Phishing as Cybercrime: an Overview of Law Enforcement Problems in Indonesia

Virginia Harizta Vianne
{virginia130970@gmail.com}

Attorney District of Metro / Doctoral of Law Program University of Lampung

Abstract. Besides various positive impacts from the growth of technology, in reality technology growth also bring various negative impacts. One of negative impact is cybercrime. Basically, there are various types of cybercrime, one of which is phishing which currently often occurs in Indonesia. Problems arise when legal provisions related to cybercrime are oriented towards retaliation against phishing perpetrators, while the victims who get so much losses are forgotten because there is no legal provision. Based on that, this research will formulate two problems, namely: What are the legal provisions related to phishing in Indonesia? and how is law enforcement in various phishing cases? This study is normative in nature and employs statutory approach and case approach. It is hoped that the research results will be able to identify legal provisions related phishing and review law enforcement problems in phishing cases in Indonesia. This research will also provide ideas as a response to identifying problems in law enforcement related phishing in Indonesia.

Keywords: Cyber Crime, Law Enforcement, Phishing.

1 Introduction

Current advances in information and communication technology have shown extraordinary progress and impact on various aspects of life. Basically, technological progress aims to have a positive impact by making human life easier. However, apart from having positive impacts, there are also various negative impacts from technological progress.[1] One of the negative impacts of technological progress is the occurrence of cybercrimes.[2] Cybercrimes refer to a crime committed with the concept of criminality that uses the internet as an intermediary in committing crimes.[3] This is proven in the following data in Figure 1:

MIC 2023, October 28, Jakarta, Indonesia

DOI 10.4108/eai.28-10-2023.2341666

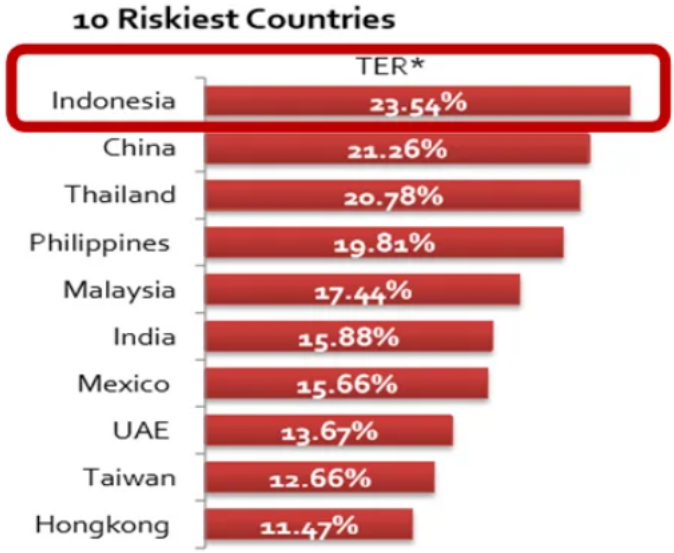

Fig 1. Data on Countries Most at Risk of Cybercrimes

In 2016, Indonesia was named the country most at risk of cybercrimes.[4] In basic terms, cybercrime could be a term that alludes to criminal action in which a computer organize is the instrument, target or put where the wrongdoing happens. This incorporates carding, spamming, phishing, hacking, breaking, ruining, online sell off extortion, check fraud, certainty extortion, character extortion, child explicit entertainment, etc. [5] There is data that shows the types of cybercrimes that most often occur in the world as in Figure 2 below:

