CYBERCRIME COMPARISON UNDER CRIMINAL LAW IN SOME COUNTRIES

Andri Winjaya Laksana
Faculty of Law UNISSULA
andriwinjaya@gmail.com

Abstract

Cybercrime has been become a major portion for law enforcement agencies and intelligence services to both national and international matter, development of information and technology's crime resulted in every country have a different policy of criminalization. The emphasis on cross-country has made a crime on the internet is not just a national issue, but has become an International problem. therefore it is important to have uniformity in the prevention of cybercrime that this crime can be solved. Based on the comparison of cybercrime that included the rules from various countries including the United States, Singapore, the Netherlands, the Philippines, Myanmar as a reference in the application of criminal law enforcement regulations regarding cybercrime seal the document.

Keywords*: Cybercrime; Comparison; Some Countries.*

A. INTRODUCTION

The development of technology has been significant, so that there was development in various aspects of community life. Including the business community, while the trade community had used the technology advances. Not only that occurred in trade traffic, but also in the trade relationship. Among the activities in the trade are also used banking services, in which the development occurs even this sector are also technological developments.[1]

Developments in information technology have transformed almost all facets of life. In one side of the computer technology has the advantage of an opportunity to get information, work, participate in politics and democratic life and other advantages, but on the other hand, information technology will "bite" real life which we have long struggled with all existing heritage. Netizens can see this as a problem to be solved before it moves further down the road and alleys of cyberspace.

From the beginning people are always looking for ease in carrying out the activities in achieving life. It has been fulfilled with the advancement of technology. Nonetheless, people are still not satisfied, so always look for the possibility to easily meet their needs.

On the other hand to achieve common needs someone actually doing is reprehensible. Both in the field of trade and nor in any field where people are doing business. Included in the negative activities are the activities in the field of banking. Resulting also in the banking sector is directly engaged in the money, so it is very gimmicky, whether in business ventures which can be positive or negative events.

1 Loebby Loqman 2002, *Kapita Selekta Tindak Pidana Di Bidang Perekonomian,* First Edition, Datacom, Jakarta, P.46.

Crime by using technology, namely information technology, especially computers and the Internet (cyber crime) has reached the stage of worrying. Advances in information technology, in addition to bringing the business world into a revolutionary (digital revolution era) the very practical, it has a horrible dark side, such as pornography, computer crimes, even digital terrorism, information warfare garbage, and hackers.[2]

The rapid development of telecommunications technology and computer technology produces multifunctional internet. This development brings us to the threshold of the fourth revolution in the history of human thought when the review of the construction of human knowledge which is characterized by the way of thinking without borders (borderless way of thinking). Acceleration technology progressively increasing the material cause continuous changes in all interactions and activities of the information society.

Advances in technology have brought about changes and rapid shifts in a life without limits. Utilization of these technologies have encouraged rapid business growth, due to a variety of information can be presented via a long distance relationship and those who want to enter into transactions do not have to meet face to face, but simply through a computer and telecommunications equipment. Developments in information technology also establish a new world society that is no longer hindered by territorial boundaries and have reversed everything away so close to the imaginary so real. But behind the progress it has also spawned new unrest-unrest with the advent of sophisticated crime in the form of cyber crime.

In accordance with the development of science and technology, especially information and communication technologies have contributed to improve actions, dissemination and use of the Internet that an adverse influence on the moral and noble personality of the Indonesian nation that threatens the life and social fabric of Indonesian society.[3]

With the existence of this gap, the current information technology in this case is a computer technology, especially the Internet has been highly developed in remote villages though and has been used as a means and media to commit crimes, the law we can not reach them so that the perpetrators of crimes technology has not yet or no can not be convicted and sentenced for the act of doing and their completion is not clear to cases of crimes other technologies is the case without the knowledge and without us knowing.

Cybercrime has been become a major portion for law enforcement agencies and intelligence services to both national and international non-pratisi exception practitioners of business, the merchant, the customer, to the end-user. In most cases, Internet crime begins by exploiting the hosts and computer networks therefore the swindlers and entruder coming across networks, especially networks based on TCP/IP protocol.[4]

2 Ade Maman Suherman 2005, *Aspek Hukum Dalam Ekonomi Global*, Revised Edition, Ghalia Indonesia, Bogor, P.189.

3 Suratman, Andri Winjaya Laksana, *Analisis Yuridis Penyidikan Tindak Pidana Pornografi Berdasarkan Undang-Undang Nomor 44 Tahun 2008 di Era Digitalisasi*, Jurnal pembaharuan hukum, Volume I No. 2 Mei-Agustus 2014, P.169.

