JLASA (Journal of Law and State Administration)
E-ISSN: 2986-4356 P-ISSN: 2986-4348
Volume 01, Number 01, March 2023 pp.7-11
https://www.mubtadiinpublishing.org/index.php/JLASA

Optimization of Cyber Law as A Legal Basis for Handling Cyber Crime in Indonesia

Marliyanti

Program Studi Ekonomi Syari'ah, STEBI Liwa, Lampung Barat, Lampung
* marliyanti.stebiliwa@gmail.com

Article

Keywords:
Information Technology; Internet; Crime; Cyber Crime Optimization; Cyber Law.

Article History
Received: Jan 11, 2023;
Reviewed: Feb 11, 2023;
Accepted: Mar 11, 2023;
Published: Mar 31, 2023

Abstract

Utilization of information and communication technology has changed the behavior of society and human civilization globally. The development of information and communication technology has led to rapid social, economic and cultural changes. In line with the development of internet technology which makes conveniences in the order of life but besides that it also causes the emergence of crimes that utilize the internet which are called cybercrimes or crimes through the internet network. Cyber Law becomes the legal basis in the law enforcement process against crimes by electronic and computer means, in other words, cyber law is needed to tackle cybercrime. By optimizing cyber law as a legal basis in cybercrime cases, it is expected that information and communication technology crimes can reduce the crime rate

INTRODUCTION

Utilization of information and communication technology has changed the behavior of society and human civilization globally. The development of information and communication technology has led to rapid social, economic and cultural changes. In line with the development of internet technology which makes conveniences in the order of life but besides that it also causes the emergence of crimes that utilize the internet which are called cybercrimes or crimes through the internet network. There have been several cases of cybercrime in Indonesia, such as credit card theft, hacking of several websites, tapping other people's data transmissions, such as e-mail, and manipulation of data by computer programmers. Cybercrime cases have increased from year to year with various modus operandi, in this case crimes via the internet network cannot be equated with conventional crimes which are subject to criminal or civil law witnesses. Crime using the internet is a form of cybercrime whose crimes cannot be proven without clear, firm and specific rules regarding these crimes so that cyber law was born in Indonesia. The term cyber law is defined as the equivalent of the word cyber law which is currently used internationally for legal terms relating to the use of

information technology. Other terms that are also used are Information Technology Law and Cyber Law. The term was born considering internet activity and the use of virtual-based information technology. The legal world has actually long expanded its interpretation of principles and norms when dealing with intangible issues, for example in the case of electricity theft which was initially difficult to categorize as a crime of theft but in the and it can be accepted as a crime. The current reality with regard to cyber activity is no longer that simple, bearing in mind that activities can no longer be limited by the territory of a country, access to them can be easily done from anywhere in the world, losses can occur to both internet actors and other people who have never had contact, for example in the theft of credit card funds through internet shopping.

In addition, the issue of proof is a very important factor, bearing in mind that electronic data is not only not yet accommodated in the Indonesian procedural law system, but in fact the data is also very vulnerable to being altered, intercepted, falsified and falsified. sent to various parts of the world in seconds. So that the resulting impact can be so fast. Information technology has become an effective instrument in global trade. Cyber activities, even though they are virtual, can be categorized as real legal actions and deeds. Juridically for cyberspace it is no longer appropriate to categorize something with conventional legal standards and qualifications to be used as objects and actions, because if this method is followed there will be too many difficulties and things that escape the law. Cyber activities are virtual activities that have a very real impact even though the evidence is electronic. This the subject of the perpetrator must also be qualified as a person who has actually committed a legal act.

METHOD

In this paper using 2 (two) approaches, namely normative juridical approach and empirical approach. The normative juridical approach is an approach by examining the rules or norms related to the problem to be discussed. This approach is intended to collect various laws and regulations, theories, and literature that are closely related to the issues to be discussed. While the empirical approach is by researching and collecting primary data obtained directly from the research object, which is related and closely related to the issues to be discussed.

DISCUSSION

Technological advances have brought about changes in all aspects of human life, now there are no barriers and geographical differences, time and distance between countries, access to trade runs smoothly and the dissemination of information runs fast and without boundaries. From all the positive things that are felt by the community with the advancement of technology, they are now starting to get worried due to the misuse of technological progress by committing harmful crimes. In the past, crimes were only conventional in nature which were carried out directly without using internet media such as threats, theft, reputation pollution, pornography, gambling, fraud to terrorism crimes now through internet media several types of crimes can be carried out online with individuals and groups with a very small risk of being caught with more many big losses for society as well as the State.

The phenomenon of information technology crime is a relatively new form of crime compared to other conventional forms of crime. Information technology crimes appear to coincide with the birth of the information technology revolution. Besides that, it is also characterized by social media interactions that minimize physical presence, which is another characteristic of the information technology revolution. Internet penetration if it is not used wisely by users will give rise to crimes in cyberspace or the like which are called cybercrimes. Cyber Law is needed, in relation to efforts to prevent criminal acts, as well as handling criminal acts. cyber The law will become the legal basis in the law enforcement process against crimes by electronic means and computers, including money laundering and terrorism crimes. In other words, Cyber Law is needed to tackle Cyber crime. Cyber Law is important to be enforced as law in Indonesia. This is caused by the development of time. According to those who are pro against Cyber Law, it is time for Indonesia to have Cyber Law, bearing in mind that traditional laws are unable to anticipate the rapid development of cyberspace. Cyber law is a new legal regime that covers various aspects of multidisciplinary law. Cyber law in Indonesian is often interpreted as telematics law.