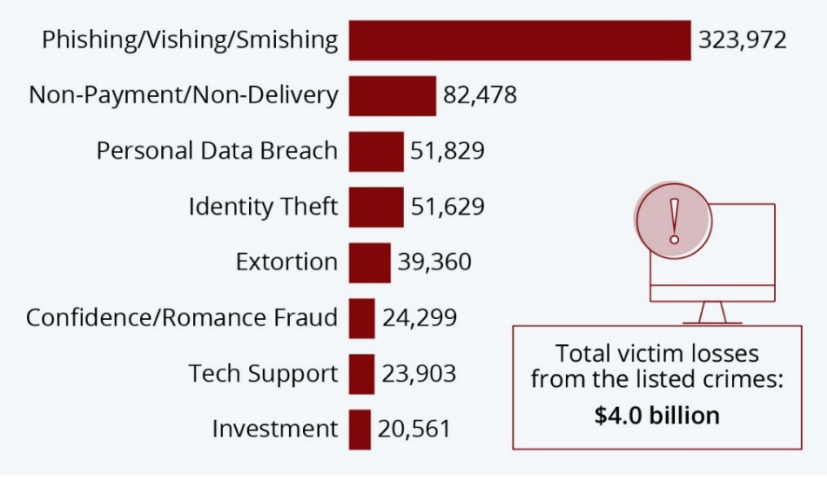

Fig 2. Types of Cybercrimes that Most Occur in the World [6]

Based on data from the FBI, the type of cybercrime that occurs most frequently in the world is phishing. Apart from phishing, there are various other types of cybercrimes with losses experienced by victims of up to 4 billion dollars.[6] Phishing could be a frame of action that undermines or traps somebody with the concept of attracting that individual. This wrongdoing

is committed by deluding somebody so that the individual in a roundabout way gives all the data the trapper needs. Phishing is included in cybercrime, which right now criminal acts are wild through computer systems.[7]

The financial sector is one of the industries that is the target of phishing crimes. The report also explains that phishing crimes in the financial sector in 2021 are still a crime that often occurs. Additional cases also occurred, in 2020 the number of phishing crimes was 22.5%, while in 2021 it rose to 29.2%. The threat of phishing attacks for mobile users in Indonesia is quite high. Various efforts are needed to overcome the threat of phishing. This needs to be done because phishing crimes will continue to increase. As more and more financial industries switch to digital services, the opportunities and increase in crime will automatically continue to increase.[8]

Efforts to overcome phishing crimes are also needed from a legal aspect. This is considering the impact of phishing crimes which result in hundreds of people losing up to billions of rupiah. For example, on January 20 2023, the Criminal Investigation Unit of the Republic of Indonesia Police arrested the perpetrator of phishing with 493 people becoming victims in this phishing case. The losses incurred are estimated at IDR 12 billion.[9] Based on this, it can be seen that the losses due to phishing are quite large and cannot be underestimated.

Crime has been accepted as a fact that is detrimental to society, namely the victim. The losses incurred can be in the form of material or moral losses. Material losses in the form of crime victims and heavy damage or destruction of objects as well as increased costs that must be incurred to overcome them. Moral loss in the form of reduced or lost public trust in the implementation of law enforcement carried out by legal officers.[10] Therefore, there is a need for research that discusses phishing as a means of scientific insight into the public regarding the dangers of phishing crimes. As well as a means of insight for law enforcement officials in dealing with phishing. Based on that, this research will formulate two problems, namely: What are the legal provisions related to phishing in Indonesia? and how is law enforced in various phishing cases in Indonesia? This research is normative research that uses statutory approach and case approach.

2 Discussion

2.1 Legal Provisions Related to Phishing in Indonesia

Phishing is an attempt to obtain information using phishing techniques. Phishing data is personal data entered by the victim on a fake page that is cloned from a certain page. Phishing activities aim to lure people into providing personal information voluntarily without realizing it. If the phishing website is successful, the data obtained will be used for crimes, including:[11]

a. Sell the obtained information.
b. Using it for political purposes.
c. Committing fraudulent acts.
d. Breaking into other verified accounts using existing data.
e. Making online loans in the name of the victim.

Indonesia already has laws and regulations related to the crime of electronic transaction fraud phishing, these laws and regulations include:[12]

a. Internet and Online Transactions Law (ITE Law) No. 11 in 2008.

b. Indonesia Criminal Code: Article 362, 378, 335, 311, 303, 282, 406.
c. Law No. 28 of 2014 related Copyright.
d. Telecommunications-related Law No. 36 on 1999.
e. Broadcasting Law No. 32 on 2002.

