POLICE EFFORTS IN REVEALING CRIMINAL ACTS OF ONLINE FRAUD

Lalu Hedwin Hanggara, Boy Nurdin
Universitas Borobudur, Jakarta, Indonesia
lalu38st@gmail.com, drboynurdin_ppslaw@yahoo.com

ABSTRACT

Crimes caused by the development and progress of Information Technology and Telecommunications are crimes related to the internet, or in foreign terms it is often called cybercrime. Cybercrime is a crime that takes advantage of technological developments, especially the internet. The internet, which presents cyberspace with its virtual reality, offers various hopes and conveniences, but behind that, problems arise in the form of a crime called cybercrime, both the computer network system itself and the computer itself which is the vehicle for committing crimes. There are a variety of digital scams such as phishing, lottery scams, video scams, identity theft and scareware. This study uses a normative juridical approach. The normative juridical approach is legal research carried out by examining literature or secondary data as the basic material to be examined by conducting a search of regulations and literature related to the problem under study. The efforts of the police in handling fraud cases online are guided by the Criminal Procedure Code (KUHAP) as well as in the Regulation of the Indonesian National Police Number 6 of 2019), namely as "Investigators and Investigators". The step taken by the Police is to trace the accounts used by the perpetrators of crimes, where the last whereabouts or position of the perpetrators of these crimes are.

Keywords: Cybercrime, Crime, Fraud.

INTRODUCTION

The development of Information and Communication Technology causes the world to become borderless which causes significant social changes to take place quickly. However, the creation of Information and Communication Technology to produce positive benefits, but it turns out to be used for negative things. One of the negative impacts arising from technological developments is the emergence of modern crimes. Crime continues to develop along with the development of human civilization, with complex quality and quantity with variations in its modus operandi (H.Abdul Wahid dan Mohammad Labib, 2005). Through electronic media there are several types of criminal acts that often occur such as criminal acts of defamation, pornography, gambling , account breaches, destruction of cyber networks (hacking), and other crimes through Electronic Media.

Crimes caused by the development and progress of Information Technology and Telecommunications are crimes related to the internet, or in foreign terms it is often called cybercrime. Cybercrime is a crime that takes advantage of technological developments, especially the internet. The internet, which presents cyberspace with its virtual reality, offers various hopes and conveniences, but behind that, problems arise in the form of a crime called cybercrime, both the computer network system itself and the computer itself which is the vehicle for committing crimes.

According to Puram et al. (2011) there are various variations of digital fraud such as phishing, lottery scams, video scams, identity theft, and scareware. Meanwhile, Button et al. (2014) mentioned other types of digital fraud, such as romance scams, malicious spam, employment scams, and investment scams. Various types of fraud are conveyed to victims or potential victims through various channels such as short messages (SMS), messages through chat applications and other social platforms including social media, email, telephone, websites, market places, and various other digital platforms (Ahmad M Ramli, 2004), (Edmon

Makarim, 2004).

One of the protection efforts is through Criminal Law, both by penal and non-penal means in Electronic Media. The crime that often occurs is fraud in the name of buying and selling business using Electronic Media which offers various kinds of products that are sold below the average price . Online business has become a trend nowadays, but it can cause harm to other people if it is used by irresponsible parties. There are so many frauds in the real world, but in cyberspace there are also cases of fraud.

A number of data and studies above show that digital fraud is a crime that seriously threatens the Indonesian people in this digital era, which not only causes financial and psychological losses but also breaches of personal data. Various factors can be assumed to influence the number and variety of digital fraud cases today. First, the competence of media users in recognizing, preventing and fighting digital fraud. Second, law enforcement and prevention regulations are not strong enough. Third, content moderation and community standards from various digital platforms that have not been fully utilized to prevent and deal with digital fraud.

Against the rampant criminal acts of fraud, the police as officers in the field of law enforcement have duties and obligations to uphold the law and provide protection to the public. We can see this in Article 13 of Law No. 2 of 2002 concerning the Indonesian National Police which states that the main duties of the Indonesian National Police are: 1. To maintain security and public order; 2. Uphold the law; and 3. Provide protection, shelter, and service to the community.

Not only looking at the types and disadvantages of digital fraud, there is also a study on digital fraud from a legal perspective. For Indonesia, one of them was carried out by Rahmanto (2018) regarding law enforcement against criminal acts of fraud based on electronic transactions which are still experiencing many obstacles. Some of these obstacles are differences of opinion in interpreting regulations, the ability of investigators, public awareness and concern, limited expert personnel, weak government oversight, and procedural constraints on the Electronic Information and Transaction Law.

