2.47400.
[4] A. N. Ramadhanti, T. A. Tias, E. D. Lestari, and A. U. Hosnah, "Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia", *jptam*, vol. 8, no. 1, pp. 1299–1305, Jan. 2024.
[5] S. Tabrani, V. . Safitri, P. A. . Nayla P, and A. U. . Hosnah, "Kejahatan Phishing Ditinjau dari Perspektif Hukum dan Kejahatan Siber", *Civilia*, vol. 3, no. 1, pp. 1–13, Jan. 2024.
[6] D. J. K. Negara, "Waspada! Kehajatan Phising Mengintai Anda." https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda
[7] I. A. D. Exchange, "Laporan Aktivitas Phishing Domain Periode Q4 2023," *https://idadx.id/*
[8] S. Rahardjo, Ilmu Hukum, 8th Edition, Bandung, PT Citra Aditya Bakti, 2014.
[9] A. Priyonggojati, "Perlindungan Hukum Terhadap Penerima Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending," *JURNAL USM LAW REVIEW*, vol. 2, no. 2, p. 162, Nov. 2019, doi: 10.26623/julr.v2i2.2268.
[10] Djarawula, N. M., Alfiani, N. N., & Mayasari, N. H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) di Indonesia Ditinjau dari Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, *2*(10), 3799–3806. https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842
[11] S. Rahardjo, Hukum Progresif: Sebuah Sintesa Hukum Indonesia, Yogyakarta, Genta Publishing, 2009.
[12] F. E. Muhammad and B. Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *JURNAL USM LAW REVIEW*, vol. 6, no. 1, p. 226, Apr. 2023, doi: 10.26623/julr.v6i1.6649.
[13] E. A. P. Manurung dan E. F. Thalib, "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022", *JHS*, vol. 4, no. 2, hlm. 139–148, Jan 2023.
[14] A. F. Sutarli and S. Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia", *Innovative*, vol. 3, no. 2, pp. 4208–4221, May 2023.
[15] M. Fadli, D. Widijowati, and D. Andayani, "Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi," *Co-Value Jurnal Ekonomi Koperasi Dan Kewirausahaan*, vol. 14, no. 12, May 2024, doi: 10.59188/covalue.v14i11.4335.
[16] A. Adnani, "Penggabungan Ganti Rugi dalam Perkara Perdata Menurut Sistem Peradilan Pidana Indonesia," *Ensiklopedia of Journal*, vol. 2, no. 3, pp. 1–8, Apr. 2020, doi: 10.33559/eoj.v2i3.462.
[17] G. Y. Pramana, "Claim for Damages in Criminal Actions to Achieve Justice for Victims," *Ius Poenale*, vol. 1, no. 1, pp. 39–50, Sep. 2020, doi: 10.25041/ip.v1i1.2066.
[18] F. T. Wahyuono, "Reformasi Regulasi Penggabungan Gugatan Ganti Kerugian dalam Hukum Acara Pidana," M. H. thesis, Faculty of Law., Universitas Islam Indonesia, Yogyakarta, 2023.
[19] I. Sari, "Perbuatan Melawan Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata," *Jurnal Ilmiah Hukum Dirgantara*, vol. 11, no. 1, Sep. 2020, doi: 10.35968/jh.v11i1.651.
[20] S. Chairunnisa, T. Murwadji, and N. Harrieti, "Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia", *Hakim*, vol. 2, no. 1, pp. 01-16, Dec. 2023.
[21] Asumsi, "Viral Uang Rp110 Juta Milik Nasabah Jenius Raib, Seberapa Aman Bank Digital?" https://asumsi.co/post/61093/viral-uang-rp-110-juta-milik-nasabah-jenius-raib-seberapa-aman-bank-digital/
[22] A. A. Agus and Riskawati. "Penanganan KasusCybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)." *Jurnal Supremasi*, Vol. 10, No. 1, 2016.
[23] Y. Yosefine, R. S. Agustina, and D. Agus, "Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan Phishing (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius)," *Yustisia Tirtayasa Jurnal Tugas Akhir*, vol. 3, no. 1, p. 57, Apr. 2023, doi: 10.51825/yta.v3i1.17650.
[24] Y. A. Nugraha and T. Saputra, "Penerapan Hukum Terhadap Tindak Pidana Doxing di Indonesia," *Jurnal Hukum Pelita*, vol. 5, no. 1, pp. 1–12, May 2024, doi: 10.37366/jh.v5i1.2670.
[25] M. D. Purwandari, "Analisis POLDA Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus Phishing," S. Ak. Thesis, Faculty of Business and Economics, Universitas Islam Indonesia, Yogyakarta, 2024.
[26] S. Mertokusumo, Hukum Acara Pedata Indonesia, Genta Publishing, Yogyakarta, 2021.
[27] D. S. Sinaga and A. Syahputra, "Tinjauan Yuridis terhadap Putusan Niet Ontvankelijke Verklaard dalam Perkara Gugatan Kurang Pihak," *Jurnal Hukum*, vol. 39, no. 1, p. 40, Apr. 2023, doi: 10.26532/jh.v39i1.30696.

BIOGRAPHIES OF AUTHORS

	**Olivia Audriana Putri**, Undergraduate Student, Faculty of Law, Atma Jaya Yogyakarta University. Email: oliviaaudr@gmail.com
	**E. Imma Indra Dewi Windajani**, Lecturer of Atma Jaya Yogyakarta University (1995–present). Undergraduate program: Atma Jaya Yogyakarta University (1990–1995). Master program: Gadjah Mada University (2002–2005). Doctoral program: Gadjah Mada University (2016–2023)**.** Area of expertise and interest: Law Business, Labour Law, Human Right, Disability Email: imma.dewi@uajy.ac.id