The obligation of phishing culprits as directed in Article 45 (2) of the ITE Law will be rebuffed by detainment for a greatest of six a long time and/or a fine of a greatest of IDR 1,000,000,000.00.[13] Then related to phishing victims according to the ITE Law, this form of fulfilling the right to protection for victims. In an electronic transaction or cybercrime is only marked by the existence of a form of case resolution in the form of criminal provisions for acts prohibited in this law for offenders. It's as stated in ITE Law of Article 45 to Article 52 related through detention and or penalties. In Indonesia, there are laws and regulations that specifically regulate the protection of victims, namely Law 31 of 2014 regarding Prisons towards Law 13 of 2006 regarding the Safekeeping of the Witnesses and Casualties accompanied by LPSK or the Witnesses and Causalities Safety Organization. It is an active institution to help witness and/or causalities various criminal offenses to obtain protection and fulfill their rights.[14]

Phishing casualties who fundamentally have to fulfill the fabric misfortunes they have experienced. The Law on the Assurance of Witnesses and Casualties known as UUPSK, states that there's security for casualties and/or witnesses of criminal acts, namely within the shape of Remuneration, Compensation, and Help. With respect to fabric misfortunes for casualties of cybercrime within the shape of phishing, compensation is a suitable strategy. As Article 1 Number 11 states that "Compensation is remuneration given to the casualty or their family by the culprit or third party."[15]

2.2 Law Enforcement in Various Phishing Cases in Indonesia

The existence of various legal provisions related to cybercrime in Indonesia, as explained in the previous sub-chapter, in fact does not make phishing perpetrators afraid to commit their crimes. In fact, phishing still continues to occur in Indonesia. The regulations related to cybercrimes have shortcomings such as duplication of regulations. As in the ITE Law with the Criminal Code as a result of the criminalization of conventional crimes into electronic transaction crimes. The content material is no longer relevant because the regulations governing conventional crimes cannot continuously be included within the category of electronic exchange wrongdoings within the Criminal Code and the Managing an account Law. Then the regulations that are no longer valid are replaced with new regulations within Govt. Regulation 82 in 2012 Regarding Transactions and Electronic Systems. This deficiency is also exacerbated by the fact that society is not yet ready for the consequences of the development of electronic transactions.[16]

The legal regulation of phishing is considered to have legal ambiguity regarding the legal regulation of cybercrime in the form of phishing because there is no article that includes concrete compensation for victims. Before the formation of the ITE Law, cybercrime cases in Indonesia were tried by applying articles that were in conformity with the requirements within the Penal Code of Conduct well punishment for cybercrime perpetrators used this Criminal Code. Section 378 within the penal code allows the employment of criminal provisions in cybercrime cases involving phishing. Legal regulations for cybercrime in the form of phishing are regulated in Article 378 of the Criminal Code concerning fraud. The use of Section 378 at penal code in prosecuting cybercrime cases is only carried out based on interpretation because there are differences

in the types of cybercrime crimes with existing conventional crimes. Even though the methods of phishing and fraud in the Criminal Code have similar elements of action, there are still differences starting from the form of the criminal act, in determining the locus of delicti to the tempo of the delicti. Cybercrime is a grouping of types of criminal acts which is a new category, because cybercrime follows rapidly developing technological developments. This requires the existence of clear special regulations in dealing with cybercrime crimes.[17]

At that point the legitimate control of cybercrime within the phising shape of as regulated in ITE Laws is that criminal sanctions cannot be forced. This is often since Section 35 within tandem to Section 51 point (1) does not contain components of lies that hurt other individuals also in Section 28 point (1) in conjunction with Article 45A passage (1). These pieces don't include parts related to fraud, such as the generation of digital data as well as digital files from the utilization of tools. The goal is to handle digital information and/or digital files as if it consisted of genuine content. It means that they do not contain elements of someone creating a site that looks like the original official site. Phishing is an act of creating a site that looks like the original site, but the site is fake. Then phishers also carry out lies to direct other people to access the fake site to enter confidential personal information and this is then discovered by the phisher. As a result, the ITE Law has created a legal void in the legal control of cybercrime in the form of phishing. The regulatory objective towards cyberattacks by means of phishing in the terms of the ITE Law is to include modifications within the ITE Law by explicitly and forcefully outlining the idea of phishing. It is also necessary to change the content and elements of Article 35 so that Article 35 can then be applied and/or imposed on perpetrators of cybercrime in the form of phishing.[18]

