JPPI Vol 10 No 1 (2020) 73 - 85

Jurnal Penelitian Pos dan Informatika

32a/E/KPT/2017

e-ISSN 2476-9266
p-ISSN: 2088-9402

Doi:10.17933/jppi.2020.100106

Cybercrime in the Context of Cellular Telephone Scams

Cybercrime dalam Konteks Penipuan Telepon Seluler

Pajar Pahrudin

Information System, STMIK Widya Cipta Dharma, Samarinda, 75123, Indonesia

pajar@wicida.ac.id

Received: 16 May 2019; Received in revised from: 26 November 2019; Accepted: 27 August 2020

Abstract

Technological advancement comes with both positive and negative impacts to the society, including the cybercrime. The main problems discussed in this study is regulation of criminal acts of scams committed through electronic media, particularly SMS, as well as the efforts to handle such crime in accordance with applicable legal provisions, both based on the Criminal Code and based on Law Number 11 of 2008 on Electronic Information and Transactions that has been amended by Law no. 19 of 2016. This study applies the Normative Legal Research method. The results showed that the criminal act of scams committed online was in principle similar to that of conventional fraud, the only difference being the means of action, namely using an electronic system, namely computers, the internet, or cellular telecommunication devices. Based on the prevailing legal provisions, online fraud can be treated similar to that conventional offenses stipulated in the Criminal Code (KUHP), so that the case handling process is also based both on the Criminal Code and Electronic Information and Transactions law.

Keywords: Scams SMS, Handphone

.

INTRODUCTION

In this era, data and information are the main commodities that can be traded and easily be accessed by users and customers. Information Technology (IT) is a general term for any technology that helps humans create, modify, store, communicate and/or disseminate information.

In everyday life, humans always communicate both with fellow humans and others. Communication is necessary because in communication, someone can receive or provide information so that information exchange occurs.

Before communication technology developed rapidly as it is now, communication was carried out traditionally. As technology has become more developed, communication can take place without direct face-to-face interaction.

There are a host of applications of communication services available, one of which is short message service (SMS) that can be done through cellular phone. Short message service (SMS) is a basic cellular telecommunication service, which is available on both GSM and CDMA networks. As a basic service, SMS service can be used on all types of cellular phones. Every SIM card from an activated operator can almost certainly be used immediately for SMS, because the SIM card will automatically provide service center settings on the cellular phone.

Ease of use, variety of services, and considerably intensive promotions from cellular operators have made SMS a popular service in the community since the late 1990s until now. Along with the development of technology and the operators and service providers' creativity, SMS services, which were originally only intended for sending messages between subscribers (point-to-point), have now developed and are more varied, with features such as polling services, ringtones, premium sms, mobile banking, ticketing.

Communication is basically a process to convey a message from one place to another. The need for communication cannot be separated from human life, however, sometimes irresponsible individuals take advantage of these means of communications by scamming via text messages. Various development in smartphone technology that can access the internet in considerable speed, slowly but surely, have changed behavior, both individuals and society in general. The development of information and communication technology has caused world relations to be borderless and has caused significant social, economic and cultural changes in society so rapidly. Nasution, (2014) stated that information technology continues to grow so rapidly and penetrates other fields, but this growth is not accompanied by control rules in its application.

Various crimes that use computer technology through the internet network have recently shown significant numbers, both in terms of quantity and quality. The use of computer media connected to the internet as a medium for committing crimes is generally known as cybercrime.

Cybercrime is the term that refers to criminal activity in which computers or computer networks become the means, targets, or places of crime. These include online auction fraud, check fraud, credit card fraud, confidence fraud, identity fraud, child pornography, etc.

Modus operandi is the way or how a crime is committed. The modus operandi of a cybercrime conducted to cellular phone users is very diverse and continues to develop in line with technological developments. However, under close examination,

many of these crimes share the same characteristics as other crimes, only the locations are different.