4 Rachmat Rafiudin 2009, *Internet Forensik*, CV Andi Offset, Yogyakarta, P.1

In connection with the perpetrators of cybercrime that has unique characteristics, the authors argue that the imposition of imprisonment for perpetrators of cybercrime as practiced in Indonesia for this is a step that is not wise. This is caused by the mismatch between the characteristics of the offender with guidance systems inmates in correctional institutions, so that the objective of sentencing how regulated in the law community will not be achieved. The author argues kind of imprisonment can be replaced with social work or criminal criminal surveillance, because there is a match between the characteristics of the perpetrators of cybercrime with the paradigm of punishment in criminal social work and criminal surveillance, so that the purpose of punishment can be achieved. Criminal and criminal social work and prospective surveillance more humane than imprisonment. Results of research in some countries, social work and criminal criminal pretty effective supervision applied to the perpetrators of the crime, including cybercrime. In eight countries around the world threatened by the criminal perpetrators of cybercrime social work, and it is not contrary to the provisions of the convention on cybercrime.

Computer-related crime is an overall form of crime directed against the computer, computer network and its users and traditional forms of crime that use or with the aid of computer equipment. The offense is differentiated into two categories namely Cybercrime. It is in the narrow sense and in a broad sense.

Cybercrime in the narrow sense is a crime against computer systems, while cybercrime in the broad sense includes crimes against the system or computer network and crimes using computer facilities. The only international instrument which regulates Cybercrime is the Convention on Cybercrime, signed in Budapest (Hungary) in 2001. The Convention is directed mainly in an effort to (1) the harmonization of the elements of the laws governing material criminal offense under national law in conjunction with the provisions of Cybercrime, and (2) complete the formal criminal law of national importance to the process of investigation, investigation, and prosecution of offenders who use or addressed on a computer system, along with the evidence relating to these crimes.

Currently the convention already in force, because it meets the requirements stipulated in the convention. Convention on Cybercrime does not regulate in detail about the types of sanctions that can be threatened left entirely to the parties ratifying or acceding to the treaty. The penalties may be imposed on people who commit a violation of the provisions of Article 2 through Article 12 is sanctions that are effective, proportionate, and can educate, including criminal deprivation of liberty (imprisonment).

Under the provisions of Article 13 can be seen that each State authorities determine what kind of sanctions threatened against the perpetrators of cybercrime to everyone, whether human or legal entities.

B. DISCUSSION

Relating to cybercrime in Indonesia, until this time the majority of cybercrime has not been regulated in a clear legal norms in the legislation, because it was in prosecuting cybercrime applied the provisions of the Criminal Code and the provisions of the Act beyond the Criminal Code. The provisions in the Criminal Code

that can be used to prosecute cybercrime by way of interpretation, extensive is the provision on the crime of counterfeiting (as stipulated in Article 263 to Article 276), the crime of theft (under Article 362 up to 367), the crime of fraud (as under Article 378 up to 395), and the crime of destruction of goods (as stipulated in Article 407 through Article 412).

Imprisonment for perpetrators of cybercrime in the Draft Bill is also very dominant, in fact none of the types of crimes that are not punishable by imprisonment. Based on the comparison between the results of a study of the 56 foreign nationals with criminal law provisions in the Indonesian criminal law and the Criminal Code draft above can be seen kind of criminal imprisonment be the most dependable staple in most countries criminal policies.[5]

Completion of cybercrime is an indicator of a decrease in work ability of Indonesian National Police in the investigation, as well as a decrease in the ability of the criminal law in solving the crime. Factors decline in legal ability to solve crimes occur because of the legal structure of the legal function is not developed in parallel so that law enforcement tends to weaken.[6]

