THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

Criminal Sanctions toward False Criminal Actors through the Internet

Henny Saida Flora
Lecturer, Department of Law, Santo Thomas Catholic University, Medan, Indonesia

Abstract:
The development of science and technology, especially information technology such as the internet is very supportive of everyone to achieve their life goals in a short time, both legal and illegal by justifying any means because they want to make a profit. The progress of current information technology and the possibility of the future is inseparable from the encouragement made by the development of communication technology and computer technology, while communication technology is driven by micro-electronic technology. As a result of the rapid and rapid development of technology and information, it will sooner or later change the behavior of society and human civilization globally, because information technology creates a world without borders, it also spurs the emergence of new modes and crime through information technology. The development of technology and information is also improving in the field of internet including fraud crimes committed through the internet. Fraud through electronic media occurs if someone intentionally makes transactions on online shopping sites fictitiously or someone who commits fraud by utilizing the means of a website even through email facilities by providing data or false promises. Fraud through the internet media is increasingly widespread among the public. By using skilled knowledge about the internet, the perpetrators then use these skills to carry out this crime. The rule of law itself does not seem to be a problem for perpetrators of fraud via the internet. The threat of punishment from Article 45 paragraph (2) of the ITE Law is only a guarantee for consumers while the perpetrators do not think about it.

Keywords: *Criminal sanctions, perpetrators, fraud, the internet*

1. Introduction

The development of the current era is synonymous with advances in technology and information that is developing very rapidly and rapidly. This phenomenon occurs in all parts of the world regardless of developed and developing countries. Most of the world community of a country are required to follow developments in technology and information, in order to compete in an increasingly modern, practical and efficient global world competition.

Along with the development of the needs of the global community, information technology has an important impact on changes now and in the future, because these developments have many advantages and positive impacts for countries in the world. There are at least two things that make information technology considered so important in spurring the growth of a country in the world, namely first, information technology contains an increase in demand for information technology products themselves, such as computers, modems, means for building internet networks and so forth. Second, facilitating to conduct business transactions, especially financial business in addition to other general businesses.

Information technology has succeeded in building a new habit for the global community, which influences changes in the pattern of life needs of the people in the social and economic fields, which are normally dealing, doing business or socializing by meeting physically or conventionally into transactions, doing business and socializing electronically i.e., meeting each other in cyberspace, because it is believed to facilitate transactions, save time, money and is not limited by space and time. The development of science and technology which is quite rapid at this time has become a daily reality even a demand of society that cannot be negotiable. The main objective of the development of science and technology is a change in the future of humanity for a better, easier, cheaper, faster and safer. The development of science and technology, especially information technology such as the internet is very supportive of everyone to achieve their life goals in a short period of time, both legal and illegal by justifying any means because they want to make a profit. The progress of current information technology and the possibility of the future is inseparable from the encouragement made by the development of communication technology and computer technology while communication technology is driven by micro-electronic technology.

As a result of the rapid and rapid development of technology and information, it will sooner or later change the behavior of people and human civilization globally, because information technology makes a world without borders. It also spurred the emergence of new modes and crime through information technology. The development of technology and information is also increasing crime in the internet field, including fraud crime.

Lately there is an interesting phenomenon that arises in the community, namely buying and selling online, which transacts buying goods or services through electronic media in cyberspace where buyers and sellers do not meet physically, and

bargaining with each other is limited to conversations in selling forums buy online. after agreement and agreement have been reached on prices and goods, transactions can be carried out by transfer. However, this triggers a crime of fraud using electronics with a variety of new module. criminal acts of fraud through electronic media occur if someone intentionally makes transactions on online shopping sites fictitiously or someone who commits fraud by using website facilities even through email facilities by providing false data or promises.

