Cybercrime Policies: Juridical Evidence and Law Enforcement Policies

Dwi Nurahman[1]
{dwinurahman_shmh@ymail.com[1]}

Law Faculty, University of Lampung, Bandar Lampung, Indonesia[1]

Abstract. This Study is oriented to know the legal aspects of Cybercrime Proving and law enforcement policies against cybercrime. This Study uses the method of Sociological Law Research (socio-legal research). The legal aspects of Cybercrime Proving have been firmly regulated in several laws and regulations in positive law in Indonesia, namely: Indonesian Criminal Procedure Code, Act Number 19 of 2016 concerning Amendments to Act Number 11 of 2008 concerning in Information and Electronic Transactions, Decision of the Constitutional Court Number 20/PUU-XIV/2016 and so on. Provisions regarding cybercrime are also regulated in international regulations namely the 2001 Convention on Cybercrime initiated by the European Union. The European Council Convention as the Protection of Human Rights in overcoming cybercrime, without reducing the opportunity for each individual to continue to develop their creativity in developing information technology. The policy of law enforcement against cybercrimes carried out with an approach that is both penal and non-penal. Seen from the perspective of criminal policy, cybercrime prevention efforts certainly cannot be done partially with criminal law (penal), but must also be taken with an integral/systemic approach or a preventative approach (non-penal).

Keywords: Cybercrime, Proof, Law Enforcement

1. Introduction

Advances in telecommunication technology have an impact on the universal life of society. The acceleration of information technology is increasingly rapidly encouraging continuous changes in the interaction and activities of the information society in the internet world.

The rapid development of information technology brings changes and movements in all aspects of life that are not limited. These technological means has stimulated rapid business growth because the various information provided through the network and transactions of the parties is sufficient through telecommunications equipment.[1] The development of information technology also creates a new world society that is no longer obstructed by territorial boundaries. However, these advances have also generated new concerns with sophisticated conversations in the form of cybercrime.

The current era of the development of a new legal order has given rise to cyber law or telematics law. Cyber law is internationally designated for laws relating to the regulation of the use of information and communication technology. Meanwhile, telematics law is a manifestation

ICETLAWBE 2020, September 26, Bandar Lampung, Indonesia

DOI 10.4108/eai.26-9-2020.2302579

of the convergence of reform of telecommunication law, media law and information technology law (information technology law), cyber law, and finally Mayan Tara law. National human activities have turned international. So it is only natural that cybercrime is included in the types of crimes that are international in nature based on the United Nations Convention Against Transnational Organized Crime (Palermo Convention) November 2000 and based on the ASEAN Declaration dated December 20, 1997, in Manila) which do not meet the provisions of the Indonesian criminal law system.[2]

Efforts to ensnare the perpetrators of Mayan Tara (cybercrime) must continue to be made, efforts to expand evidence become a solution for law enforcement. Proving Mayan Tara's crimes in the Indonesian criminal justice system has become an important topic, especially since the issuance of Law Number 11 of 2008 which currently has been amended by Act Number 19 of 2016 which governs Electronic Information and Transactions. The latest provisions of the law have accommodated evidence in the criminal justice process.[3] The evidentiary regulations must be based on the correct procedural law evidentiary systems and principles in Indonesia. It can be seen that Mayan Tara (cybercrime) knows no boundaries and timing of events because victims and perpetrators are often in various countries. All actions are carried out only from computers that have internet access without being noticed by other people/witnesses, so this crime is included as a transnational crime whose disclosure often involves law enforcement in more than one country.

Observing this matter, it can be agreed that cybercrime has a different character from general crime both in terms of the perpetrators, victims, modus operandi and the crime scene. Evidentiary systems in the current era of information technology face great challenges and need serious handling, especially in efforts to eradicate crime in cyberspace (cybercrime). To be able to conduct in-depth discussions on this issue it is necessary to conduct in-depth research to provide a clear picture in terms of proving *Mayan Tara* crime (cybercrime) both regulated in Indonesian criminal procedure law and the verification and study of the jurisdiction in the transnational sphere.

2. Literature Review and Hypothesis Development

In general, what is meant by computer crime or cybercrime is "efforts to enter and or use computer facilities or computer networks without permission and against the law with or without causing changes and or damage to computer facilities that are entered or used". many new types of crimes that are not only transnational but also manifest in virtual actions have made the international community aware of the need for new international legal instruments that can be used as international legal norms in dealing with cybercrime cases (crimes in the virtual world).

