Responsibility of Maya World Crimes in Indonesia's Legal System

Henny Saida Flora
Faculty of Law, Universitas Katolik Santo Thomas Sumatera Utara
hennysaida@yahoo.com

ABSTRACT

Information and communication technology has changed the behavior of society and human civilization globally. In addition, the development of information technology has caused the world to be indefinitely and cause significant social change to take place so quickly. Information technology is now a double-edged sword, because in addition to contributing to the improvement of welfare, advancement, and human civilization as well as an effective arena of action against the law one of which is cyber crime. In Criminal Law any person who commits a crime, especially a cyber crime, remains to be observed whether the perpetrator may be subject to criminal liability if committing a crime or a violation of a crime. A person who commits a criminal offense may be liable to a crime if it satisfies all elements contained in criminal liability, whereas if the person does not fulfill any of the elements of criminal liability, it can not be punished by any lawsuit. This criminal liability issue is closely related to the error. The entire laws and regulations contained in the Criminal Code as well as the special law outside the Criminal Code, in this case is the Law Number 11 Year 2008 on Information and Electronic Transactions, in essence a unity a punishment system consisting of general rules and special rules. The general rules are contained in the Criminal Code and special rules are contained in the Information and Electronic Transactions Act, all of which will be imposed on the cyber crime if there is an element of criminal responsibility in the perpetrator.

Keywords: *Criminal Acts, Perpetrators, Maya Crime World*

1. INTRODUCTION

Almost all countries believe that science and technology is one important factor in supporting the growth of a country, in other words the progress of a country one of them is determined by its mastery of science and technology. Countries capable of mastering science and technology in degrees of degree will occupy a more dominant position compared with countries that have not mastered science and technology.

At this time, technology has grown rapidly. A technology has not been widely known by all walks of life has emerged again new technologies that again other new technologies. This results in rapidly obsolete technology. In addition, people are also required to always make adjustments to the technology continuously, because if they do not adjust or do not follow the development of technology it will be left behind in everything.

Although computer technology is relatively easy compared to other technologies but the computer has been progressing rapidly in a relatively short time. Computers as one manifestation of the success of the development of science and technology today is very beneficial in every aspect of human life. The existence of a computerized system will facilitate human to achieve various purposes in an effort to improve the welfare of his life. Computers as advanced technology products are inevitable in the development of human life. The application is now growing no longer in the university environment, research centers and laboratories for scientific purposes but now has grown in industrial environments, individuals, government agencies, military / defense security, law and justice and banking.

Information and communication technology has changed the behavior of society and human civilization globally. In addition, the development of information technology has caused the world to become boundless (borderless) and cause a significant social change so rapidly. Information technology is now a double-edged sword because in addition to contributing to the improvement of welfare, advancement and human civilization as well as effective arena of action against the law one of which is cyber crime. Banking world including banks in Indonesia have utilized the advanced technology of this computer was not spared from the rise of cyber crime (cyber crime).

On April 21, 2008, the Government approved the enactment of Law Number 11 Year 2008 on Information and Electronic Transactions containing 54 articles with 13 chapters namely General Provisions, Principles and Purposes, Information Documents and Electronic Signatures, Electronic Certification Clearance, and Electronic Systems. Implementation of electronic systems, electronic transactions, domains of intellectual property rights and

protection of private rights, prohibited conduct, dispute resolution, government roles and community roles, criminal provisions, transitional and closing provisions.

However, with the enactment of the law does not mean that internet-related issues are to be completed, not only the existence of the ITE Law which is widely viewed as highly controversial, also related to its implementation. This criticism concerns the existence of misleading, both with the universal rules of human rights in expressing opinions and harmonization between laws in the legal system.

In Indonesia the problem of cyber crime is not a new thing, but the rules to criminalize cyber crime with special rule device in the form of cyber law (UU ITE) is a new issue, because in 2008 Indonesia actually has a special umbrella for cyber crime. The criminalization policy is a policy in determining an act which was not originally a criminal act (not punishable) into a criminal offense (a criminal act). So basically criminalization policy is a part of criminal life by means of criminal law and therefore includes part of criminal law policy, especially its formulation policy.