Comparison criminalization of "cybercrime" in seventy foreign countries are: Albania, South Africa, Argentina, USA, Azerbaijan, Bangladesh, the Netherlands, Belgium, Botzwania, Brazil, Bulgaria, Blyelorusia, Chile, China, Cyprus, Cheznya, Denmark, Estonia, Finland, Georgia, Italy, Iceland, Jamaica, Nicaragua, Slovakia, Slovenia, Sri Lanka, and Tunisia. etc., obtained descriptions of Cybercrime settings as follows:

a. Countries that have not made amendments to the Criminal Code and does not have specific legislation to regulate Cybercrime is Argentina, Bangladesh, Bostwania, Cyprus, Cezhnya, Iceland, Jamaica, Nicaragua, Slovakia, Slovenia, Sri Lanka, and Tunisia. [7]
b. The countries who have made amendments to the Criminal Code is Azerbaijan, the Netherlands, Byelorussian, Denmark, Estonia, Finland, Georgia, Germany, Hungary, Italy, Canada, Kazakhstan, Kyrgyzstan, Korea, Croatia, Latvia, Lithuania, Malta, Mexico, Norway, France , Peru, Poland, Russia, Tajikistan, Turkmenistan, New Zealand, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, Turkey, Ukraine, Uzbekistan, and Greece[8]
c. Countries that amend the Criminal Code simultaneously publish the Law especially set Cybercrime is the United States, China, (Computer Information Network and Internet Security, Protection And Management Regulation), Korea (Act on Promotion of Information and Comunications Network Utilization and Information Protection, etc; and Infratructure Information Protection Act), Malta (Computer Misuse 2001), and Nicaragua (Copyright Law of 1999)[9]

5 Barda Nawawi Arief, 2003, *kebijakan legislatif dalam penanggulangan kejahatan dengan pidana penjara*, Publisher Agency Diponegoro University, Semarang, P.201-202

6 Mahfud MD, in 2000, *Politik Hukum Nasional*, Alumni, Bandung, P. 35

7 http: www.cybercrimelawnet. accessed on 20 November 2016 23:40 GMT

8 *Ibid.*

9 *Ibid.*

Based on the exposure of the criminal law governing cybercrime can be summed up as follows;

a. In regulating Cybercrime, there are four alternative arrangements, namely (1) enforce the Criminal Code conventionally by expanding the understanding of certain terms through the interpretation of the law, (2) to amend the Criminal Code, (3) issuing regulations that specifically regulate related crime with the computer; and (4) to amend the Criminal Code at the same time issuing a special Act governing cybercrime.
b. State that the first set of cybercrime legislation in particular, and have at most legislation governing the world "cybercrime" (cyberlaw) is the United States. While the latter country issuing Special Act governing Cybercrime is Mauritius in 2003 (The Computer Misuse And Cybercrime Act 2003)

Criminalization in cyberspace by special arrangement outside the Criminal Code should be done carefully, not to create the impression which violates the principle of *Ultimum Remedium* (Ultima Ratio Principle) and backfired in the social life in the form of excessive criminalization (over-criminalization), which actually reduces authority of the law. Juridical comparative study was instrumental in conducting criminal offenses prevention policy information technology in the future.

The development of information technology crime resulted in every country have a policy of criminalization different. The emphasis on cross-country has made a crime on the internet is not just a national issue, but has become an International problem. This can be seen from the recommendations issued by the United Nations through a congress or also the Council of Europe.

Combating the crime of information technology into a problem in the countries of the world. The arrangement is also different in each country. Therefore, it needs study comparative law (comparative juridical) to determine how well the legal arrangements to forward the issue of criminal offenses related to information technology, especially the criminalization and regulation models.

1. United States of America

Widespread use of the Internet that is unmatched in the United States has led, and continues to cause various studies, policy proposals and draft legislation that regulate against the abuse of the use of technology's information. The United States has imposed a variety of laws that criminalize acts associated with the criminal offense of information technology.

Cybercrime settings in the United States, among others, the Computer Fraud and Abuse Act (Title 18 Part I Chapter 47 Section 1030 entitled "Fraud and related activity in connection with computers"), in the United States Congress in 1986 which aims to tackle the hacking to computers. The setting of the Computer Fraud and Abuse Act amended in 1994, 1996 and 2001. The forms of information technology criminal offense stipulated in Section 1030 are as follows:[10]

"whoever –

1. having knowingly accessed a computer without authorization or exceeding

10 http://blog.washingtonpost.com/securityfix/2008/07/senate_approves_bill_to_fight.html accessed on 2 November, 2016.

authorized access, and by means of such conduct having Obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted the data, as defined in paragraph y. Of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so Obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communication, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it,