Crime in the information technology sector is a mode of crime through the internet network and its users. The nature of this crime could be of an international scale. This crime includes two categories, namely cyber crime in the sense of crimes against existing systems in computers, and cyber crimes in a broad sense, namely crimes against network systems and those using computer software media.[4]

Theory used in this study is the theory of law enforcement. The next hypothesis in scientific writing is this: the legal aspects of Cybercrime Proving have been firmly regulated in several laws and regulations in positive law in Indonesia, namely: Indonesian Criminal Procedure Code, and

Act Number 19 of 2016. Provisions regarding cybercrime are also regulated in international regulations (Convention on Cybercrime) namely the 2001 Convention on cybercrime initiated by the European Union. The policy of law enforcement against cybercrime is carried out with an approach that is both penal and non-penal.

3. Research Method

This paper uses the method of Sociological Law Research (socio-legal research). Sociological Law Research (sociologic research) is a research that focuses on the law as Norms (rules) and thus is positive legal research. This article also describes the reality in accordance with the legal facts that occur in detail and thoroughly, as well as collecting data from a natural setting by utilizing the researcher as a key instrument as a peeler of the problem to be studied.

4. Discussion and Analysis

4.1 Legal Aspects of Cybercrime Proving

An important substance regulated in Act Number 19 of 2016 is regarding the regulation of electronic transactions and concerning cybercrime. Material this regulation is an implementation of several principles of international provisions. Act Number 19 of 2016 contains prohibited acts in Article 27 to Article 36. Provisions of Article 42 also regulate the provisions of the investigation, namely: "the investigation referred to in this law is conducted based on the provisions in the Criminal Procedure Code and the provisions in this law".

Therefore, the system of evidence adopted is a system/theory of evidence based on the law in a negative manner, that is the system based on Article 183 of the Criminal Procedure Code, which states: "Judges must not impose a crime on someone unless with at least two legal pieces of evidence he gained the conviction that a crime had actually taken place and that the defendant was guilty of it". Thus, it means that the evidence must be based on the provisions of the law, namely the legal evidence set out in Article 184 of the Criminal Procedure Code, namely:[5]

1. Witness testimony

Formal requirements for witness statements set out in the Criminal Procedure Code, among others, are stated at court and an oath or appointment is taken before the witness gives a statement. Whereas the material requirements for witness testimonies include:

a) the information given is about the event that he heard, saw, and experienced himself by stating the reason for his knowledge;
b) not opinions, inventions or expert statements;
c) there is more than one witness following the principle of *unus testis nullus testis*;
d) not the information he obtained from other people (*testimonium de auditu*);

e) There is a match between one witness's testimony with another and one witness's information with other evidence.

In the case of cybercrime, due to its virtual nature, evidence using witness statements cannot be obtained directly. Witness statements can only be in the form of the results of conversations or only hear other people. This testimony is known as *testimonium de auditum* or hearsay evidence, although this kind of testimony is not used as evidence, in practice, it can still be used as consideration for the judge to strengthen his conviction before making a decision. The possibility that can be used as witness testimony is through the results of interactions in the cyber world, such as chatting and e-mail between internet users, or also through the information of a certified computer system administrator.

2. Expert statements

Description The expert is formally regulated as an expert in the field of science and his competence when asked to attend the trial. For example, such as computer scientists, network experts, software experts and other experts. The expert's statement becomes significant if the prosecutor submits electronic evidence to prove the culprit of cybercrime. The role of expert statements here is to provide an explanation in court that the electronic documents/data submitted are legal and can be legally accounted for.

3. Letter of evidence (Article 184 letter c and Article 187 of the Criminal Procedure Code)

Types of letters recognized based on evidence are letters issued by authorized officials, authentic letters, proof of payment, letters issued by agencies/agencies, letters of agreement that are attached to legal relationships, and so on with reference to Article 187 of the Criminal Procedure Code. "Letters" in the case of cybercrime have changed from their written form to unwritten and online. There are two categories of evidence in a computer that has been certified. First, if a computer system has been certified by an authorized body, then the results of the computer print-out can be trusted for authenticity. Example receipts issued by a bank in ATM transaction. This evidence has the power of proof, although further trials are needed in the trial. Secondly, proof of certification from the authorized body can be categorized as documentary evidence, because it was made by and or an authorized official. Other types of evidence can be in the form of electronic evidence. As long as both of this evidence are issued/made by the authorities in a computer network system and a computer network system can be trusted, then the letter has the same evidentiary power as the documentary evidence.

