International Journal of Law and Society
Vol. 1, No. 2, April 2024
e-ISSN : 3046-9562, p-ISSN : 3046-9619, Page 56-66

Law Enforcement Efforts Against Criminal Offences Of Fraud Based On Online / Electronic Transactions

Satria Muhammad [1], Syiful Asmi Hasibuan [2]
[1,2] Universitas Pembangunan Panca Budi

Jl. Gatot Subroto Km.4,5 Sei Sikambing 20122 Kota Medan, Sumatera Utara
Korespondensi penulis: satriamhd260497@gmail.com

Abstract. *Fraudulent acts are currently flourishing following the era and technology advancement. Laws and regulations are made to anticipate this, but the existing laws and regulations seem like unable to combat the crime amid their increase in occurrences. This research aims to: firstly, to identify law enforcement against the e-commerce-based frauds; and secondly, to identify the obstacles in criminal law enforcement against e-commerce-based frauds. This research was conducted by using normative juridical method through literature research by examining secondary data including legislation, research results, scientific journals and references. The research results describe that the e-commerce- based fraudulent acts in principle are similar to the conventional frauds but differ in the evidences or means of action as the latter uses electronic systems (computers, internet, telecommunications equipment). Therefore, the legal enforcement against this kind of frauds is still under the applicability of the Indonesian Criminal Code and the Law No. 19 of 2016 regarding Amendments to the Law No. 11 of 2008 regarding Information and Electronic Transactions. Further, the law enforcement against the fraudulent acts in electronic-based transactions has been prevented at least by the following five factors, the laws and regulations, law enforcers, infra-structure or facilities that support the law enforcement, community and cultural factors.*

Keywords: *Law Enforcement; Fraud; Electronic Transactions.*

INTRODUCTION

Electronic Information and Transactions is one that is often used in everyday life in the form of mobile phones, laptops, the internet, internet banking, social media (which includes the internet network), e-money, and others that include electronics and information. In this case there are always limits and regulations in the use of information and electronic transactions. Making laws and regulations on the use of Information Technology and Electronic Transactions requires the principles of legal certainty, benefits, prudence, good faith, and freedom of choice of technology or technology neutral. And to guarantee recognition and respect for the rights and freedoms of others and to fulfil fair demands in accordance with considerations of security and public order in a society.

The making of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions in order to realise justice, public order and legal certainty. In making laws and regulating article by article to anticipate and regulate the legal system against crimes that often occur in cyberspace commonly referred to as "cybercrime" or often called Cyber Crime, there must be firmness in eradicating crimes against Cyber and taking action against a Cyber Crime committed by the perpetrator, this is to build public confidence in the use of computers and computer networks so that there are no obstacles when using it.

Received March 31,2024; Revised April 04,2024; Published April 30, 2024
* Satria Muhammad, satriamhd260497@gmail.com

Online fraud is one of the cyber crime criminal offences because it uses software or electronic media to commit fraud. Online fraud is usually charged with the ITE Law although Article 28 paragraph (1) of the ITE Law does not specifically explain online fraud. Article 28 paragraph (1) of the ITE Law states that every person intentionally, and without the right to spread false and misleading news that results in consumer losses in electronic transactions. Article 45 paragraph (1) of the ITE Law states that every person intentionally and without the right to spread false and misleading news that results in consumer harm in electronic transactions as referred to in article 28 paragraph (1) of the ITE Law shall be punished with a maximum imprisonment of 6 years and or a maximum fine of Rp 1 billion.

Cyber crime itself is a crime that starts with computers or computer networks as its main element. The term occurs because basically these activities where computers and computer networks are used for Online fraud is one type of e-commerce crime is the use of software or internet services with the aim of deceiving or taking advantage of victims, such as stealing personal data or information that can trigger identity theft. Cybercrime in a broad sense is all forms of crime directed against computers, computer networks and their users, and traditional forms of crime using or with the help of computer equipment. One type of crime by utilising the internet media is fraud with electronic transaction mode.