2. *intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -*
   a. *information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair credit Reporting Act (15 USC 1681 et seq.);*
   b. *information from any department or agency of the United States; or*
   c. *information from any protected computer if the conduct Involved an interstate or foreign communication;*
3. *intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is EXCLUSIVELY for the use of the Government of the United States or, in the case of a computer not EXCLUSIVELY for such use, is used by or for the Government of the United States and such conduct that Affects use by or for the Government of the United States;*
4. *knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, UNLESS the object of the fraud and the thing Obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period;*
5. *a. knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
   b. intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
   c. intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;
6. *knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through the which a computer may be accessed without authorization, if -*
   a. such trafficking Affects interstate or foreign commerce; or
   b. such computer is used by or for the Government of the United States; " Or '

7. *with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; "*

The United States has set Concerning to "Internet Gambling", through the Federal Government to implement the Wire Act, the Travel Act, The Professional and Amateur Sports Protection Act and the Interstate Transportation of wagering Paraphernalia Act, attention is also directed at the issue of sexual immorality (obscenity) and adult entertainment and cyberporn, especially children pornography. In this regard may be mentioned the obscenity provisions of the Federal Law, the form "Transportation of Obscene Matters for Sale or Distribution" (18 USC Section 1465) and "Communications Decency Act of 1996".

Act in the United States governing the criminalization of acts related to information technology than those listed United States Congress also noted in some special rules, among others:

a. Prohibition Act of 1997 on Electronic Theft
b. Introduced to close a loophole in copyright law that does not recognize the US prior to copyright infringement if the defendant did not benefit.
c. *National Stolen Property Act* 1934 (Act national swag 1934) and the Economic Espionage Act of 1996 (Economic Espionage Act of 1996) prohibits the abuse of trade secrets.
d. *Identity Theft and Assumption deterrence Act of* 1998 (Act Identity Theft and Assumption Denial 1998)

2. Singapore

In Singapore, there is an interesting development of the information technology crime prevention policies. On the basis of the Computer Misuse Act (CMA) 1993 Act misuse Computer (Computer Misuse Act, CMA) Singapore 1993 modeled based on English Law in 1990, which ruled to 4 (four) things:

a. Unauthorized access;
   Article 3 of the Law prohibits the CMA containing 'hacking' which causes a computer plays a function for the purpose of securing unauthorized access to the program or any data stored on the computer.
   Article 3, paragraph 1 only aimed at unauthorized access.
   Article 3, paragraph 2 access to any resulting losses that exceed the value of 10,000 dollars will be subject to heavy penalties.
b. Access to the hidden intentions;
   Article 4 of the CMA Act criminalizes unauthorized access where there is a purpose to commit or facilitate acts of violations involving property, fraud, dishonest act, or acts that result in bodily injury.
c. Modification of the contents of the computer; and
   Article 5 of the CMA Act relating to the modification of the contents of the computer unauthorized and accidental such as data, computer software programs and databases for example by inserting a virus into the computer system.
d. Intercepting a computer service.
   Article 6 of the Law CMA introduces a new concept of the use of or unauthorized interception of computer services, it may be more

like a theft of service or computer use time.

In 1998 CMA experienced amendments, which through criminal weighting and the creation of new criminal offenses are trying to strengthen the protection of computer systems set up CMA 1993. The development of new forms of misuse of the Internet network resulted CMA Act requires expansion of coverage so that on 24 July 1998 Amendments to the passing of the Computer Misuse Act.

Amendment CMA 1998 which aims to strengthen the level and nature of the protection of computer systems that have been set by the previous law. Amendments to renew the CMA with five (5) ways:

a. Proposed a definition of damage as vandalism on a computer or the integrity or availability of data, programs or systems or information. Amendments to connect the crime by the level of damage caused, thus helping the overall objective to prosecute offenders commensurate with the damage they caused or the threat posed.
b. Penalties against various types of violations have been enhanced and apply to everyone. Thus, the initial fines for violations under Article 3, the existing maximum $ 5,000 for a first offense and double for a second offense or repeated condemnation; there is also a new prison sentence for an offense that is repeated in jail for 3 years. Likewise, the provisions of Article 5, paragraph 1 has been increased to a fine of $ 10,000 and / or three years in prison for a first offense, and the punishment a second time or recurring plus 20,000 dollars or imprisonment for 5 years.
c. The setting of the offense with ulterior motives under Article 4 and inclusion, based Sub Article 4 (a) new about the reference for someone who has the authority to access a computer but has preferred the authority to commit the same offense. In addition, the maximum penalty for all violations of the hidden and minimum penalties for offenses involving property, fraud, dishonesty and personal injury remains unchanged, despite the reorganization of the entire Article.