4. Others evidence (Article 184 (1) letter d and Article 188 of the Criminal Procedure Code)

The Criminal Procedure Code sets limits in terms of the source of instructions, namely that instructions can only be obtained from witness statements, letters, and statements of the accused. To be used as a source of guidance, all three pieces of evidence must be valid, and therefore, the instructions produced will also be valid.

In cybercrime, physical evidence collection is difficult to fulfill. The easiest way to gather evidence is to look for clues that indicate the existence of an evil intention in the form of unauthorized access. For example, by seeing and listening to witness testimony in court, or electronic mail or print out of data, or also from the defendant's statement in court.

5. Defendant's statement (Article 184 letter e and Article 189 of the Criminal Procedure Code)

The defendant's statement is what the defendant stated in court about the actions that he did or which he knew or experienced himself. For the defendant's statement to be declared valid, the formal requirements that are stated at the hearing and the material requirements of the information about the actions the defendant did or knew or experienced him must be fulfilled.

The provisions of Article 5 paragraphs (1) and (2) of Act Number 19 of 2016 describe that all electronic transactions are valid evidence. The provision in Article 44 states: “Evidence for investigation, prosecution and examination in court according to the provisions of this law are as follows:[6]

a. all the objects of evidence in this law;
b. form of evidence as regulated in Article 1 number 1 and number 4 as well as Article 5 paragraph (1), paragraph (2), and paragraph (3).

Electronic Information can be used as valid evidence according to the law on Information Technology and Electronic Transactions, although it is difficult to be classified as valid evidence as referred to in Article 184 paragraph (1) of the Indonesian Criminal Procedure Code. Electronic Information and/or Electronic Documents are declared valid if using Electronic Systems under the provisions stipulated in Act Number 19 of 2016.

Post Constitutional Court Decision Number 20/PUU-XIV/2016 related to Article about Article 5 of Act Number 19 of 2016 it is necessary to reorganize the position of electronic evidence and its acquisition procedures in the Indonesian criminal justice system. The Constitutional Court has stated the phrase "electronic information and/or electronic documents" in the above provisions contrary to the 1945 Constitution. The Constitutional Court then changes the phrase to "Specifically Electronic Information and/or electronic documents as evidence carried out in the context of law enforcement at the request of the police, prosecutors and / or other law enforcement institutions determined under the law as determined in Article 31 paragraph (3) Act Number 19 of 2016 concerning Amendment to Act Number 11 of 2008 concerning Information and Electronic Transactions [7]”

Provisions of Article 44 of Act Number 19 Year 2016 states evidence based on this Law is "other evidence in the form of Information Specifically Electronic and/or electronic documents as evidence are carried out in the context of law enforcement at the request of the police, prosecutors and/or other law enforcement institutions determined based on the law as determined in Article 31 paragraph (3) of Act Number 11 of 2008 concerning information and Electronic Transactions referred to in Article 1 number 1 and number 4 and Article 5 paragraph (1), paragraph (2) and paragraph (3).”

The Law Products of the Constitutional Court change status of electronic information and electronic documents in criminal law enforcement which consequently makes all electronic information / electronic documents that can become evidence must be obtained based on procedures in accordance with article 31 paragraph (3) of Act Number 19 the of 2016 concerning Amendments to Act Number 11 of 2008 concerning Information and Electronic Transactions, beyond that electronic information / electronic documents are not allowed as evidence.