In line with this, the shortcomings contained in statutory regulations affect the efficacy with which legislative rules against phishing offenses are being implemented in law enforcement in Indonesia. This is proven that the regulations used in resolving cases of phishing fraud crimes are only regulations that do not follow developments in electronic transaction technology. So that it does not have a deterrent effect on perpetrators or banks that are weak in monitoring the confidentiality of customer data. The implementation of the ITE Law in enforcing phishing fraud in Indonesia still has shortcomings, including:[19]

a. People who use technology freely, which means that people are truly apathetic and not recognize the limitations of the prohibitions contained in the ITE Law.
b. The thinking and abilities of the Indonesian people are considered not to fully understand the consequences of using electronic transactions. All electronic transaction activities are considered to be safe so that no illegal actions will occur. This clearly defines the role of the ITE Law in law enforcement against cybercrimes such as phishing.
c. The factor is that law enforcement is less strict in following up on cases of electronic transactions such as phishing fraud so that it does not have a deterrent effect, even though these crimes can disturb the community.

Tackling cybercrimes through phishing must follow current developments. To tackle these crimes, criminology can be used as a basis for understanding cybercrime perpetrators through phishing, which then provides a strong picture of cybercrime. Criminological studies of cybercrime through phishing can be studied using a cyber criminology approach because cyber criminology is able to provide an explanation of crimes against cyberspace. As well as routine activity theory, which sees crimes targeted

at targets who do not understand technology. Apart from that, there is no protection of data privacy and there is motivation so that the government can take action by providing guidance, guarding and using technology for technology users. Based on social control theory, it can also provide an analysis of the factors that cause cybercrime through phishing to provide prevention so that cybercrime does not occur through phishing. So that the study can be used as evaluation material for policy makers in terms of overcoming cybercrime by using theories in criminology as future law builders.[20]

3 Conclusions

The legal provisions governing cyber phishing in Indonesia are contained in several regulations, namely: ITE Law, Criminal Code, Act 28 in 2014 regarding Copyright, Act 36 in 1999 regarding Telecommunications and Act 32 in 2002 concerning Broadcasting. The existence of various legal provisions related to cybercrime in Indonesia, in fact does not make phishing perpetrators afraid to commit their crimes. Even phishing still continues to occur in Indonesia. The regulations related to cybercrimes have shortcomings such as duplication of regulations. Apart from that, the legal regulation of phishing is considered to have caused legal ambiguity regarding the legal regulation of cybercrime in the form of phishing because there is no article that includes concrete compensation for victims. Thus, the problem of law enforcement in phishing crimes is due to legal provisions that do not follow current developments and needs.

References

[1] Wirasaputra, Ardy, Fikri Riduan, Pramudhya, Riyan, Zulkahfi, and Widyah Noviana. "Dampak Dari Perkembangan Teknologi Informasi Dan." *Jurnal Kreativitas Mahasiswa Informatika* 3, no. 2 (2022): 206–10. http://openjournal.unpam.ac.id/index.php/JATIMIKA/article/viewFile/16943/11413.

[2] Supanto. "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy." *Yustisia Jurnal Hukum* 5, no. 1 (2016). https://doi.org/10.20961/yustisia.v5i1.8718.

[3] Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426. https://jurnalfsh.uinsby.ac.id/index.php/qanun/article/view/1132.

[4] "Cyber Crime Indonesia - Waspadailah! Hantaman Serangan Cyber." Accessed September 18, 2023. https://proxsisgroup.com/cyber-crime-indonesia/.

[5] Sulisrudatin, Nunuk. "Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit." *Jurnal Ilmiah Hukum Dirgantara* 9, no. 1 (2014): 26–39. https://doi.org/10.35968/jh.v9i1.296.

[6] "Chart: The Most Common Types of Cyber Crime | Statista." Accessed September 18, 2023. https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/.

[7] Wibowo, Mia Haryati, and Nur Fatimah. "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime." *JOEICT(Jurnal of Education and Information Communication Technology)* 1, no. 1 (2017): 1–5. https://www.jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69.

[8] Nur Latifah, Fitri, Imron Mawardi, and Bayu Wardhana. "Threat of Data Theft (Phishing) Amid Trends in Fintech Users During the Covid-19 Pandemic (Study Phishing In Indonesia)." *Perisai : Islamic Banking and Finance Journal* 6, no. 1 (2022): 74–86. https://doi.org/10.21070/perisai.v6i1.1598.