Therefore, in cyber crime perpetrators can not continue and only refers to the Act of Information and Electronic Transactions only, but there must be a new concept of the Criminal Code. Because the old Criminal Code is no longer able to reach new criminal acts created by the development of the era, for it needed new concepts about the Criminal Code to optimize criminalization **of cyber crime perpetrators.**

Problems

As for the problem in writing is How the perpetrators accountability to cyber crime in the Criminal Code and the Law on ITE?

2. DISCUSSION

1. **Crime Against Cyber Crime (Cyber Crime)**

The emergence of today's information technology revolution and the future will not only have an impact on the development of the technology itself, but also affect other aspects of life such as religion, culture, social, politics, private life, society and even nation and state. The global information network or the internet today has become one of the means to commit crimes both domestically and internationally. The Internet becomes a medium for criminals to commit crimes with an international nature and beyond the limits or sovereignty of a country. All of this is a very interesting motive and modus operandi for the perpetrators of digital crime.

The regulation of cyber crime relating to confidentiality, integrity, the existence of data and computer systems, the use of computers as a crime tool as well as related to the contents of the data payload are:

a. Illegal Access (unauthorized access to a computer system) that is intentionally and without right to unauthorized access to all or any part of the computer system, in order to obtain computer data or other improper intent, or relate to a computer system connected to the system another computer. Illegal acces or also known as joy computing known by using someone else's computer without permission is a deed that tinkle the contents of other people's computers, both software and hardware. Illegal acces is usually done by people who want to open or steal certain data from someone's computer. The use of computers or data theft is done offline. This means that the computer does not have to always connect with the Internet network. This can be categorized as an adverse action if viewed from a polite point of view. But if this is considered a criminal act also no problem. Because illegal acces can be analogized as using the property of others without asking permission first from the owner. Computers can be classified in a person's personal property which in a person's computer typically inserts important and secret files that no one else should know. such as a company-owned computer. To anticipate the action of joy computing need to be installed password. In fact there are some people to secure the data, he installed the passwords layered start installing boot password, login password, password folder and password file. Regarding this issue, Article 30 of Law Number 11 Year 2008 on Information and Electronic Transactions has been able to ensnare the perpetrators. Article 30 of Law Number 11 Year 2008 regarding Information and Electronic Transactions states that everyone intentionally and without right or illegally accessing other people's computers and / or electronic systems (paragraph 1) by any means (paragraph 2) in what way also for the purpose of obtaining electronic information and / or electronic documents (paragraph 3), in any manner that violates, breaches, exceeds or breaches the security system. The criminal provisions of Article 30 of Law Number 11 Year 2008 regarding Information and Electronic Transactions are regulated in Article 46 of Law Number 11 Year 2008. For paragraph (1) the criminal provision is a maximum

imprisonment of six years and or a fine of not more than six hundred million rupiah. Whereas paragraph (2) of Article 46 provides for the longest imprisonment of the purpose of the year and or a fine of not more than seven hundred million rupiah. For paragraph (3) the criminal provision is a maximum imprisonment of eight years and or a fine of not more than eight hundred million rupiah.

b. Data Interference (disrupt computer data). That is to deliberately commit a destructive act, delete, deteriorate, alter or hide (suppresission) computer data without rights. The offender of this case is often called a hacker. Hackers literally mean to hack or hack. In the broadest sense are those who infiltrate or do the destruction through the computer. Hackers can also be defined as people who love to learn the ins and outs of computer systems and experiment with them. For law enforcement, the community and the media environment itself hacker is defined as cybercrime. But for the hacker community, the term computer criminals is called a cracker. The difference makes something, while crackers destroy / destroy it. Hacking is also defined as intrusion activity into a computer or network system in order to abuse or damage the existing system. The definition of the word misuse has a very broad meaning, and can be interpreted as the theft of confidential data. As well as the inappropriate use of email, such as spamming or looking for network gaps that allow to be entered. Nowadays a lot of people who have an oddity with a fad to try toughness of a company's security system or personal network. Some of them do have a noble purpose, that is to hone their skills in network security technology and usually after they successfully break through the existing security system, they with the willingness to inform the gap to the concerned to be perfected. But there is also a really pure because fad supported by the motives of revenge or evil intent to steal something of value. Article 38 of the Telecommunication Law has not been able to reach the acts of interference data or the interference system known in cyber crime. If the acts of interference and interference data are causing damage to the computer then Article 406 paragraph (1) of the Criminal Code can be applied to such actions. Article 32 Paragraph (1) of Law Number 11 Year 2008 stipulates: "Every person intentionally and without right or illegally in any way altering, adding, reducing, transmitting, destroying, removing, transferring, concealing electronic information, and / or documents electronics owned by others or publicly owned. The contents of the aforementioned article may be used to entrap the perpetrator of the crime, since its criminal elements have been fulfilled. The criminal provisions are regulated in Article 28 paragraph (1) of Law Number 11 Year 2011 which is a maximum imprisonment of eight years and or a fine of at most two billion rupiah.