This internet fraud can be blamed as violating Article 378-395 of the Criminal Code as a fraud or Article 28 paragraph (1) of Law Number 11 Year 2008 concerning information and electronic transactions (UU ITE) governing the spread of false and misleading news that harms consumers or Article 378 of the Criminal Code jo Article 28 paragraph (1) jo Article 45 paragraph (2) of the ITE Law. The threat of punishment for violators is a maximum imprisonment of six years and or a maximum fine of Rp. 1,000,000,000 (one billion rupiah) but the rules above are different from the reality in the community. Fraud through the internet media is increasingly widespread among the public. By using skilled knowledge about the internet, the perpetrators then use these skills to carry out this crime.

2. Forms of Electronic Transactions

Transactions are events that involve environmental factors and affect financial position. Today these environmental elements include the environment in cyberspace and the indirect world so that electronic payment transactions also emerge. Electronic transactions are legal actions carried out using computers, computer networks and / or other electronic media. Electronic payment transactions are payments that are legally valid and are carried out using computers, computer networks, and / or other electronic media. The forms of electronic transactions are debit cards, credit cards, mobile banking, online / internet banking.

A debit card / debit card is a plastic card that can be used by the owner for electronic transactions referring to his bank account or other financial institutions. The use of this debit card is at transactions at ATMs or at cashiers at supermarkets that support payment using a debit card. In some cases, cards are specifically designed for online payment through the internet so there is no physical form of the card. Payment using a debit card requires that we have a balance in advance on the account concerned with our debit card so that we can use the saldot to transact.

Credit cards are also the same in the form of plastic cards as debit cards, but the system is in the form of credit, which is that credit card issuers first lend money to consumers at the time of the transaction. Consumers are required to pay their credit load at every time unit, usually every month.

Mobile banking is a transaction of a bank consumer with his account using a mobile device. Consumers can usually check balances, transfer balances, credit payments, other payments or other bank transactions through their mobile devices. Usually through the SMS feature on mobile devices, but there are also mobile applications that can be downloaded for certain mobile devices.

Online banking makes it easy for consumers to transact with banks, almost all bank transactions can be done using online banking such as payments, loans, investments, or balance transfers. Online banking uses internet networks in the transaction.

In the concept of a transaction, each transaction must be made written information as evidence such as receipts or invoices commonly called proof of transactions. For electronic payment transactions themselves in accordance with ITE Law, these transactions must be poured through a form of agreement or contract that is also carried out electronically. According to Article 18 of the ITE Law, electronic contracts are agreements contained in the electronic system, the evidence of transactions contained in the electronic system is binding on the makers and on transactions using debit cards and credit cards, proof of transactions can use invoices printed by the machines used at the time of the transaction and on mobile banking and online banking proof of the transaction can use electronic documents that exist at the time of the transaction.

3. Fraud Mode of Operations in Electronic Transactions over the Internet by Carding

Mode is interpreted as a conscious urge to act in accordance with a specific purpose or intention to commit a crime while the modus operandi is defined as a method of working that is used to commit a crime, many ways are carried out by perpetrators of crime to get victims easily. Understanding the modus operandi in the scope of crime is the operation of ways or techniques that are specifically characterized by a criminal in carrying out his evil deeds.

Cyber-crime is a crime committed through internet media which uses computer equipment. As for several cases of cybercrime that often occur or are rife in Indonesia are as follows:

3.1. Carding

Carding crime techniques have existed since 2000 before the Act No. 11 of 2008 concerning Information and Electronic Transactions. In handling this carding case, law enforcers use the Criminal Code Articles to ensnare the perpetrators.

3.2. Fraud via SMS

The mode is by sending sms lottery prizes on behalf of a well-known company. This mode of crime is increasingly prevalent in Indonesia. The contents of the text encourage victims to call the number provided by the perpetrator. Then when the victim calls the number, the victim is asked to send a sum of money as a condition for taking the prize. After sending the money the victim did not receive any gifts from the sender of the sms.

3.3. Using Websites to commit Fraud

This mode is done by using lottery paper in a package of certain food products in the paper listed a fake website address of a well-known company. Through the website the victim is tricked by the perpetrators that the lottery really exists.