[9] Indonesia, CNN. "Bareskrim Tangkap 13 Tersangka Penipuan Link Phising, Korban 493 Orang," 2023. https://www.cnnindonesia.com/nasional/20230120102615-12-902941/bareskrim-tangkap-13-tersangka-penipuan-link-phising-korban-493-orang.

[10] Purwanti, Yuli, Fathur Rachman, Tedi Gunawan, and Andriansyah Kartadinata. "Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung." *Audi Et AP : Jurnal Penelitian Hukum* 2, no. 01 (2023): 64–71. https://doi.org/10.24967/jaeap.v2i01.2088.

[11] Hayati, Malahayati, and Darul Fata. "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising." *Djtechno Jurnal Teknologi Informasi* 2, no. 1 (2021): 21–28. https://doi.org/10.46576/djtechno.v2i1.1252.

[12] Dm, Yusuf, Addermi, and Jasmin Lim. "Kejahatan Phising Dalam Dunia Cyber Crime Dan Sistem Hukum Di Indonesia." *Jurnal Pendidikan Dan Konseling* 4, no. 5 (2022): 8018–23.

[13] Aditya, Ande, Iman Ferrary, Sri Hartini, Prihatini Purwaningsih, Universitas Ibn, Khaldun Bogor, Data Pribadi, and A Pendahuluan. "Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang." *Yustisi: Jurnal Hukum Dan Hukum Islam* 10, no. 2 (2023): 1–12.

[14] Saristha, Tuage Natalia. "Perlindungan Hukum Terhadap Saksi Dan Korban Oleh Lembaga Perlindungan Saksi Dan Korban (Lpsk)." *Lex Crimen* 2, no. 2 (2013): 56–64.

[15] Warsiti, and Tuti Markoni. "PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN CYBER CRIME BERBENTUK PHISING DALAM TRANSA." *Jurnal Multidisiplin Indonesia* 10, no. 10 (2022): 1109–25.

[16] Yustitiana, Rhesita. "PELAKSANAAN PENGATURAN HUKUM TINDAK KEJAHATAN FRAUD PHISHING TRANSAKSI ELEKTRONIK SEBAGAI BAGIAN DARI UPAYA PENEGAKAN HUKUM DI INDONESIA DIKAITKAN DENGAN TEORI EFEKTIVITAS HUKUM." *Jurnal Hukum Visio Justisia* 1, no. 1 (2021): 98–126.

[17] Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal Usm Law Review* 6, no. 1 (2023): 226. https://doi.org/10.26623/julr.v6i1.6649.

[18] Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1, no. 2 (2021): 68–81. https://doi.org/10.22437/pampas.v1i2.9574.

[19] Setiawan, Radita, and Muhammad Okky Arista. "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana." *Recidive* 2, no. 2 (2013): 139–46. https://jurnal.uns.ac.id/recidive/article/viewFile/32324/21500#:~:text=Di dalam Undang-Undang Nomor,pengguna dan penyelenggara Teknologi Informasi.

[20] Ode, La, and Muhammad Ichsan. "KAJIAN SOSIOLOGI KRIMINAL TERHADAP PENANGGULANGAN CYBERCRIME MELALUI PHISING." *Jurnal Darussalam: Pemikiran Hukum Tata Negara Dan Perbandingan Hukum* 1, no. 1 (2018): 39–48.

[21] Gani, Alcianno G. "Cybercrime (Kejahatan Berbasis Komputer)." *Jurnal Sistem Informasi Universitas Suryadarma* 5, no. 1 (2014): 16–29. https://doi.org/10.35968/jsi.v5i1.18.

[22] "Indonesia Peringkat 4, Ini Dia 7 Negara Pengguna Internet Terbesar Di Dunia - GoodStats Data." Accessed September 18, 2023. https://data.goodstats.id/statistic/agneszefanyayonatan/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-FLw6V.

[23] "Naik 1,03%, Pengguna Internet Di Indonesia 2022 Capai 204,7 Juta | Headline.Co.Id." Accessed September 18, 2023. https://www.headline.co.id/15918/naik-103-pengguna-internet-di-indonesia-2022-capai-2047-juta/.