c. System Interference (interrupt the computer system), that is intentionally and without right to interfere with the functioning of computer systems by entering, transmitting, destroying, deleting, declining, altering, or hiding computer data. The act of spreading computer virus programs and email bombings (electronic mail chain) is part of this type of crime that is very common.

d. Illegal Interception in The Computers, System and Computer Networks Operations (unauthorized interception of computer systems and computer operational networks), that is intentionally intercept without rights, by using technical equipment, computer data computer systems, and or computer operating networks not intended for the general public from or through a computer system including the electromagnetic waves emitted from a computer system carrying some data. The act is done with the intention of not good, or related to a computer system that is connected with other computer systems.

e. Theft Data (Stealing Data). Namely the activity of obtaining unauthorized computer data either for self-use or for giving to others. Identity theft is one of these types of evil that is often followed by the crime of fraud. This crime also often followed by crimes of data leakage. Leakage and Espionage data (leaking data and spying) involving spying and / or leaking of confidential electronic data either in the form of confidential corporate state secrets, or other data not intended for public, to any other person, body or company other, or foreign country.

f. Misuse of Devices, intentionally and without rights, produce sell, seek to

obtain for use, import, distribution or other means of interest, equipment including computer programs, computer passwords, access codes or such data, so that all or part of the computer system may be accessed for the purpose of unauthorized access, unauthorized interception, interruption of data or computer systems, or committing acts against other law.

g. Credit card Fraud (credit card fraud) is a fraudulent creditcard fraud that uses unauthorized computers and credit cards as a tool in committing crimes.
h. Bank Fraud (bank fraud). Fraud Bank is a bank fraud that is done by using a computer as a tool to perform transactions with different modus operandi.
i. Service offered Fraud (Fraud through the offering of a service that is fraud through the offer of services that exist in the internet can be email, community service, etc .. usually the form of services that given not in accordance with the offered
j. Computer Related Fraud (Fraud via computer), this crime is an activity of manipulation of information especially about finance with a target to dredge profits as much as possible.
k. Computer Related Forgery, Digital signature as a method of securitization primarily in the use of public networks as a means of data transfer, until now is one of the safest methods. It is said to be safe because digital signatures are formed from a series of algorithms only takes a very long time.
l. Computer Related Batting (gambling via computer). Gambling through computers lately is very lively. Usually will be asked to open an account on-line, where our balance is a money that will be used to play various gambling. And the balance can be refunded if we want, but of course already cut interest by service companies used. Gambling is a computer is an act of doing regular gambling that uses the computer as a tool in supporting his actions so that the act can be temporarily threatened with Article 303 of the Criminal Code

ITE Law is perceived as cyber law in Indonesia, which is expected to regulate all affairs of the internet world (cyber) including in giving punishment against cybercrime perpetrators. Cyberlaw is a shared need, cyber law will save the national interest, internet businessmen, academics, and society in general, so it should be supported. In general it can be concluded that the Law of ITE can be called a cyberlaw because the content and wide coverage of cyber crime to deal with internet banking, although on some sides there is not too straightforward and also there is a little missed.

2. **Criminal Law Enforcement Measures against Cyber Crime (Cyber Crime)**

In conducting criminal law enforcement against especially about cyber crime, legal action is carried out by the investigator consisting of Indonesian National Police and Civil Servant Investigator. The investigation is conducted under the Criminal Code and the Electronic Information and Transaction Act (UU ITE).