3.4. Defamation through Facebook

Crimes with this mode where the perpetrators can take various actions that can harm the victim for example by distributing pornographic photos in the victim's account

The carding phenomenon is a crime that was born as a result of the rise of online transactions and advances in information technology by using credit cards as a means to make payments. Carding is a form of internet fraud, which is an act of dishonesty or fraud by using the internet or technology that is directly supported by the internet. Fraud referred to in carding is in the form of using an illegally obtained credit card number to order a number of goods or transactions online. there are many examples of carding cases carried out by unscrupulous Indonesian citizens, where the average victim is a foreigner both living in Indonesia and abroad. There are two common carding case modes:

- The credit card misuse mode that is included in the Payment Fraud term is a crime committed by paying online transactions on the internet using a stolen credit card number or payment canceled after the ordered item is shipped
- The case of misusing credit cards (carding) with the term Fraud Involving Auctions, which is a crime committed by offering an online auction of goods but after the bidder sends money online on the internet, the item is never sent.

There are several offender techniques for getting a credit card number before using it in a card generator, namely:

- Buy information. Buy to someone who has active credit card information. Usually someone who has someone's credit card data, but he can't use card numbers or technology stuttering so that for me to get the profit he sells to hackers.
- Get credit card numbers through chattingan activities on the internet. Chattingan is usually done with strangers. Then with deception, the stranger tells his credit card information.
- Take the carelessness of the owner. If we make a transaction using a credit card by asking someone else, then the person we told secretly keeps the credit card number for harmful purposes.
- Pitfalls online. Creating a stealth site that provides e-commerce services, where someone has to enter information about their credit card.
- Cooperating with certain parties, for example, with lodging, shopping, restaurants where transactions are done with a credit card.
- Hacking an e-commerce site with its ability in algorithms and programming, it can break down data bases from foreign and domestic sites that are well known.
- Someone sent an e-mail claiming to be from a credit card issuer and as if checking our data by asking for the card number, expired date, billing address, pin, mother's biological name and date of birth. However, the pop-up technique is made as if the e-mail is really from a credit card issuing bank. The deceived person will provide the information requested in the email.

After the perpetrators get credit card information using the above technique, then the perpetrator uses a card generator to get 1000 other credit card numbers. After that, several selected credit card numbers are entered again in the verifier software to determine the validity of the credit card numbers so that they can be used to buy goods online. One credit card is used to buy at one merchant. So, use a different credit card at each merchant so that credit card clickers don't get caught if the credit card data runs out too much. Then the carding technique developed every year.

4. Criminal Sanctions for Fraudulent Criminals via the internet

Fraud via the internet already has a prohibition in the ITE Law and this fraud through the internet is not directly carried out by human beings or done through transactions and people are more likely to use the ITE Law if someone commits a crime using the internet, because this crime not done manually, everything is done in the occurrence of transactions, things that are not desirable relating to criminal acts are the ITE Law. In the ITE Law the criminal threat is more severe than the criminal threat in the Criminal Code. If there is a criminal act of fraud through the internet, then the punishment applied in imposing a crime is more inclined to the ITE Law because it is not directly carried out because it uses the internet media so the ITE Law is applied.

The forms of fraud in the Criminal Code in Article 378 consist of:

- With the intention of moving people
- The goal is to hand over objects and write off receivables
- The act is intended to benefit themselves and others by way of breaking the law

The form of ITE criminal offense in Article 28 paragraph (1) consists of elements, namely:

- Error: on purpose
- Against: law without rights
- Acts: spread
- Object: false and misleading news
- As a result of actions: resulting in consumer losses in electronic transactions

Article 378 of the Criminal Code has an element of self-benefit and others, resulting in the emergence of submission of objects by someone who successfully deceived so that it is moved according to the wishes of the perpetrators. Article 378 of the Criminal Code has deficiencies in important objects of fraud crime, namely electronic media facilities to commit online fraud. In contrast to Article 28 paragraph (1) of the ITE Law it is not clear that fraud is shown and it does not matter who benefits (themselves or others), the most important is the loss of consumers from electronic transactions