One that often occurs is Cyber Crime Phishing, people often do not realise that Cyber Crime Phishing is very detrimental to victims who have experienced this crime.

Phishing (password harvesting fishing) is a crime of fraud by using fake emails or fake websites that aim to trick other users. The use of fake emails or fake websites is intended to obtain user data. The use of user data is often to send an email that seems to come from an official company, for example a bank with the aim of obtaining a person's personal data, such as User ID, PIN, account number, credit card number and so on.

As for the case or cases that have occurred in Cyber Crime Phishing, namely the theft of a person's User ID under the guise of link fraud to commit crimes in the form of hate speech and the spread of false news or hoaxes, the perpetrator does this using a person's user ID to manipulate the public, so the public thinks it is the victim's action, even though there is someone who is the real perpetrator who controls the victim's user ID.

In this case, the defendant is legally and convincingly proven guilty of committing the crime of "Intentionally and without the right to distribute and make accessible Electronic Information and Electronic Documents that contain insults and defamation", as regulated and punishable in Article 45 paragraph (3) of Law of the Republic of Indonesia No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and

Transactions jo. Article 27 paragraph (3) of Law No. 11 of 2008 on Electronic Information and Transactions as in the First Subsidiary Indictment of the Public Prosecutor. Judging from the example of the case or cases above, the decision of the Panel of Judges of the Medan District Court with Decision No. 3006/Pid.Sus/2017/P: 3006/Pid.Sus/2017/PN.Mdn, decided to sentence the perpetrator with Cyber crime, which began with Phishing with the aim of conducting hate speech and spreading false news or hoaxes.

THEORETICAL REVIEW

A theoretical framework is a conceptual structure used to structure and organise ideas, concepts, or propositions in a research or study. The theoretical framework assists researchers in designing and explaining the relationship between the variables under study and provides a foundation for developing hypotheses or understanding observed phenomena.

Theoretical frameworks play an important role in research as they assist researchers in formulating relevant research questions, planning appropriate research methods, analysing data, and interpreting research results more systematically. Theoretical frameworks also allow researchers to structure their findings into a broader context and enhance understanding of the phenomenon under study. "law enforcement theory" refers to a conceptual framework or approach used to explain how laws are enforced in a society. It encompasses various views and strategies used by law enforcement agencies, such as police, prosecutors, and courts, as well as factors that influence the implementation of the law. Some common theories of law enforcement include:

1. Deterrence Theory: This theory argues that strict and effective law enforcement can deter crime by intimidating individuals from breaking the law for fear of the consequences.
2. Reintegrative Shaming Theory: This concept emphasises the importance of restoring social relationships between offenders, victims and the community after an offence, by using mechanisms such as shame and remorse to change behaviour.
3. Labeling Theory: This theory highlights how law enforcement can affect an individual's identity by labelling them as "lawbreakers", which can exacerbate their criminal behaviour through stigmatisation.
4. Restorative Law Enforcement Theory: This approach emphasises the restoration of relationships damaged by crime through dialogue, reconciliation and personal responsibility, involving the offender, victim and community in the recovery process.

5. Community-Based Law Enforcement Theory: This is an approach where the community is actively involved in the law enforcement process, by co-operating with law enforcement agencies to prevent crime and improve the environment.
6. Critical Law Enforcement Theory: This theory examines conflicts of interest and inequality in law enforcement, as well as how power structures and ideologies affect the implementation of law in society.
7. Procedural Justice Theory: Highlights the importance of fair treatment and transparent procedures in the justice system to ensure public confidence in law enforcement.

RESEARCH METHODS

This research method uses 2 kinds of approaches, namely a statute approach and a conceptual approach. Normative legal research is also called library research or document study, because this research is conducted or aimed only at written regulations or other legal materials. The research specification in this study is to use a statutory approach, namely the approach intended to look carefully and analyse all laws and other regulations related to the legal issues currently being faced. This research uses normative juridical, namely by collecting data by means of library research.