The authority of the civil servant investigator as stated in Article 43 of the ITE Law is:

a. Receive reports or complaints from a person about a crime under the provisions of the ITE Law
b. Calling any person or other party to be heard and / or examined as a suspect or witness in connection with alleged offense in the field related to the provisions of the ITE Law
c. Conduct an examination of the correctness of reports or information regarding criminal offenses under the provisions of the ITE Law
d. Conduct examination of persons and or business entities that are suspected of committing a crime under the ITER Law
e. Conducting inspection on tools and or facilities related to information technology activities suspected to be used to conduct criminal tinda based on UU ITE
f. Conduct a search of a certain place allegedly used as a place to commit a crime under the provisions of the ITE Act
g. Conducting sealing and seizure of information technology tools and / or facilities allegedly used in deviation from the provisions of legislation
h. Require the necessary expert assistance in the investigation of a crime under the ITER Act and / or
i. Conduct a termination of criminal investigation under the ITER Act in accordance with applicable criminal procedural law.

As for the special authority of PPNS ITE, among others:

1. Entitled to conduct arrest and detention (Article 43 paragraph (6) UU ITE)
2. Submitting the warrant begins the investigation and the results of the investigation to the prosecutor and coordinates with the POLRI (Article 43 paragraph (7) of the ITE Law).

The special requirement of the investigation shall be conducted with due regard to the protection of privacy, confidentiality, smooth public services, data integrity / data integrity in accordance with the provisions of legislation

(Article 43 paragraph (2) of the ITE Law). The special protection of electronic systems of electronic search and / or seizure of electronic systems related to alleged criminal offenses shall be made by the permission of the local district court (Article 43 paragraph (3) of the ITE Law). In the conduct of searches and / or seizures of the electronic system the investigator shall maintain the maintenance of public service interests (Article 43 paragraph (4) of the ITE Law).

While the protection of human rights is contained in Article 43 paragraph (6) of the ITE Law, which affirms, in the case of arrest and detention, the investigator through the public prosecutor shall request the appointment of the local court chairman within one twenty-four hours. Electronic information and electronic data, including prints, are defined as valid evidence as an extension of valid evidence in accordance with Article 1 paragraphs 1 & 4 of the ITE Law. As for the requirements of electronic information and electronic documents in accordance with the provisions of the Law on ITE (Article 5 paragraph (3) UU ITE).

3. CONCLUSION

Cyber crime prosecution often faces obstacles, especially in arresting suspects and seizure of evidence. In the arrest of suspects often the police can not determine exactly who the perpetrators because they do enough through the computer that can be done anywhere without anyone knowing so there is no witness who knows directly

Cyber activities, although virtual in nature, can be categorized as real actions and legal acts. The juridical for the cyber space is no longer in place to categorize something by the size and qualifications of conventional law to be made object and action, because if this way taken will be too much trouble and things that escape from the law snares. cyber activity is a virtual activity that has a very real impact even though the evidence is electronic. Thus the subject of the culprit must also be qualified as a person who has committed a real legal act.

In the cyber space the perpetrators of violations often become difficult to get snared because Indonesian law and courts do not have the jurisdiction of perpetrators and legal acts that occur, since transnational offenses are transnational but the consequences have legal implications in Indonesia. In international law are known three types of jurisdiction namely jurisdiction to establish laws, jurisdiction for law enforcement and jurisdiction to prosecute.

REFERENCES

Andi Hamzah, 2009, *Delik-Delik Tertentu di dalam KUHP*, Sinar grafika, Jakarta

Agus Rahardjo, 2002, *Cybercrime,* Citra Aditya Bakti, Bandung.

Asril Sitompul, 2010, *Hukum Internet*, Citra Aditya Bakti, Bandung

Aloysius, Wisnubroto, 2000, Kebijakan hukum Pidana dalam Penanggulann Penyalahgunaan Komputer, Penerbit Univresitas

Barda Nawawi Arif, 2006, Tindak *pidana Mayantara, Perkembangan Kajian Cyber Crme di Indonesia*, Rajagrafindo Persada, Jakarta.

Barda Nawawi dan Muladi, 2007, Bunga Rampai Hukum Pidana, Alumni, Bandung.

Efa Laela Fakhriah, 2009, *Bukti Elektronik Dalam Sistem Pembuktian Perdata*, Alumni, Bandung.

M. Ahmad Ramli, *Cyber law dan HAKI dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung.

Niniek Suparni, 2009, *Cyberspace, problematika, & Antisipasi Pengaturannya*, Sinar Grafika, Jakarta,

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta

Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik*

Kitab Undang-Undang Hukum PIdana