Seeing the comparative arrangement between the two articles, the imposition of criminal liability will certainly have a difference, namely the difference in criminal sanctions in Article 378 of the Criminal Code and Article 28 paragraph (1). Article 378 of the Criminal Code only contains 4 years of imprisonment while in Article 28 paragraph (1) of the ITE Law does not directly include criminal sanctions, but is stated in Article 45 paragraph (2) of the ITE Law, which is a maximum of 6 years in prison and also contains sanctions of Rp. 1,000,000 unknown legal subjects of the legal entity (corporation) in the Criminal Code which resulted in the escape of the legal subjects for criminal liability. Unlike the case with the ITE Law which is already familiar with legal subjects in the form of legal entities (corporations).

After seeing the difference in regulation and criminal liability between Article 378 of the Criminal Code and Article 45 paragraph (2) jo Article 28 paragraph (1) of the ITE Law there are several important points, namely:

- The Criminal Code has an element of benefiting oneself and others, whereas in the ITE Law it is not clear to whom the fraud is addressed, the most important thing is the existence of consumer losses in electronic transactions no matter who benefits.
- The Criminal Code does not yet know the legal subject of a legal entity (corporation) while the ITE Law has recognized the legal subject of a legal entity (corporation)
- The Criminal Code does not recognize electronic transactions or electronic media, which in this case are important objects for perpetrators to commit fraud via the internet, in the ITE Law, information, transactions and electronic media are known.
- There are differences in the consequences and objectives of the actions stated in Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law in the two laws. Article 378 of the Criminal Code aims to benefit themselves and / or others, the result of which is the delivery of objects from people who have been successfully influenced to be moved according to the wishes of the perpetrators, the giving and writing off of receivables whereas in Article 28 paragraph (1) of the ITE Law it is not listed the element of purpose is the advantage of who the perpetrators of the crime are, this article only lists the consequences of the crime namely consumer losses in electronic transactions.
- There is a clear and detailed way to commit a criminal offense in the Criminal Code, namely with a false name, false dignity / position, as well as a series of lies and deception, whereas in the ITE Law there is no escape method that only includes actions that is spreading lies and misleading news.
- The existence of different threats in the Criminal Code and the ITER Law, the difference is seen by the existence of financial penalties in the ITE Law. In Article 378 of the Criminal Code the criminal threat is a maximum imprisonment of four years, while in Article 28 paragraph (1) jo Article 45 paragraph (2) of the ITE Law the threat of punishment is a maximum imprisonment of six years and / or a maximum fine of Rp. 1,000,000,000 (one billion rupiah).

The Criminal Code as the main legal basis for criminal punishment in Indonesia has regulated the rules prohibiting the criminal acts of fraud set forth in Article 378 of the Criminal Code. The element of fraud in Article 378 of the Criminal Code is still a conventional fraud, namely fraud that generally occurs and is intended for all things that exist in the real world. The use of Article 378 of the Criminal Code is inappropriate if it is used to ensnare a criminal offense through the internet which is found in cyberspace by using electronic media as a means to commit criminal acts, due to limitations in the evidence which are limited by the Criminal Code and jurisdictional issues in handling cybercrime case.

Article 28 paragraph (1) of the ITE Law does not directly regulate conventional and non-online fraud, but the elements in Article 28 paragraph (1) of the identical ITE Law have some similarities to the conventional fraud set out in Article 378 of the Criminal Code and has a special characteristic that is the recognition of electronic media evidence and the expansion of jurisdiction in the ITE Law. In this case the lex specialis derogate legi generale principle is applied. Article 28 paragraph (1) of the ITE Law is a lex specialis derogate legi generale from Article 378 of the Criminal Code. In addition to having more specific elemental characteristics in the context of criminal prosecution for fraud via the internet, Article 28 paragraph (1) of the ITE Law has fulfilled several principles in the principle of lex specialis derogate legi generalis, namely:

a. The provisions found in the general rule of law still apply except those specifically regulated in special legal rules
b. The provisions of the lex specialis must be equal to the provisions of the lex generale (the law)
c. The provisions of the lex specialis must be in the same legal environment as the lex generalis.