The mode of SMS scams frequently occurs in the communities, in both the lower- and upper-class communities. However, in such cybercrime cases it is difficult to find the perpetrator because the cards used for committing the crime are usually immediately destroyed after completing the transaction, making tracing difficult.

It is necessary to pay attention to how the state provides legal protection for victims of cybercrime and the extent to which criminal law can contribute to the new regime related to the abuse of modern information technology.

The criminal law has the principle of legality, as stipulated in Article 1 paragraph 1 of the Indonesian Criminal Code, no act shall be punished unless by virtue of a prior statutory penal provision. As cases of SMS scams have only emerged in the era of information technology, the Criminal Code has existed long before and has been in effect in Indonesia since the era of the Dutch colonial government.

Law number 11 of 2008 on electronic Information and Transaction (UU ITE) was established on 21 April 2008. This Law has served as the regulation which stipulate provisions concerning crimes which utilize informatics means, technology and electronics as well as provisions on protection for the communities in the event of scams, including SMS scams.

It is stated in the preamble to this law which states that the national development is a sustainable process that must constantly be responsive to the various dynamics that occur in society. The Law also states that electronic information and/or electronic documents and/or the printouts of such electronic information and/or electronic documents are valid legal evidence. This provision is an extension to legal evidence in accordance with the applicable procedural law in Indonesia, namely Law Number 8 of 1981 on Code of Criminal Procedure (KUHAP).

Based on this definition, according to Law Number 11 of 2008, electronic evidence or electronic documents such as proof of SMS are considered valid evidence. This Law, which has been amended by Law Number 19 of 2016, is applicable to any person who commits a legal act as regulated in this law which violates one's interests, either within or outside the jurisdiction of Indonesia.

The Criminal provisions in Law Number 11 of 2008 are stipulated in Article 27 to Article 37. Therse articles regulate prohibited acts or acts that violate the law and can be subject to criminal sanctions. The provisions of paragraoh (4) refer to the provisions of extortion and/or threats stipulated in the Criminal Code (KUHP).

METHODOLOGY

Tis study applies the the normative juridical research method where the reference materials used are statutory regulations as the main material (primary legal materials and secondary legal materials) which include literatures, legal books, legal journals, scientific works, journals discussing the ITE Law and the role of criminal law in tackling criminal acts of scams via SMS.

RESULTS AND DISCUSSION

Cases of SMS scams which lure their victims by lottery prizes have been rampant in around 2011. This include rampant circulation of the horrendous

SMS "*mama minta pulsa* (mom, get me cellular credit)" scams. Not a few people or cellular phone users are deceived by this fraudulent SMS.

In order to reduce the rampant scam case, the Indonesian Telecommunication Regulatory Body (BRTI) appealed to operators to block cellphone numbers used to deceive victims. BRTI also asked cellular operators to implement a new regulation scheme for paid cross-operator SMS and reduce sales of free calls and SMS. The goal is to minimize fraudulent crimes using the modus operandi utilizing the cellular phones.

Such interference from the regulators, operators, and the police in the forms of firm actions against the perpetrators of fraudulent SMS has succeeded in reducing the circulation of SMS scams in the country. However, it did not last long, unsettling SMS reappeared and haunted the public.

This time, the Financial Services Authority (OJK) opened a Financial Customer Care (FCC) service to receive complaints about SMS scams received by the public. In the middle of last year alone, OJK has received tens of thousands of complaints from the public regarding fraud via SMS.

The lure of winning the lottery with cars or cash prizes is a surefire way to ensnare potential victims. Perpetrators require the victims to transfer money to certain account numbers or provide another cellular phone number within the message for further inquiries. Many of people do not aware that they have been targeted for fraud.

For example, when someone is in the middle of an actual trading process and expecting for the sellers' follow up then suddenly receive an SMS which says "just wire the money to the account number xxxxxxxxxxx on behalf of Mr. xxx", this person would assume that the message was sent by his/her counterpart. Assuming that it was an actual deal, this person would immediately transfer the fund and only then the person would realize that it was a fraud.