3. Netherlands

Netherlands establishing a committee called Franken commission tasked advise on setting cybercrime crime. The Commission considers cybercrime as ordinary crimes (ordinary crime) done with computer technology (high-tech) so that only enhance the Wetboek van Strafrecht (Criminal Code of the Netherlands) in 1993 to be used to combat the cybercrime (certainly with additions) with enter at certain criminal provisions. Franken Commissie cybercrime formulate some criminal acts in the formulation of Wetboek van Strafrecht, the formulation of the nine forms of abuse (misbruikvormen) are:

a. Without the right to enter a computer system;
b. Without the right to take (onderscheppen) computer data;
c. Without the right to know (kennisnemen);
d. Without the right to copy / copies;
e. Without the right to change;
f. Retrieving data;
g. Without the right to use the equipment;
h. Sabotage of computer systems;
i. Disrupted telecommunications

4. Myanmar

Myanmar made a policy on information technology since 20 September 1996 concerning the Development of Computer Science (Computer Development Law), which requires that the user-computer users in importing, possessing or using a computer must have a permit from the Ministry of Communications, Posts and Telegraphs. This law is specifically targeted at computers that are sending and receiving of data (that is utilizing the Internet). Article 34 of the Act specifically shows the sanctions given to people who do a job and distributed possess or transmit any information deemed confidential by the state that violates the political, legal and economic order as well as the national culture.

5. Philippines

At first the Philippines disregard of protection against the development of technology and information, but progress with the virus "I Love You" recognized issued by the student in the Philippines that lead to the dissemination of damage to the tissue around the world, who not only seized global attention but also urged action emergency by all countries. The case of the virus "I Love You" encourage the Philippine government issued a policy on June 12, 2000 by authorizing the E-Commerce. The Act contains a partial legal recognition of the authenticity of the messages and electronic documents, mostly in line with international trends. Hacking and cracking action is already contained in Section 33 (1) of the Act, identifying hacking and cracking which refers to the unauthorized access to or do annexation into a server / computer system or to the information and communication systems; or any access to reduce, alter, steal, or destroy using a computer or information and communication equipment are similar, without the knowledge and permission of the owner of the computer or information systems and communications, including inserting computer viruses and the like, which resulted in the reduction, destruction, alteration , theft or disappearance of electronic documents will be threatened with arrest and fines penalties.

C. CONCLUTION

Study of harmonization and synchronization with the material/substance criminalization of the act in the virtual world can not only be made to the convention or the law of other countries, but also the necessary input from experts in the field of cyber, because they are more aware of what conduct is and how it sees as a disadvantage or harm so it is worth being criminalized.

Through the study of comparative law (comparative judicial) criminal offenses against computer systems (against a computer system or network) is adjusted by the countries in the world are: illegal access, illegal interception, data interference, system interference. ITAC (Information Technology Association of Canada) on "International Information Industry Congress (IIIC) 2000 Millenium Congress" in Quebec on 19 September 2000 provides that: "Cybercrime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enable crime ".

BIBLIOGRAPHY

Books:

Ade Maman Suherman 2005, *Aspek Hukum Dalam Ekonomi Global*, Revised Edition, Ghalia Indonesia, Bogor.

Barda Nawawi Arief, 2003, *kebijakan legislatif dalam penanggulangan kejahatan dengan pidana penjara*, Publisher Agency Diponegoro University, Semarang.

Loebby Loqman 2002, *Kapita Selekta Tindak Pidana Di Bidang Perekonomian,* First Edition, Datacom, Jakarta.

Mahfud MD, in 2000, *Politik Hukum Nasional*, Alumni, Bandung.

Rachmat Rafiudin 2009, Internet Foeronsik, CV Andi Offset, Yogyakarta

Laksana, Andri Wijaya, and Suratman Suratman "Analisis Yuridis Penyidikan Tindak Pidana Pornografi Berdasarkan Undang-Undang Nomor 44 Tahun 2008 di Era Digitalisasi", *Jurnal pembaharuan hukum*, Volume I No. 2 Mei-Agustus 2014

Internet :

http://blog.washingtonpost.com/securityfix/2008/07/senate_approves_bill_to_fight.html

http: www.cybercrimelawnet.