Seeing the differences and similarities in the elements of the two articles, Article 28 paragraph (1) of the ITE Law can ensnare perpetrators of online fraud.

5. The Difficulties of Proof in Fraud Criminal Acts through the Internet

The obstacle or difficulty in proving this fraud is regarding the limitations of the equipment owned by the authorities or authorized institutions in handling cyber-crime cases, the removal of evidence by the perpetrators and bearing in mind that the cybercrime case has a very wide area broad, not only between provinces in Indonesia but also across national borders. As for some of the obstacles in proving criminal fraud via the internet are internal technical constraints and external technical constraints.

Internal technical constraints consist of:

- Lack of understanding and mastery in the field of information technology, some police investigator personnel still do not master information technology and there is no internet socialization.
- Too much workload of investigators in the cybercrime unit. Investigators are not focused on dealing with cybercrime, especially fraud through the internet.
- Lack of modern facilities in the search for evidence. Understanding investigators who do not understand the general crime with cybercrime how to technically treat both witnesses and evidence because cybercrime is processed and needed specifically unlike other evidence of criminal acts. for example, software when an investigator turns off and revokes a laptop or computer that is being used, the evidence is lost and how to crack codes that have been set up in such a way that the investigator tries to open the codes that have changed the data displayed.

6. The Difficulties of Proof in Fraud Criminal Acts Through the Internet

The obstacle or difficulty in proving this fraud is regarding the limitations of the equipment owned by the authorities or authorized institutions in handling cybercrime cases, the removal of evidence by the perpetrators and bearing in mind that the cybercrime case has a very wide area broad, not only between provinces in Indonesia but also across national borders. As for some of the obstacles in proving criminal fraud via the internet are internal technical constraints and external technical constraints.

External technical obstacle is the difficulty of obtaining evidence contained in fraud cases via the internet resulting in the process of investigation and investigation often stalled, because this includes cybercrime, the evidence to conduct the investigation process is only in the form of electronic information and electronic documents, because the crime scene occurred on the internet, the investigator searches and observes using the internet and if needed the investigator collaborates with other institutions. The obstacles that are often experienced at the time of verification are:

6.1. Difficult to Get the Address of the Perpetrator

The most common obstacle in the verification process is that the address registered in the perpetrator's identity is fictitious, because the perpetrator easily creates a KTP with a false name and address to carry out the action. and the perpetrators also eliminate traces by disposing of the perpetrator's telephone number so that his position cannot be traced to the next address that can still be searched for and where his presence can still be found then the police will continue to look for it

6.2. The High Mastery of Actors in Operating Information Technology

Internet access that serves websites that have not been controlled to make online fraud increasingly widespread in the community because of the ease of access, coupled with the ability of fraud perpetrators through the internet which is increasingly sophisticated in operating fraudulent websites.

6.3. The Principle of Bank Secrecy Is Not To Provide Suspected Customer Identity

6.3.1. Online Fraud

Constraints on bank secrecy have become a hindering factor in the investigation process because bank procedures will not provide the identity of their customers to other people before approval from the customer, sometimes the Bank knows the registered account is fictitious, and the police have no collaboration with the Bank to reveal the perpetrator's account.

7. How to Overcome the Difficulties in Proving Fraud Criminal Acts via the Internet

To overcome the obstacles or difficulties in proving criminal acts of fraud through the internet there are two types of efforts made, namely internal technical efforts and external technical efforts. Internal technical effort is an effort made before the occurrence of a criminal offense and an external technical effort is an effort carried out after the crime has occurred.