It turns out that it is not easy for the police to uncover Information Technology crimes. The handling of cybercrime through the Criminal Law in Indonesia is carried out by applying the provisions of the Criminal Code (KUHP) and the provisions of the Criminal Law outside the Criminal Code as a legal basis (Widodo, 2009). Law Number 11 of 2008 concerning Information and Electronic Transactions explicitly regulates criminal provisions for perpetrators of fraud through Electronic Media in Article 28 paragraph (1) there is a provision that: 'Every person intentionally and without right spreads false and misleading news that results in consumer losses in Electronic Transactions.'

RESEARCH METHOD

The normative juridical approach is used in this study, according to Soerjono Soekanto (Ronny Hanitijo Soemitro, 1990). In this legal research, the author tries to examine laws and regulations related to the problem being researched, namely related to cyber crime as stated in the 1945 Constitution of the Republic of Indonesia; Law Number 19 of 2016 regarding Information and Electronic Transactions.

Normative juridical research uses secondary data sources. Secondary data in the type of normative juridical research is data sourced from legal materials, consisting of primary legal materials, secondary legal materials, and tertiary legal materials (Marzuki, 2005).

Legal materials as secondary data used to analyze legal issues in this thesis are as follows.

1. Primary Legal Materials, namely legal materials that regulate the use of social media, buying and selling online (Nasution, 2008). The primary legal materials used in this study include:

a. The 1945 Constitution of the Republic of Indonesia
b. Law Number 19 of 2016 concerning Information and Electronic Transactions

2. Secondary Legal Materials, namely materials that provide an explanation of primary legal materials, such as draft laws, research results, or opinions of legal experts (Amarudin dan Zainal Asikin, 2010)
3. Tertiary Legal Materials, namely legal materials that provide instructions and explanations of primary legal materials and secondary legal materials, for example dictionaries (law, English and Indonesian), encyclopedias and others (Soerjono Soekanto dan Sri Mamudji, 1985).

RESULTS AND DISCUSSION

Law on Consumer Protection for Online Transactions

It is important to protect victims of crime, because first, society is seen as a system of institutionalized trust. This belief is integrated through the norms expressed in institutional structures, such as the police, prosecutors, courts, and so on. The occurrence of a crime against the victim can mean the destruction of the belief system, so that the regulation of criminal law and other laws relating to the victim will function as a means of restoring this belief system.

Second, there are social contract and solidarity arguments because the state can be said to have a monopoly on all social reactions against crimes that prohibit private actions. Therefore, if there are victims of crime, the state must pay attention to all victims by improving services and regulating rights. Third, victim protection which is usually associated with one of the goals of punishment, namely conflict resolution. Resolving conflicts caused by criminal acts will restore balance and bring a sense of peace in society.

Referring to the implementation of the protection of the rights of victims of crime, including victims of fraud via the internet as a result of violation of the human rights concerned, the basis for the protection of victims of crime can be seen from several theories, including the following (Mansur, D. M. A., & Gultom, 2005):

1. The theory of utility, this theory focuses on the greatest benefit for the largest number. The concept of providing protection to victims of crime, including victims of fraud via the internet, can be applied as long as it provides greater benefits than not applying the concept, not only for victims of crime, but also for criminal law enforcement as a whole.
2. Responsibility Theory, Legal subjects are essentially responsible for all legal actions they commit so that if someone commits a crime and causes someone to suffer, a loss (in a broad sense), that person must be responsible for the losses incurred, unless there is a reason that frees him. Regarding the perpetrators of criminal acts of fraud via the internet, based on the theory of responsibility, the perpetrators must be held accountable for the legal actions they have committed, unless there is reason to acquit the perpetrators.
3. Compensation Theory, as an embodiment of responsibility, because of their mistakes towards other people, the perpetrators of criminal acts are burdened with the obligation to provide losses to people or their heirs. Regarding fraud via the internet, based on the theory of compensation, the perpetrator must compensate for losses if the victim makes a claim for compensation. This compensation can be made by combining civil cases and criminal cases in accordance with the provisions of articles 98 to 101 of the Criminal Procedure Code.

Victims of the occurrence of a crime in electronic transactions, one of which is the victim of fraud via the internet, is the party that suffers the most and is disadvantaged, therefore it is necessary to have a protection from the state. Victims' rights must be seen as a form of equal treatment for everyone before the law (equality before the law).