Examples of the circulating SMS scams are as follow:

1. SMS scam on lottery from the number +6285386119773 on 15 September 2020 at 16:50 pm saying: "*SHOPEE SEPTEMBER, anda M-dapatkan h4diah cek Rp.175.000.000dari SHOPEE 2020 untuk Informasi pin [J7k2b59] klik S.ID/programhadiah-2020*." (SHOPEE SEPTEMBER, you have received a check of Rp175,000,000 from SHOPEE 2020. Information on PIN [J7k2b59] klick S.ID/programhadiah-2020).

2. SMS scam sent from +6285251310960, on 10 September 2020 at 16:59 which says: "*SIM CARD Anda resmi mendapatkan Rp. 175.000.000 Pada kode Pin [25f4777] info klik s.id/shopeeid542*" (your SIM CARD has officially received Rp175.000.000 with PIN code [25f4777] info klick s.id/shopeeid542).

3. SMS scam sent by +6285330038486 on 3 September 2020 at 13:15 pm: "*REJEKI 2020 Selamat anda mendapatkan cek tunai dari SHOPEE 2020 untuk Info ID_KBR99D7 Klik Ling : http://bit.ly/supershoping2com".* (REJEKI 2020 Congratulation you have received a check from SHOPEE 2020 for info ID_KBR99D7 Klik Ling : http://bit.ly/supershoping2com).

4. SMS scam sent from +6282339618310 on 16 September 2020 at 15:39 pm: "*nomor anda terpilih mendapatkan Rp. 125 juta program tahunan Rejeki*

SHOPEE 2020 code ID[257A7G77] untuk cara pengambilanklik bit.ly/infohadiah1212" (your number has been selected to receive Rp.125 million from Rejeki SHOPEE 2020 program code ID[257A7G77] for instruction click bit.ly/infohadiah1212).

5. *Info Resmi*
   Selamat, No. Anda Terpilih
   Mendapatkan hadiah ke-2
   Cek Tunai Rp175juta dari PT. Shopee
   Pin Pemenang (B8337h9) U/Info Klik:
   bit.ly/pesta-shopee255
   dikirim oleh 082346034113
6. *Pesan Resmi*
   PT. Shopee Indonesia
   No. Anda mendapatkan Hadiah
   Ke-2 Cek Tunai Rp175juta
   PIN Pemenang (B8337H9)
   U/Info Hadiah klik bit.ly/bigsale-10m85
   dikirim oleh 081525877957
7. *PESAN TERAKHIR!*
   Anda pemenang terpilih
   HADIAH SHOPEE
   Rp. 125.000.000
   PIN (AAQ2099)
   Info klik link:
   bit.ly/shopee-newyearwinsale
8. *Anda Pemenang KE2*
   Rp.125.000.000.00
   SHOPEE REJEKI
   awal tahun 2020
   PIN.(AAQ2099)
   Silahkan buka link di bawah
   bit.ly/undianhadiahshopee
9. PESAN TERAKHIR
   Anda Pemenang
   Undian SHOPEE
   ELEKTROSALE 4.4
   Rp.150.000.000,-
   PIN: (C118D89)
   U/Info Klik:
   bit.ly/shopeeid-44
10. Surat keputusan
    PT.SHOPEE
    menetapkan anda
    Sebagai pemenang
    K-2
    Cek 175jt
    PIN:j7k2b59
    u/info klik;
    layananshopee tk
11. Pesan resmi
    Anda pemenang
    Undian SHOPEE
    Big Ramadan
    Rp. 150.000.000,-
    Pin: (C118D89)
    U/Info klik:
    bit.Iy/ramadanshopee20
12. Kpd Anda sbgai
    Pemenang ke2
    Undian shopee
    Ramadhan Big sale
    cek 175
    ID: J7K2B59
    ayo ambl hadiah anda
    U/Info Klik
    www thrshopee cf
13. SHOPEE INDONESIA!!!
    Selamat…
    No.Anda Resmi Meraih
    Hadiah THR Rp.175Juta
    Dari SHOPEE
    ID Pemenang
    (J7K2B59)
    U/Info Hadiah Klik:>
    bit.ly/gebyar-thrshopee83
14. SHOPEE THR
    Slmt.
    No.+6287813xxxxxx
    Anda resmi
    men-dptkan hadiah
    ke-2 cek tunai
    Rp.175jt kode PIN
    pemenang :(25f4777)
    U/Info hadiah
    klik.
    www.grandprize23.com