4.2 Law Enforcement Policy against Cybercrime

1. Penal Approach

Judging from the criminal policy (crime prevention policy), criminal law is not a primary/strategic policy tool. A fundamental/strategic policy is to prevent and eliminate the causes or conditions that cause crime. Seen from the perspective of criminal policy, efforts to tackle crime (including combating cybercrime) certainly cannot be done partially with criminal law (a means of punishment), but must also be taken with an integral/systemic approach. As one form of high-tech crime, it is natural that cybercrime prevention efforts must also be pursued with technology (techno prevention). Besides that, a cultural/cultural, moral/educational, and even global (international cooperation) approach is needed because cybercrime can transcend national boundaries (transnational/trans-border nature).[8]

In an effort or policy to tackle cybercrime with criminal law, a workshop on "computer-related crimes" held at the UN Congress X in 2000 stated that member states should try to harmonize the provisions relating to criminalization, verification, and procedure. So the problem is not only how to make criminal law policies (criminalization policies, formulations, and legislation) in the field of dealing with cybercrime, but how there is harmonization of criminal policies in various countries. This means that the criminalization policy on the problem of cybercrime is not only a matter of national policy (Indonesia) but also related to regional and international policies.

Criminal politics is the policy of determining an event that is not a criminal act (not convicted) to become a criminal act (a punishable act). So, in essence, criminal politics is part of a criminal policy using penal law, therefore, it is part of a "criminal law policy".

2. Non-Penal Approach

The non-penal approach according to Hoe angels is the crime prevention approach without the use of punishment without prevention, which includes community planning mental health, national mental health, social worker and child welfare, and the use of civil and administrative law. The "non-penal" crime prevention policy is more a precautionary measure before the crime. The main orientation is to overcome various things that are conducive to the occurrence of a crime and focus on legal and social phenomena that can significantly cause or increase crime. studied from the aspect of crime prevention policy, non-criminal politics in a strategic situation and the main role that must be maximized.

Mayan Tara crime (cybercrime) requires global action in its response, considering that these crimes are often transnational in nature. Various policies and efforts in overcoming these crimes include:

a. Modernization of material criminal law and formal criminal law, which is elaborated with international regulations related to special crimes in the telecommunications sector.
b. National satellite security protection by referring to the provisions of applicable international standards.
c. Professionalism of expertise of law enforcement officers regarding the process of handling cases in the internet sector.
d. Increase public legal awareness.
e. Increasing cooperation between countries, be it bilateral, regional, and multilateral in the field of cybercrime.

f. Harmonization of the issue of jurisdiction to uphold state sovereignty which applies because it is transnational.[9]

5. Conclusion

1. The legal aspects of proving cybercrime have been firmly regulated in several laws and regulations in positive law in Indonesia, namely: Indonesian Criminal Procedure Code, Act Number 19 of 2016, Decision of the Constitutional Court Number 20/PUU-XIV/2016 and so on. Provisions regarding cybercrime are also regulated in international regulations namely the 2001 Convention on Cybercrime initiated by the European Union. The European Council Convention in overcoming cybercrime, without reducing the opportunity for each individual to continue to develop their creativity in developing information technology.
2. Law enforcement policies against cybercrime are carried out with a penal and non-penal approach. Penal can be in the form of criminalization to streamline positive laws related to cybercrime. Non-Penal, in the form of an approach to prevent the occurrence of *Mayan Tara* (cybercrime) crimes, such as increasing the knowledge of law enforcement officers about technology and information, increasing facilities and infrastructures in proving efforts, and increasing international cooperation.

References

[1] D. M. A. Mansur and E. Gultom, *Cyber Law - Legal Aspects of Information Technology*. Bandung: Refika Aditama, 2005.
[2] Widodo, *Mayantara Crime Law Aspects*. Yogyakarta: Aswaja Pressindo, 2013.
[3] T. R. R. Nitibaskara, *Perpetuation and Crime Trap*. Jakarta: YPKIK, 2009.
[4] S. Suseno, *Cyber Crime Jurisdiction*. Bandung: Refika Aditama, 2012.
[5] B. Suhariyanto, *Information Technology Crime (Cybercrime)*, vol. 74. Jakarta: Raja Grafindo, 2012.
[6] A. Wahid and M. Labib, *Crimes of Mayantara*. Bandung: Refika Aditama, 2005.
[7] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Comput. Secur.*, vol. 45, pp. 58–74, 2014.
[8] B. Nawawi Arief, *Mayantara Crime: Development of Cyber Crime in Indonesia*, vol. 62. Jakarta: Raja Grafindo, 2006.
[9] M. Mulyadi, *Criminal Policy, Integral Approach to Penal Policy and Non-Penal Policy in Combating Violent Crimes*, vol. 47. Medan: Pustaka Bangsa Press, 2008.