In buying and selling goods through online media there is a sale and purchase agreement, thus issuing an agreement, namely an agreement that originates from an agreement or often referred to as a named agreement, Buying and selling through online media should follow existing regulations One type of sale and purchase transaction online that are currently widely

used are through Instagram, Facebook and online buying and selling shops such as Zalora, Shopee. Every trade transaction has risks and problems, one of the cases encountered was when the consumer felt disadvantaged because he did not receive the goods he bought, as a result he complained that he was deceived by an online store that used a Facebook account. Another case that occurs in online buying and selling is that consumers buy goods but after the goods are received they are not in accordance with what was promised.

In Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information & Electronic Transactions, the article imposed is Article 28 paragraph (1), which reads as follows: (1) Everyone uses intentionally & without rights share false & misleading information that causes consumer losses in Electronic Transactions. The penalty for this article is imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 1 billion (Article 45 paragraph [2] of the ITE Law). For proof, you can use electronic evidence and/or printed results as an extension of evidence as stated in Article 5 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, in addition to other conventional evidence in accordance with the Book Criminal Procedure Code (KUHAP).

The rights of victims in the Criminal Procedure Code that are relevant to the rights of victims of criminal acts of fraud via the internet are as follows:

1. Right to Report (Article 108 Paragraph (1) of the Criminal Procedure Code)
2. Right to exercise control over investigators and public prosecutors (article 77 jo 80 KUHAP)
3. The Right to Claim Compensation Due to a Criminal Act by Merging Civil Cases with Criminal Cases (Article 98 to Article 101 of the Criminal Procedure Code).

Based on the principle of online transactions, usually several parties prioritize the aspect of trust or "trust" to sellers and buyers. The principle of online transaction security has not yet become a major concern, especially when transactions are carried out on a small or medium scale with a nominal transaction that is small or not too large. One of the reasons for the many fraudulent transactions is through online/internet media or other telecommunication media. With so many frauds that have occurred, it would be better if you are more selective in making online transactions and be more careful in order to reduce fraud, as a consideration if you are going to make buying and selling transactions online.

Not only large amounts of fraud but small amounts of fraud also often occur, but consumers more often just leave it alone and don't report it because a small nominal does not make them experience big losses. a little whereas regarding online fraud in Law number 11 of 2008 concerning Information and Electronic Transactions there is no explicit regulation, what is regulated in the ITE Law is the spread of misleading false news which results in consumer losses in electronic transactions.

Looking at the provisions of the ITE Law, the focus is on the existence of misleading fake news which results in losses for consumers. It doesn't matter how much loss it causes. In addition to the ITE Law, provisions regarding fraud can also be found in Article 378 and Article 379 of the Criminal Code (KUHP). With the sound of the article as follows:

> Article 378 of the Criminal Code:
> *"Whoever with the intent to unlawfully benefit himself or others by using a false name or false prestige (hoedaningheid); by deception, or a series of lies, inducing another person to hand over something to him, or to give a debt or write off a receivable, is threatened, for fraud, with a maximum imprisonment of four years".*
> Article 379 of the Criminal Code:
> *"The acts formulated in Article 378, if the goods handed over are not livestock and the price of the goods, the debt or credit is not more than twenty five rupiahs, it is threatened*

as light fraud with a maximum imprisonment of three months or a maximum fine of two hundred and five twenty rupiahs".

If you look at the provisions in Article 379 of the Criminal Code, it is explained how much loss can be reported and can be distinguished whether the crime is fraud or minor fraud. Looking at the provisions of Article 379 of the Criminal Code, it is explained that what is meant by mild fraud is not the minimum price of goods Rp. 2,500,000.00, - but the price of the goods in question is not more than Rp. 2,500,000.00, -. So even though the amount of loss suffered is small, it is included in light fraud and is included in the realm of crime.

Based on article 28 F of the 1945 Constitution of the Republic of Indonesia, it can be said that by forming the ITE Law, it means limiting the use of information technology. However, what needs to be emphasized is that the ITE Law was formed to regulate all electronic use freely but responsibly.

Related to the use of the internet, which is the utilization of information technology and electronic transactions, therefore it must be carried out in accordance with Article 3 of the ITE Law. In practice, the actors or organizers of the electronic system have obligations as written in Article 15 of the ITE Law, namely:

1. Every Electronic System Operator must operate the Electronic System reliably and safely and be responsible for the proper operation of the Electronic System.
2. Electronic System Operators are responsible for their Electronic System Operations.
3. The provisions referred to in paragraph (2) do not apply if it is proven that force majeure, errors and/or negligence on the part of the Electronic System user has occurred.