Law enforcement in the form of transnational crime (cyber crime) in practice is influenced by legal factors which often become one of the obstacles to law enforcement which in practice is related to jurisdictional issues. This problem is that legal experts themselves admit that doubts about the determination of jurisdiction in cyber space. international in the conventional sense, based on geographic and time boundaries while multimedia communication and information are international, multi-jurisdictional and without geographic boundaries so that until now it has not been ascertained how the jurisdiction of a country can be applied to multimedia communication today as one of the utilization of technology information.

The existence of law regarding cybercrime has a close relationship with regard to the prevention and handling of cybercrimes that can appear in cyberspace (internet network). Cyber law is expected to become a legal basis for the law enforcement process against crimes committed using internet facilities, in this case including money laundering and terrorism cases. Cyber law really needs to be enforced in Indonesia. This can be proven by the increasing number of crimes committed via the internet by criminals. The scope of cyber law basically covers every aspect related to individuals or legal subjects who use and utilize internet technology starting from the time they go online and enter cyberspace or cyberspace.

The scope of cyber law is:

a. Copyright
b. Trademark rights
c. Slander
d. Slander, Blasphemy, and Humiliation (Hate Speech)
e. Attacks Against Computer Facilities (Hacking, Viruses, Illegal Access)
f. Internet Resource Settings such as Ip-Address and domain name (Internet Resource Regulations)
g. Individual Convenience (Privacy)

h. Precautionary Principles (Duty Care)
i. Common Crimes Using IT as a Tool (Criminal Liability)
j. Procedural Issues, such as jurisdiction, evidence, etc. (Procedural Issues: Jurisdiction, Investigation, Evidence, etc)
k. Contracts or Electronic Transactions and Digital Signatures (Electronic Contract and Electronic Signature)
l. Pornography
m. Internet Theft (Robbery)
n. Protection for consumers (Consumer Protection)
o. Use of the internet for everyday purposes, such as use for e-commerce, e-government , or e-education .

cyber law is narrowed down to the conditions that exist in Indonesia, then the scope of cyber law can be divided into two types based on their nature, namely:

1. In Public Law: Jurisdiction, Ethics of Online Activity, Consumer Protection, Antitrust, Fair Competition, Taxation, Regulatory Agencies, Data Protection and Cybercrime .
2. In Civil Law: Intellectual Property Rights (IPR), E-Commerce , Electronic Contracts, Domain Names, and Insurance.

Even though cyber law enforcement in Indonesia has not been specifically regulated, several existing laws and regulations already have rules regarding the regulation of handling cyber crimes. Like the Electronic Information and Transaction Law, this Law regulates the handling of defamation, hate speech, uploading illegal content, and other cyber crimes related to interference, such as interference with electronic data and information and interference. to an electronic system. In a broad sense, conventional crimes committed through online media can also be applied to provisions in the Criminal Code (KUHP), such as cases of trafficking in persons committed via the internet. In addition, Law Number 3 of 2011 concerning Transfers of Funds and Banking Crimes and Money Laundering Crimes in Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes (UU TPPU) can also be enforced.

Cyber law, namely the law that limits cybercrime (cybercrime through the internet network). Cyber law is needed on the basis of law in various countries, namely "space and time". Meanwhile, computer networks and the internet have broken the boundaries of space and time. Although the evidence is virtual and electronic, cyber activity is virtual activity with real impact. Cyberlaw is not a necessity, but a necessity to face the reality that exists today, namely the existence of crime on the internet or what is called cybercrime. Cyber Law is urgently needed, related to efforts to prevent criminal acts, as well as handling criminal acts. Cyber Law will become the legal basis in the law enforcement process against crimes through electronic means and computers, including money laundering and terrorism. In other words, Cyber Law is needed to overcome cybercrimes.

CONCLUSION

The more Technology The more information the impact is positive and negative. The positive side of cyberspace is of course adding to the trend of world technological development with all forms of male creativity. In addition to the negative impact, it can cause crimes called *cyber*crimes or crimes through the Internet network. The increasing number of related crimes based on the use of computer and telecommunications network technology is increasingly making Internet network users nervous about information system security policies, the most important of which is the order of national law in the form of Cyber *Law*. With strict cyber laws in the international world, it might be possible to reduce the number of crimes in cyberspace.

REFERENCES

Golos PR., "Cybercrime Law Enforcement in the Indonesian Legal System in Seminars on Evidence and Handling of Cybercrime in Indonesia". 2007.

Makarim, Edmon. *Introduction to the Laws of Telematics* . Jakarta: RajaGrafindo Persada, 2007.

Napitupulu, Darmawan. "Study of the Role of Cyber Law in Strengthening National Information System Security". *Deviance Journal of Criminology Vol.1, No.1.* 2017. Pg. 100-113.

Raharjo, Agus. *Cybercrime, Understanding, and Technological Prevention Efforts.* Bandung: PT. Citra Aditya Bakti, 2002.

Tantawi, Dahlan Ali, Suhami. "Protection of Victims of Cyber Crime in the Indonesian Criminal Law System". *Journal of Postgraduate Law Studies at Shia Kumala University, Volume 2, No. 1, February 2014* . 2014. Pg. 32-40.