Library research is a type of research by collecting materials related to research that comes from scientific journals, various kinds of literature, and from this research. The sources of legal materials that this research uses are primary and secondary legal materials. Primary legal materials are legal materials that are authoritative, that is, have authority. Legal material consists of legislation, official records.

Primary legal materials used in this research include the 1945 Constitution (UUD 1945), Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP), Law Number 73 of 1958 concerning Declaring the Enactment of Law No. 1 of 1946 of the Republic of Indonesia concerning Criminal Law Regulations for the Entire Territory of the Republic of Indonesia and Amending the Criminal Code (KUHP), Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Witness and Victim Protection (UU PSK). Secondary legal materials are legal documents or materials that provide explanations of primary legal materials such as books, articles, journals, research results, papers and so on that are relevant to the issues to be discussed. Secondary legal materials used by this research include: books, and legal journals.

The data analysis technique used is by means of qualitative analysis which is explained descriptively to describe how criminal responsibility for the perpetrator.

RESULTS AND DISCUSSION

Indonesia does not yet have a special law/cyber law that regulates cybercrime However, there are several other positive laws that apply generally and can be imposed on cybercrime offenders, especially for cases that use computers as a means, including:

a. Criminal Law Code

Articles in the Criminal Code are usually used more than one Article because it involves several acts at once articles that can be imposed in the Criminal Code on cybercrime, namely:

1. Article 362 of the Criminal Code is charged for carding cases where the perpetrator steals another person's credit card number, although not physically because only the card number is taken by using card generator software on the Internet to make transactions in e-commerce. After the transaction is made and the goods are delivered, then the seller who wants to cash out the money at the bank is rejected because the card owner is not the person who made the transaction.
2. Article 378 of the Criminal Code can be charged for fraud by ostensibly offering and selling a product or goods by placing an advertisement on a website so that people are interested in buying it and then sending money to the advertiser. However, in reality, the goods do not exist. This is known after the money is sent and the goods ordered do not arrive so that the buyer becomes deceived.
3. Article 335 of the Criminal Code can be applied to cases of threats and extortion made through e-mail sent by the perpetrator to force the victim to do something in accordance with what the perpetrator wants and if not carried out will have a harmful impact. This is usually done because the perpetrator knows the victim's secret.
4. Article 311 of the Criminal Code can be charged for defamation cases using the Internet. The modus operandi is that the perpetrator distributes an email to the victim's friends about a story that is not true or sends an email to a mailing list so that many people know about the story.
5. Article 303 of the Criminal Code can be imposed to ensnare gambling games conducted online on the Internet with organizers from Indonesia.
6. Article 282 of the Criminal Code can be imposed for the distribution of pornography and pornographic websites that are widely circulated and easily accessible on the Internet.

c. According to Article 1 point (1) of Law No. 36 of 1999 on Telecommunications or Law No. 11 of 2008 on the Internet & Electronic Transactions, telecommunication is any transmitting, sending, and/or receiving of information in the form of signs, signals, writings, pictures, sounds, and noises through wire, optical, radio, or other electromagnetic systems. From this definition, the Internet and all of its facilities are a form of communication tool because it can send and receive any information in the form of pictures, sounds and movies with an electromagnetic system. Misuse of the Internet that disturbs public or private order can be sanctioned by using this Law, especially for hackers who enter other people's network systems as stipulated in Article 22, namely Everyone is prohibited from committing acts without rights, unauthorized, or manipulating the Internet:

1. Access to telecommunication networks
2. Access to telecommunication services
3. Access to a dedicated telecommunications network

Personal data protection in preventing phishing is very necessary in this case. Personal data protection can be divided into two, namely general and specific. General means personal data that is generally obtained in access to public services or listed in official identity. Specific personal data means that the personal data is sensitive to the security and comfort of the life of the owner of the personal data, besides that to obtain specific personal data, the owner of the personal data must first agree. From the various types of crimes described above, the point in this research is the type of cybersquatting crime which specifically is phishing.