It can be noted that the ITE Law itself has been able to protect consumers and ensnare perpetrators of light and heavy fraud because there are already binding articles and sanctions given for criminal acts. However, back to consumers who are sometimes hesitant or don't dare to report to the authorities on the grounds that the cost of settling cases is not worth the price of the losses suffered and also takes a lot of time. In addition, consumers do not understand applicable laws and do not understand or do not know what they should do if they do not get their rights from business actors who commit fraud.

Efforts made by the Police in Revealing Online Fraud Crimes

In law enforcement carried out by the police, it begins with an investigative process after receiving a report. Investigation is a series of actions to seek and find an event that is suspected of being a crime in order to determine whether or not the action can be investigated according to the method regulated under this law.

The police as a component, element, subsystem of the criminal justice system is clearly visible. In the current legislation (both in the Criminal Procedure Code (KUHAP) and in the Regulation of the Indonesian National Police Number 6 of 2019) they are referred to as "Investigators and Investigators".

Everyone who experiences, sees, witnesses and/or becomes a victim of an event constituting a crime has the right to submit a report or complaint to investigators and/or investigators, both orally and in writing. Any person who knows of a conspiracy to commit a crime against public peace and security or against life or property is obliged to immediately report this matter to investigators or investigators. Every civil servant in the course of carrying out his duties who knows about the occurrence of an event constituting a criminal act is obliged to immediately report this to the investigator or investigators.

Investigators who know, receive reports or complaints about the occurrence of an event that is reasonably suspected to be a criminal act must immediately take the necessary investigative action. In the case of being caught red-handed without waiting for the investigator's order, the investigator must immediately take the necessary actions within the framework of the

investigation. Regarding this action, the investigator is obliged to make an official report and report it to the investigator in accordance with the law.

Reports or complaints submitted in writing must be signed by the complainant or complaint. Reports or complaints submitted verbally must be recorded by the investigator and signed by the complainant or complainant and the investigator. In the event that the reporter or complainant is unable to write, this must be stated as a note in the report or complaint. In carrying out investigative duties, investigators are required to show identification. In carrying out investigative duties, investigators are coordinated, supervised and given instructions by investigators.

The following are the sections of criminal procedural law that concern investigations as follows:

1. Provisions on investigative tools.
2. Provisions regarding knowing the occurrence of offenses.
3. Examination at the scene.
4. Summons of suspects or defendants.
5. Temporary detention.
6. Search.
7. Examination or interrogation.
8. Official report (search, interrogation and on-site inspection).
9. Foreclosure.
10. Case aside.
11. Delegation of cases to the public prosecutor and their returns.

In the event that the criminal act has been investigated by the investigator, he shall immediately submit the results of his investigation to the public prosecutor through the investigator. Reports from investigators to investigators are accompanied by minutes of examination which are sent to the public prosecutor. Likewise if the criminal case is not submitted to the public prosecutor.

In discussing the powers of investigators and investigators above, it is necessary to also discuss the authority of the "Police" as investigators and investigators according to the provisions of the Republic of Indonesia National Police Regulation Number 6 of 2019 concerning the Police, as follows:

1. According to Article 16 paragraph (1), that in the context of carrying out the tasks referred to in Articles 13 and 14 in the field of criminal proceedings, the Indonesian National Police has the authority to:
   a. Carry out arrest, detention, search and confiscation.
   b. Prohibit any person from leaving or entering the scene of the case for the purposes of investigation.
   c. Bringing and presenting people to investigators in the context of investigations.
   d. Ordering the suspect to stop and asking and checking personal identification.
   e. Examination and confiscation of letters.
   f. Calling people to be heard and examined as suspects or witnesses.
   g. Bring in the necessary experts in connection with the examination of cases.
   h. Hold an end to the investigation.
   i. Submit the case file to the public prosecutor.
   j. Submit a request directly to the authorized immigration official at the immigration checkpoint in an urgent or sudden situation to prevent or deter people suspected of committing a crime.
   k. Provide instructions and assistance with investigations to civil servant investigators and receive the results of investigations by civil servant investigators to be submitted to the

public prosecutor.

l. Take other responsible actions according to law.

2. According to Article 16 paragraph (2), that "Other actions as referred to in paragraph (1) letter I are investigative and investigative actions carried out if the following conditions are met:
   a. Not contrary to a rule of law.
   b. In line with the legal obligation that requires the action to be carried out.
   c. Must be appropriate, reasonable, and included in the position environment.
   d. Reasonable consideration based on compelling circumstances.
   e. Respect human rights".