These SMS were sent to the writer's number.

Report any SMS scams in the forms of fund transfers to certain account numbers to OJK's FCC service by following these steps:

1. Screen capture or screenshot the SMS scam
2. Report the screen capture via OJK customer service e-mail konsumen@ojk.go.id)
3. In addition to *e-mail*, you can also contact 1-500-655
4. Account number and Bank name are required as evidence in order for OJK to follow up the report. OJK will order the bank

to freeze the account in order to avoid future scams.

5. OJK also coordinates with Ministry of Communications and Informatics (MCI) to block the celluler numer used for crime.

In addition to OJK customer service, public may submit complaints on SMS scams through electronic mail to MCI at the email address *aduankonten@mail.kominfo.go.id***.**

Perpetrators of SMS scams can be charged under Article 28 paragraph (1) of the electronic Information and Transaction Law (ITE) with the sanctions of a maximum of 6 years of prison or a fine of Rp1 billion.

Cybercrime as a Threat

The development of global computer network technology or the Internet has created a new world called cyberspace, a computer-based communication world that offers a new reality, namely virtual reality.

Cybercrime actors who use cellular phones as objects of crime are targeting user data, collections or security systems with motives for certain purposes, for example, user data is used as marketing objects, theft of collections for commercial purposes.

For this reason, telecommunications providers must be able to identify attacks against users they manage so that all existing systems, collections and data are safe from attacks that can harm many parties. Some of the supporting factors are:

a) Computational and communication technology which enables the creation, collection and manipulation of information in place.
b) International network infrastructure to support connections and operational capabilities for users.
c) Developing Online information.
d) Emerging common internet access frameworks.
e) One of the challenges currently faced by telecommunications service providers is how to protect their collection of information from various kinds of disturbances and threats against their customers.

Definition of *Cybercrime*

Cybercrime is a form of crime that occurs because of the use of internet technology. Some experts assume cybercrime as computer crime. The U.S Department of Justice defines the criminal computer as "any illegal act requiring knowledge of computer technology for its perpetration, investigation, or rosecution".

This definition is identical to that given by the Organization of European Community Development, which defines computer crime as "any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Abdul Wahid (2005) states that Cyber Crime is any kinds of use of computer networks for criminal purposes and/or high-tech crimes by misuse of the convenience of digital technology. From some of the above definitions, it can be briefly defined that cybercrime is an illegal act committed by using the internet based on the prowess of technology, computers and telecommunications, whether for profit or not, which is detrimental to other parties.

Ikka (2018) argues that in the world of the Internet, the potential for crime is very large and the perpetrators are very difficult to apprehend because

in this virtual world, most of them use fictitious identities.

Sumarwani (year) states that "This development has brought humans to the threshold of the fourth revolution in the history of human thought when viewed from the construction of human knowledge which is characterized by a borderless way of thinking".

Characteristics of Cybercrime

In conventional crime, two types of crime are recognized as follows:

1) Blue Collar Crime

   This crime is a type of crime carried out conventionally such as robbery, theft, murder, etc.

2) White Collar Crime

   This type of crimes of is divided into four groups of crimes, namely corporate crimes, bureaucratic crimes, malpractice, and individual crimes.