Phishing is one type of crime that should be watched out for because accuracy and accuracy in the use of electronic media are the main factors so as not to get caught in this phishing. In Indonesia, many people utilize the internet network to follow global developments, from the use of social media to banking transactions using electronic media that tend to be targeted by cyber criminals in this type of phishing. Cyber crime in the form of phishing is a cybercrime crime that makes data falsification on a fake website that looks similar to the original website, but has the same goal of obtaining information about other people's identities that will be used illegally without the knowledge of the original owner.

This discussion discusses the legal regulation of phishing which is considered to have occurred legal vagueness regarding the legal regulation of cyber crime in the form of phishing because of the absence of articles that include compensation for victims in a concrete manner. Before the formation of the ITE Law, cyber crime cases in Indonesia were tried by applying articles that have elements in the Criminal Code so that the criminalization of cyber criminals using the Criminal Code.

In the Criminal Code, criminal provisions in the case of cyber crime in the form of phishing can be used based on Article 378 of the Criminal Code. Legal arrangements against cybercrime in the form of phishing are regulated in Article 378 of the Criminal Code on fraud as it is known that phishing is generally an act of fraud. Fraud formulated in Article 378 of the Criminal Code is: "Whoever, with intent to unlawfully benefit himself or another, by using a false name or false dignity, by deceit, or a series of lies, induces another person to deliver any property to him, or to give a debt or to cancel a debt, shall, being guilty of fraud, be punished by a maximum imprisonment of four years". The use of Article 378 of the Criminal Code in the criminalization of cybercrime cases is only carried out based on interpretation because there are differences in the types of cybercrimes with existing conventional criminal acts, although the methods of phishing and fraud in the Criminal Code have similar elements of action but there are still differences ranging from the form of criminal acts, in determining the locus delicti to the tempos delict.

The ITE Law imposed on the perpetrators of phishing, the types are imprisonment and fines, there is no threat of additional criminal sanctions. So the criminal system used does not have an innovative type of criminal sanction that is unique to criminal acts in the field of information and electronic transactions.The legal regulation of criminal acts of phishing compensation for victims of perpetrators is charged with Article 28 paragraph (1) of the ITE Law, the criminal provisions can be seen in Article 45A paragraph (1) stipulates that: "Every person who fulfills the elements as referred to in Article 28 paragraph (1) or paragraph (2) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah)".

The ITE Law only explains that the form of fulfillment of the right to protection for victims in an electronic transaction or cyber crime is only given a solution in the form of a form of case settlement in the form of criminal provisions aimed at the perpetrators of criminal acts where this is stated in Article 45A paragraph (1) of the ITE Law, the penalty is imprisonment and / or a fine.

This is clearly contrary to the Restorative Justice Theory which supports the resolution of criminal cases not to provide suffering to the perpetrators, but to try to give the burden on the perpetrators to be responsible for the losses caused to victims and society. Restorative Justice Theory is also considered to be the philosophical basis for the application of imprisonment as an ultimum remedium, so that Restorative Justice Theory is more suggestive of monetary criminal sanctions such as fines and compensation.