Efforts by investigators to overcome internal obstacles:

- Conduct training for every member of cybercrime. Improving the ability of police resources by providing training to members so that cases related to cybercrime can be handled optimally. Because in carrying out their duties each member of the National Police is required to be professional in handling all cases from receiving reports from the public, the investigation process, the investigation process to the filing process and also each year the modes of fraud are increasingly varied and more sophisticated, therefore the police are demanded to be able to overcome the types of crimes that are sophisticated, also improve facilities and infrastructure and equip equipment that supports the process of investigation and investigation so as to facilitate in handling cases related to cybercrime, especially criminal fraud through the internet.
- Improve the investigator's performance and conduct a case evaluation after each case. Improvement and evaluation is intended so that all members of the investigator can realize the weaknesses and shortcomings in each case of fraud via the internet so that in handling every case that will be faced next, each member is ready to handle the case optimally by evaluating this case can also understand the shortcomings and mistakes of members

who work less than the maximum so that it is used as a warning to every other member so as not to make carelessness in carrying out further tasks in the future.

- Submitting an application for the addition of facilities and infrastructure that supports the incompleteness of operational facilities and infrastructure severely impedes the process of investigation and investigation because fraud cases through the internet really require very sophisticated equipment to be able to prove a crime.

The Investigator's effort to overcome external obstacles is to establish cooperative relationships with related parties. One effort to overcome obstacles to fraud cases through the internet is to establish relationships or cooperation with agencies relating to criminal acts of fraud via the internet. Building this collaboration is very important because it can support the search for electronic evidence as well as to find the whereabouts of the perpetrators. Investigators usually cooperate with agencies related to fraud via the internet, one of them with the Bank which is often used by perpetrators in conducting electronic transactions, internet service providers, and establishing cooperation with the ministry of telecommunications and information and establishing relationships with institutions for the purposes evidence of expert testimony in accordance with the needs of the investigation, investigation and other necessary evidence. The evidence obtained by the investigator will later be followed up by the judge at the beginning of the process of proving criminal acts in court and so on.

8. Conclusion

- Criminal sanctions against fraud perpetrators via the internet are carried out using Article 45 paragraph (2) jo Article 28 paragraph (1) of the ITE Law. In addition to Article 45 paragraph (2) of the ITE Law, perpetrators of online fraud can also be accounted for in Article 378 of the Criminal Code but because it has been specifically regulated, Article 45 paragraph (2) of the ITE Law is used.
- There are two difficulties in proving fraud through the internet, namely internal and external constraints. Internal constraints consist of a lack of understanding and mastery in the field of information technology, too much workload of investigators in the cybercrime unit, and a lack of modern facilities in the search for evidence. External constraints consist of difficulty in getting the address of the perpetrators, the high mastery of the actors in operating information technology and the principle of bank secrecy.
- Tackling the difficulties of proving fraud via the internet is done with two efforts, namely internal efforts and external efforts carried out by conducting training for each member of cybercrime, improving the performance of investigators and adding more sophisticated facilities or facilities. An external effort is to collaborate with related parties or agencies related to cybercrime, namely Telkomsel.

9. References

i. Ali Mahrus, 2013, *Asas-Asas Hukum Pidana Korporasi*, Raja Grafindo Persada, Jakarta
ii. Chawawi, Adami, 2001, *Pelajaran Hukum Pidana* I, Raja Grafindo Persada, Jakarta
iii. ----------, 2004, *Kejahatan Terhadap Harta Benda*, Bayu Media, Jawa Timur.
iv. Manthovani, Reda, 2006*, Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia* Malibu, Jakarta
v. Maskun, 2014, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Kencana, Jakarta
vi. Rahardjo, Agus, 2002*, Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Citra Aditya Bakti, Bandung
vii. Saleh, Roeslan 1985, *Tindak Pidana dan Pertanggungjawaban Pidana*, Aksara Baru, Jakarta
viii. Suparni, Niniek, 2019, *Cyberspace Problematika dan Antisipasi Pengaturannya*, Sinar Grafika, Jakarta
ix. Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang *Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*