Cybercrime is a crime that arises as a result of the virtual world community on the internet, which has its own characteristics that are different from the two models above. The unique characteristics of cybercrime include the following five points:

a. Scope of crime
b. The nature of the crime
c. Perpetrator
d. Crime mode
e. Types of losses arising from the above characteristics.

To facilitate the handling, cybercrime can be classified into:

a. Cyberpiracy

   The use of computer technology to reprint software or information, then distribute the information or software through computer technology.

b. Cybertrespass

   The use of computer technology to increase access to an organization's or individual's computer system.

c. Cybervandalism

   The use of computer technology to create programs that interfere with electronic transmission processes, and destroy computer data.

Types of Cybercrime

The types of cybercrime based on their motives include:

1. Cybercrime as a pure crime, where a person commits a crime deliberately, in which the person deliberately destroy, steal, or disturb an information system or computer system
2. Cybercrime as an act of gray crime.

   The motive of such crime is not clearly distinguished between a pure crime or not considering that it is a tresspassing without destroying, stealing or disturbing information system or computer system.
3. Cybercrime that attacks individuals.

   Crimes committed against other people with the motive of vengeance or for entertainment which aim to destroy one's good name, or attempts to exploit other for personal satisfaction. For example, pornography, cyberstalking, etc.
4. Cybercrime that attacks copyright (property rights). A crime committed against someone's work with the motive of duplicating, marketing, modifying the

purpose of personal/public interest or for material/non-material purposes.

Cybercrime Modes

Modes and manners of committing cybercrime:

1. *Unauthorized Access to Computer System and Service*

   Crimes committed by tresspassing/infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system entered.

   Usually criminals (hackers) do so with the intention of sabotage or theft of important and confidential information. However, there are also those who commit it simply because they feel challenged to penetrate a system that has a high level of protection. This crime has become more prevalent with the development of internet/intranet technology.

2. *Illegal Contents*

   This crime involves entering data or information on the internet about something that is false, unethical, and can be considered to violate the law or disturb public order. For example, fake news or defamation that can harm other parties' reputation, pornography, or disclosure of state secret information, agitation, and propaganda against the legitimate government, and so on.

1. *Data Forgery*

   It is a crime to falsify data on important documents stored as scriptless documents via the internet. This crime is usually aimed at e-commerce documents by making as if a "typo" occurred which will ultimately benefit the perpetrator.

2. *Cyber Espionage*

   It is a crime that takes advantage of the internet network to carry out espionage activities against other parties, by entering the target party's computer network system. These crimes are usually directed against business rivals whose important documents or data are stored in a computerized system.

3. *Cyber Sabotage and Extortion*

   This crime is committed by disrupting, destroying or deleting data, computer programs or computer network systems connected to the internet. Usually it is committed by inserting a logic bomb, a computer virus or a certain program, to make data, computer program, or computer network system cannot be used, fail to run properly, or runs as the perpetrator's intentions. In several cases, when such a crime is committed, the perpetrator offered to repair the data, computer program or computer network system that had been sabotaged, of course for a certain fee. This crime is often referred to as cyberterrorism

4. *Offense Against Intellectual Property*

   This crime aims at intellectual property rights owned by other parties on the internet. For example, illegally imitating the appearance of a web page on another person's site, broadcasting information on the internet that turns out to be someone else's trade secret, and so on.

5. *Infringements of Privacy*

   This crime aims at a person's information which is highly classified or confidential. This crime is usually committed on a a person's personal information stored on computerized personal data forms, which, if known by other people, can incur material or immaterial losses, such as credit card numbers, ATM PIN numbers, information on disabilities or hidden diseases

and so on.

6. *Cracking*

   This crimesuses computer technology to destroy the security system of a computer system to commit theft, anarchist actions after gaining an access. The terms hackers and a crackers are often misinterpreted, where people associate hackers with negative actions, ewhile in fact, hackers are people of great interests to programming and believe that information is invaluable and aware of the fact that not all information can be published and are confidential.