Investigation of online-based fraud cases, these online-based fraud cases are different from ordinary criminal cases. The perpetrators of these online-based fraud crimes carry out their crimes anytime, anywhere, at an unspecified time, without the knowledge of other people, because these online-based fraud perpetrators usually use social media, fake accounts. Online-based fraud crimes often occur, usually in buying and selling online tickets, buying and selling motorized vehicles, buying and selling clothes, electronics, and so on. Agreements made between sellers and buyers are also based on trust, and do not meet in person, because transactions are carried out online. Usually, before making a transaction, the seller and the buyer communicate via messengers, direct messages, and so on. After an agreement is reached between the seller and the buyer, payment is usually made by transferring a certain amount of money to the seller's account. The step taken by the Police is to trace the accounts used by the perpetrators of crimes, where the last whereabouts or position of the perpetrators of these crimes are.

The investigation was carried out after a victim complaint related to online-based fraud. After receiving a money transfer from the victim, the perpetrator deactivated their account, cellphone number, and did not send the items that the victim had ordered. Because the item doesn't exist. Investigations conducted by the police regarding this cybercrime crime are carried out by tracing accounts or sources where the area of the cybercrime perpetrator's account is located. The police traced the whereabouts of the perpetrators by tracing the perpetrator's Internet Protocol ("IP Address") address stored on the website managing server which was used as a means or tool for the perpetrators to commit their crimes. After getting the whereabouts of the perpetrators, the police were in the process of arresting them.

However, not all cases of online-based fraud can be processed or arrested. In Supreme Court Regulation Number 2 of 2012 Article 1, it is explained that the words "two hundred and fifty rupiahs" in articles 364, 373, 379, 384, 407 and 482 of the Criminal Code are read as IDR 2,500,000.00 or two million and five hundred thousand rupiahs. Then, in Article 2 paragraph (2) and paragraph (3) it is explained, if the value of the goods or money is not more than IDR 2,500,000.00, the Chief Justice shall immediately appoint a Single Judge to examine, hear, and decide the case with the Procedure The Rapid Examination regulated in Articles 205-210 of the Criminal Procedure Code and the Chief Justice do not stipulate detention or an extension of detention.

CONCLUSION

Based on the results of the discussion that has been described, in this study it was concluded that basically the form of online-based fraud that is carried out is almost the same as conventional fraud. It's just that the difference is in terms of evidence. The statutory regulations, as well as the sanctions imposed are the same but there are additions to this online-based fraud. Police officers, in this case as the gateway in law enforcement acting as investigators, have difficulties because they are constrained by the evidence obtained in corroborating cases. Legal protection in Law no. 11 of 2008 concerning Information and Electronic Transactions and Article 378 of the Criminal Code. And the sanctions have been explained in Article 45 paragraph

(2) of the ITE Law and the proof that law enforcers can use electronic evidence and/or printed results as an extension of the evidence is in Article 5 paragraph (2) of Law No. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions in addition to other conventional evidence in accordance with the Criminal Procedure Code. In addition to the ITE Law and the Criminal Code, Article 378 Fraud is also contained in Article 379 of the Criminal Code which explains how much loss can be reported and can be distinguished whether the crime is fraud or minor fraud.

REFERENCES

Ahmad M Ramli. (2004). *Cyberlaw & HAKI dalam Sistem Hukum Indonesia*. Rafika Aditama.

Amarudin dan Zainal Asikin. (2010). *Pengantar Metode Penelitian Hukum*. PT. Raja Grafindo Persada.

Edmon Makarim. (2004). *Kompilasi Hukum Telematika*. Grafindo Persada.

H.Abdul Wahid dan Mohammad Labib. (2005). *Kejahatan mayantara*. Rafika Aditama.

Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law : Aspek Hukum Teknologi Informasi.*

Marzuki, P. M. (2005). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

Nasution, B. J. (2008). *Metode Penelitian Ilmu Hukum*. Mandar Maju.

Ronny Hanitijo Soemitro. (1990). *Metodologi Penelitian Hukum dan Jurimetri*. Ghalia Indonesia.

Soerjono Soekanto dan Sri Mamudji. (1985). *Penelitian Hukum Normatif*. CV Rajawali.

Widodo. (2009). *Sistem Pemidanaan Dalam Cyber Crime*. Laksbang Mediatama.