Material loss for victims of cyber crime in the form of phishing, restitution is the right method. As in Article 1 point 11 which states that "restitution is in the form of compensation given to the victim or his family by the perpetrator or third party." This is also regulated in Article 1 point 8 of Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Witness and Victim Protection, which states, "protection is all efforts to fulfill rights and provide assistance to provide a sense of security to witnesses and / or victims who must be implemented by LPSK or other institutions in accordance with the provisions of this law. The Law on Witness and Victim Protection is still facultative, because it depends on the decision of the LPSK to fulfill the rights of witnesses and victims. Another weakness is: this law does not explain further on what criminal offenses restitution can be submitted, so law enforcers do not necessarily facilitate victims to apply for the right to restitution. The submission of the victim's right to restitution becomes an uncertainty, which leads to the uncertainty of the type or qualification of the criminal offense as a requirement. The general rule of Criminal Code does not recognize the type of 'compensation punishment'. Conditional punishment that contains compensation under Article 14c of the Criminal Code on conditional punishment is basically not criminal in nature and is only a substitute to avoid or not to undergo punishment.

Criminal law must be used as an effective and efficient effort to restore the situation, so there are 2 important things needed here, namely: First, the equality of imprisonment with other economic sanctions such as fines. Second, the application of restorative justice as an effort to restore the situation between the perpetrator, the victim, and the state. As revealed by Marilyn Armour with the theory of restorative justice that sees "crime is a broken relationship between three players: the perpetrator, the victim and the community." This change in the concept of punishment is needed because the consequences caused by imprisonment are greater in negative effects and do not prove its success in reducing crime rates. This change in the concept of punishment is necessary because the consequences of imprisonment are greater than the negative effects and have not proven its success in reducing the crime rate.

Policy in legislation is absolutely necessary for law enforcers and the government to overcome and take action against criminals, as well as cyber crime, of course the type of statutory law must be in accordance with the type of crime and the way to uncover cases of cyber crime. The government of the Republic of Indonesia is committed to fighting cybercrime. The enactment and ratification of the 2008 Electronic Information and Transaction Law, or the 2008 ITE Law, is a new chapter for the government of the Republic of Indonesia to fight crimes based on communication and information technology.

The more rapid the use of technology, the more vulnerable to the level of crime committed by irresponsible people to carry out their actions both fraud, theft and defamation via the internet. This chapter will explain and what are the efforts made by the Indonesian government in taking action against information and communication technology-based crimes both domestically and by international syndicates operating in the sovereign territory of the Unitary State of the Republic of Indonesia. Policy to combat cyber crime policy is defined as a series of concepts and principles that become the outline and basis of plans in the implementation of a job, leadership, and how to act about government, organization and so on. Statement of ideals, objectives, principles and guidelines for management in an effort to achieve goals.

Public policy can be national, regional or local such as laws, government regulations, presidential regulations, ministerial regulations, regional or provincial regulations, governor's decisions, district or city regulations, and decisions of the regent or mayor, Terminology of public policy (public policy) is apparently a lot, depending on the angle from which to interpret it Easton provides a definition of public policy as the authorative allocation of values for the whole society or as a forced allocation of values to all members of society.

How to overcome the crime of Phsising itself can be said to be not as easy as imagined. Of course, the police need an active role from the community to report various kinds of phishing actions that occur. If you experience or become one of the victims of crime in cyberspace, report it to the cyber police. So that later there can be a legal process that runs to handle the case you are experiencing, it is very important to know the characteristics of phishing crime so as not to become one of its victims. The most common characteristic used by perpetrators to commit fraud is by luring prizes and then asking to provide some personal data, therefore when getting a message that may not make sense then there is no need to respond. Also be careful when someone sends you a link that looks suspicious.

How to deal with phishing on a Wordpress website. On the other hand, if you're a website owner who's been targeted by phishing activities, here's how to solve this online crime on a Wordpress website:

a. Use Plugins to Clean Phishing Malware

   Do not let the website be used as a means of stealing the data of visitors or customers of online stores, so, use anti-malware plugins on the Wordpress website.plugin options that can be used.

b. Always Update Wordpress

Wordpress is a platform that regularly updates. In addition to adding features, updates are also used to add security holes that are often exploited by phishers. To prevent your website from being attacked by malware.

c. Install SSL Certificate for Website Security

   As discussed earlier, the role of SSL is very important to ensure the transaction security on a website. If you haven't used it yet, immediately install an SSL certificate on the Wordpress website. installing SSL is easy.

d. Strict User Management If your Wordpress website is managed by many people, do user management well.