7. *Carding*

   It is a crime which uses computer technology to carry out transactions using another person's credit card, incurring material and non-material losses.

Cybercrime Countermeasures

To tackle the increasingly widespread internet crime, it is necessary for every country to have awareness on the dangers of internet abuse. Followings are the global measures to counter ctbercrime:

1) The modernization of the national criminal law and its procedural law to be in line with international conventions related to such crimes.
2) Increasing the standard of security for the national computer network system in accordance with ithe nternational standards.
3) Increasing the understanding and expertise of legal officials regarding efforts to prevent, investigate, and prosecute cases related to cybercrime.
4) Increasing citizen awareness about the dangers of cybercrime and the importance of preventing these crimes.
5) Increasing cooperation between countries in the field of technology regarding cybercrime violations. So broadly speaking, for global countermeasures, cooperation between countries and the application of standardized international laws to combat cybercrime is required.

Law Enforsement

Cybercrime law enforcement, especially in Indonesia, is influenced by five factors, namely the law, the mentality of law enforcement officers, community behavior, facilities and culture. Law cannot enforce itself; it always involves humans and also involves human behavior in it.

The law also cannot be enforced without law enforcement. Law enforcers are not only required to be professional and smart in implementing legal norms but also deal with someone and even groups of people who are suspected of committing crimes.

Along with the development of technology and the development of crime, especially the increasingly alarming development of cybercrime, law enforcers are required to work harder because law enforcers are the first line of defence to fight against cybercrime. For example, UN Resolution No.5 of 1963 on efforts to combat crimes against technology misuse, indicates that currently the world is facing a critical and serious crisis that must be addressed immediately.

The Criminal Code (KUHP) is still used as the legal basis for catching cybercrime, especially the types of cybercrime that meet the elements in the articles of the Criminal Code, and Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE),

The perpetrator or suspect under the ITE Law is likely to be subject to Article 27 paragraph (3) in

conjunction with Article 45 paragraph (1) of the ITE Law, with the threat of 6 years in prison and a fine of Rp1 billion. The law shall be viewed as a producer of order, therefore it must be guarded in various ways, including the idea of legal certainty.

The Role of Criminal Law in Tackling SMS Scams

Secara umum hukum pidana berfungsi untuk mengatur

In general, criminal law functions to regulate people's lives so that public order can be created and maintained. Humans, in an effort to meet the different needs and interests of their lives, sometimes experience conflicts with one another, which can cause harm or interfere with the interests of others.

In an effort to meet the necessities of life, the law provides rules that limit human actions, so that they cannot do everything as they please. With regard to the objectives of criminal law (S*trafrechtscholen*), there are two ideologies of the formation of criminal law regulations, namely:

According to Sudarto (YYYY) the function of criminal law can be distinguished as follows:

1. Common functions

   Criminal law is a part of law, therefore the function of criminal law is similar to the function of law in general, namely to regulate social life or to organize order in society;

2. Special functions

   The special function for criminal law is to protect legal interests against acts that intend to rape them (r*echtsguterschutz*) with sanctions in the form of crimes that are sharper in nature when compared to sanctions contained in other branches of law.

In criminal sanction, there is a tragic factor (something unpleasant) so that there is a metaphore for criminal law that says criminal law is like slicing one's own flesh or a double-edged sword which means that the criminal law aims to protect legal interests (for example: life, property, independence, honor), but if there is a violation against the prohibitions and orders, it actually imposes injury (hurts) the legal interests (objects) of the offender. It can be said that the criminal law provides rules for dealing with evil acts. In this case it is necessary to remember that as a means of social control the function of criminal law is subsidary, meaning that criminal law should only be introduced (used) if other efforts are inadequate, namely:

1. There are three types of legal interests that must be protected, namely

   1) Individual legal interests (*individuale belangen*), for example legal interests against the right to live (life), legal interests over bodies, legal interests in property rights, legal interests against self-respect and reputation, legal interests against moral feelings, and so on;
   2) The legal interests of the community (*sociale of maatschappelijke belangen*), for example for the legal interests of security and public order, traffic order on the highway, and so on;
   3) The legal interests of the State (*staatsbelangen*), for example legal interests for state security and safety, legal interests towards friendly countries, legal interests for the dignity of the head of state and representatives, and so on.

In this regard, the role of criminal law can be seen as an effort to prevent people from committing a criminal act, and a role as a tool to deal with

criminal acts committed and efforts to overcome them.

Efforts to prevent crime can mean creating certain conditions so that crimes do not occur, including formulation of laws. Meanwhile, mitigation or repressive efforts are to enforce the rules of criminal law by imposing criminal penalties on those who violate these criminal rules.

2. Crime prevention efforts:

a. *Criminal application*

For example, Article 378 of the Criminal Code with a maximum sentence of 4 years, so in this system, both lawsuits and verdicts.

b. *Preventif without punishment*

For example, by applying maximum punishment to the perpetrators.

For example, a conditional/probationary sentence indirectly provides prevention (from crime) to the public even though it is not subject to punishment or as shock therapy to the community.

c. *Influencing views of society crime and punisment* public views on crime and punishment through the mass media. For example, disseminating a law by providing a description of what are the offense and the threat of punishment.

3. Crime prevention consists of two main parts, namely:

1) Preventive efforts are initial efforts made by the police to prevent criminal acts from occurring.
2) Repressive action in the form of crime prevention is the application of criminal law rules for those who violate them.

The law enforcement mechanism for criminal cases of fraud through electronic media in the criminal procedure law has regulated the process of handling cybercrime starting from investigations to court decisions. SMS scam is also a category of cyber crime.

Obstacles in law enforcement in cases of SMS scams include:

1. SMS scams are usually committed by multiple conspiring perpetrators.
2. Perpetrators often moves places.
3. The perpetrator used several cellular cards and then destroyed them after being used.
4. In general, investigators have not been trained to carry out tracing using modern information technology. Many investigators are not technology savy.
5. SMS scam is considered a high-tech crime, while there are limited Forensic Computing Laboratory at the Regional Police stations, in fact, some do not have one.
6. The legal awareness of victims of SMS scams to report is still very low, due to the understanding that reporting to the police will result in higher costs than the amount of losses suffered.
7. The law of evidence used by investigators is solely bound by the Criminal Procedure Code. Meanwhile, fraud with electronic devices can also be proven with recorded images or sound. In the Criminal Procedure Code this has not been regulated so that law enforcers are still hesitant to use the ITE Law in investigations.
8. The position of witnesses to victims of criminal acts of scams is very decisive in the evidence in court, while most of the victim witnesses are located far away and some even are abroad. This can hamper the law enforcement process because

the cost of bringing in victim witnesses is considerably high.

9. No regulations in place in Indonesia which regulate SMS scams, online buying and selling transactions, resulting in the commonly occurred fraud.
10. Investigating institutions (Police and Attorney) have not had any collaboration with the operators to anticipate cases of SMS scams.

Even though the ITE Law does not limitatively say "scam", but in relation to elements of consumer losses and elements of electronic transactions, article 28 paragraph 1 will complement article 378 of the Criminal Code, when the criminal act of fraud is committed using SMS facilities available on electronic devices (cellular phone). So, Law No. 11 of 2008 jo (Law No. 19/2016) as an extension of the Criminal Code if the crime is committed with information technology or electronic devices/cellular phones.

For this reason, every member of the community must be aware of the criminal act of fraud via sms by paying attention to the following steps:

1. Report to the police immediately whenever SMS scams occur.
2. Check the accuracy of the information through official channels.
3. Report via SMS to the provider before reporting to the police.
4. Be alert and careful and do not easily believe.
5. Do not be easily tempted and make financial transactions.