CONCLUSIONS AND SUGGESTIONS

Cyber Crime merupakan aktivitas kejahatan dengan menggunakan fasilitas computer atau jaringan computer tanpa ijin dan melawan hokum, baik cara mengubahnya atau tanpa perubahan (kerusakan) pada fasilitas komputer yang dimasuki atau digunakan, atau kejahatan yang dengan menggunakan sarana media elektronik internet karena dikategorikan sebagai kejahatan dunia maya, atau kejahatan di bidang komputer dengan cara illegal, Dapat pula dikategorikan sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.

The legal regulation of online fraud in the form of phishing needs to be amended to the ITE Law by formulating the concept of phishing concretely and changing the contents and elements in Article 45A paragraph 1 so that later Article 45A paragraph 1 can be applied so that a victim can get fair legal protection in accordance with the principles and principles of "equality before the law". This aims to seek criminal law reform in order to achieve justice by building a restorative justice-based criminal law design that has deterrent power. There is a need for regulations that encourage the application of punitive damages. In accordance with the Restorative Justice Theory, the perpetrator should return what the perpetrator has taken from the victim. If the perpetrator cannot return, then the perpetrator will be auctioned his property and if the auctioned property is not enough, it will be replaced with confinement for a certain period of time in accordance with applicable laws and regulations and is also required to pay a fine in accordance with applicable laws and regulations.

Efforts Made by the Government in Overcoming Cyber Phishing Crimes Used to Take Personal Data on Digital Trading Sites Policies in legislation are absolutely necessary by law enforcers and the government to tackle and take action against criminals, as well as cyber

crime, of course the type of statutory law must be in accordance with the type of crime and the way to reveal cases of cyber crime. The government of the Republic of Indonesia is committed to fighting cybercrime.

REFERENCES

TextBook

Andi Hamzah, Aspek-aspek Pidana di Bidang Komputer, penerbit Sinar Grafika, Jakarta, 2005. Hlm

Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif HukumPidana Positif. *Jurnal Pembaharuan Hukum*, 1(3), 287-296.

Elisabeth Nurhaini Butarbutar, Metode Penelitian Hukum (Bandung: Refika Aditama, 2018

Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana prenada media group, 2013

Suratman and Phillips Dilla, Metode Penelitian Hukum Bandung: Alfabeta, 2015 Deris Setiawan, Sistem Keamanan Komputer, (Jakarta: PT Elex Media Komputindo, 2005

Journal

Pribadi Debitur Dalam Aktivitas Pinjaman Online.," Jurnal Ius Constituendum 7, no. (2022)

Mia Haryati Wibowo and Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime," JoEICT (Journal of Education And ICT) 1, no. 1 (2017)

Sugeng Riyadi, "Efektifitas Undang-Undang Nomor 23 Tahun 2011 Tentang Pengelolaan Dan Pemberdayaan Zakat Dalam Rangka Mengentaskan Kemiskinan," *Jurnal Usm Law Review* 1, no. 2 (2019)

Muhammad Kamran and Maskun Maskun, "Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika,"

Barda Nawawi Arief, Beberapa Aspek Kebijakan Penegakan Dan Pengembangan Hukum Pidana, Bandung: Citra aditya bakti, 1998.

Marilyn Armour, "'Restorative Justice: Some Facts and History,'" *Tikkun* 27, no. 1 (2012),

Alison Liebling, "Prisons in Transition*," International Journal of Law and Psychiatry* 29, no. 5

Hardianto Djanggih, 2013, Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime. Jurnal Media Hukum Vol 1 dan 2.

Victor, Jozef Rudy dan Yawan, Jefry Bernhard. 2010. Cara Mudah Forex Trading Online. STIH Manokwari, Manokwari, hlm.