CONCLUSION

One of the negative impacts of the information technology is the emergence of a new crime mode using cellular phone in the form of fraud using the short message service (SMS). The increase in fraud using cellular phones is because perpetrators consider that their crimes will not be cracked by both victims and the police.

As previously described, it can be concluded that the regulation regarding fraud committed through electronic media is in principle similar to that of conventional fraud, the only difference is the means of action, namely using electronic systems (computers, internet, telecommunication equipment-cellular phones). Therefore, legally, fraud through electronic media can be treated the same as conventional offenses stipulated in the Criminal Code (KUHP). Thus, in the process of handling cases, law enforcement officials can apply legal provisions, both those contained in the Criminal Code and the legal provisions contained in Law No. 11 of 2008 (Law No. 19/2016).

Likewise with the proceedings, fraud through electronic media will be formally processed and handled by investigators, in accordance with the provisions stipulated in the Criminal Procedure Code. This is also in accordance with the provisions subject to criminal penalties in accordance with Article 45A paragraph (1) of Law 19/2016, fraud that causes consumer losses in Electronic Transactions. In Article 1 number 2 of Law 19/2016, it is explained that what is meant by Electronic Transactions is: Legal actions carried out using computers, computer networks, and/or other electronic media.

Recommendation

It is necessary to increase the human resources of investigators as law enforcers for mastery of technology and information technology, because SMS scam is a crime using electronics which are increasingly sophisticated in its modus of operation.

A Forensic Computing Laboratory needs to be held at least in every Regional Police in every province, so that law enforcement against Fraud via SMS can run smoothly.

It is necessary to disseminate the ITE law to the public to raise the level of public legal awareness of the importance of victim witnesses so that the public is ready to report if fraud occurs.

REFERENCES

Anton Hendrik Samudra," Modus Operandi Dan ProblematikaPenanggulangan Tindak Pidana Penipuan Daring, MIMBAR HUKUM Volume 31, Nomor 1, Februari 2019, page 64

Arief, Barda Nawawi, (2006). Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia. PT. Rajagrafindo Persada, Jakarta.

Cahyo Handoko, (2016). Kedudukan alat bukti digital dalam pembuktian cybercrime di pengadilan Jurisprudence, Vol. 6 No. 1 Maret page.8

Eko Noer Kristiyanto, (2016). "Urgensi Keterbukaan Informasi Dalam Penyelenggaraan Pelayanan Publik," Jurnal De Jure 16, No. 2: 231–244. page. 232.

Ikka Puspitasari, (2018). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia, Jurnal HUMANI 8,No. 1: 1–14. page. 3.

M.E. Fuady. (2005). Fenomena Kejahatan melalui internet di Indonesia, Media Tor, Vol 6 No. 2 Desember, page. 256.

Nasution, Mahyuddin & Sitompul, Opim & Nasution, Sawaluddin. (2014). https://www.researchgate.net/publication/326380527_Perspektif_Hukum_Teknologi_Informasi/citation/download

Putri Ratnasari. (2015). Mekanisme terhadap penegakan hukum tindak pidana penipuan melalui media eletronik. Lex Administratum, Vol. III/No.1/Jan-Mar, page.135

Sajitpto Rahardjo, (2010) Penegakan Hukum Progresif, Penerbit Buku Kompas

Tony Yuri Rahmanto, (2019). Jurnal Penelitian Hukum DE JURE,Vol. 19 No. 1, Maret: 31 – 52

Theodorus J.B.R. Penipuan dengan Menggunakan Telepon Seluler Ditinjau dari KUHP,Users/ACER/Downloads/5565-9425-2-PB%20(1).pdf, UNISIA NO. 63/XXX/I/2007, page.83

Wahid, Abdul dkk, (2005). Kejahatan Mayantara, PT Refika Aditama, Bandung.