OPEN ACCESS
Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Adoption of the Law on Information and Electronic Transactions against Cyber Crime

Aulia[1*]

[1]Lecturer of Faculty of Law, Pekalongan University, Indonesia

DOI: 10.36348/sijlcj.2023.v06i03.001 | **Received:** 17.05.2021 | **Accepted:** 20.06.2021 | **Published:** 09.03.2023

***Corresponding author:** Aulia
Lecturer of Faculty of Law, Pekalongan University, Indonesia

Abstract

The development of computer technology and the internet provide implications-the implications are significant in the settings and the establishment of regulations in cyber space and cyber laws as well as to the development of crime in cyberspace or often referred to as cybercrimes. Of the various things that need to be emphasized that the internet was not initially designed for tracking and tracinguser behavior, but it is designed for the needs of the military in the face of war the world at that time. Normatively, with the establishment of Law Number 11 Year 2008 On Information and Electronic Transactions as new rules that apply, and all the population is considered to have been knowing. Adoption of the Law on Information and electronic transactions against cybercrime. In the era of industrial Revolution 4.0 is the current utilization of the technology, the more massive the better government agencies, private companies, national banking, center for research and society. Sociological research empirical, then studied at first is secondary data, to then proceeds with the research on primary data lapangam or to the community. The author will give an overview first the definition and the classification of crime is cybercrime, the perpetrators and victims of form and modus operandi as well as how the public reacts to kejehatan cybercrime such. Cybercrime is a criminal activity in the virtual world with a network utilizing the computer as a tool and a network of the internet as a medium. In a broader sense, cybercrime is all the illegal actions committed through a computer network and the internet to get advantage by harming the other party. Then in the narrow sense, cybercrime are all illegal actions that are intended to attack computer security systems and the data processed by a computer system.

Keywords: Application, The Information And Electronic Transaction Law, Cyber Crime.

I. INTRODUCTION

The sophistication of the technology at the time are now attracting many people to use it because it is considered simplify and ease the work. We know that the sophistication of the technology affect the attitude and mental state of the individual communities, so people will be dependent on the equipment or the technology of a virtual world. The nation of Indonesia, though lagging behind the technology with other developed countries but in the era of industrial Revolution 4.0 is the current utilization of the technology, the more massive the better government agencies, private companies, national banking, research centers and the wider community.

In the world of information technology or the digital world can be a deviation occurs or abuse and the term is often called Cyber Crime. Cybercrime is derived from the word that means the virtual world or the internet and crime means a crime. In other words, cybercrime is any crime that happens in the virtual world or the internet. Cybercrime or crime in the virtual world itself is one of the deeds or actions of the negative world of the internet as a platform that is currently widely used in society circles both groups, young and old both women and men.

Cybercrime is a criminal activity in the virtual world with a network utilizing the computer as a tool and a network of the internet as a medium. While nature is the broadest sense, cybercrime is all the illegal actions committed through a computer network and the internet to get advantage by harming the other party. Then in the narrow sense, cybercrime are all illegal actions that are intended to attack computer security systems and the data processed by a computer system.

Volodymyr Golubev call it a crime cybercrime this in various posts, among others, as cyber space I virtual space offence, a new dimension of high tech

crime, a new dimension of transnational crime, and a new dimension of white collar crime [1].

According to *Organization of European Community Development* (OECD) *cybercrime* is all forms of illegal access to a data transmission. That means, all forms of unauthorized activities in a computer system including a crime [2].

In general, the notion of cybercrime itself is defined as a crime in the realm of the virtual world that utilizes computer technology and the internet as the main target. As has been mentioned, the act of cybercrime is often incessant digital technology, communication and information more and more in use by the wider community.

Efforts to bring a legal instrument in accordance with the development of the world information technology and telecommunications into something that is not negotiable, given the need to include legal efforts to prevent and provide a deterrent penalties for the perpetrators of cybercrime. Developments in the field of technology to change the world's relationship seems to be without limits (borderless) associated with cultural, social and economic dynamic unfolding so quickly. Information technology is not only able to increase the progress of development, welfare and civilization, but also can cause negative changes that are not in accordance with the rule of law already in force [3].

It still remains one issue that originate in the fact that the legislation does not know on the issue of the development of the technique. A challenge for the experts of the law is not aimed at the deepening of technical tools. They do not have to explore the tools that help and indeed the more necessary is the material related to (criminal) legal experts should focus more attention on the issue of actions that should be given to confront the evil growing in this digital era. So the law has to face the crime cybercrime is almost all the cases the law should have sense along with the development of science and technology.

II. RESEARCH METHODS

In this study, the authors will provide an overview first the definition and the classification of crime is cybercrime, the perpetrators and victims of form and modus operandi as well as how the public reacts to kejehatan cybercrime such. Will then be given an analysis in depth of the adoption of the law the Law the Information and electronic transactions as that really apply to an act of law and as the law that should be applied by the court to cases of crimes that occur.

This study intended to explore in depth of the steps that can be done to prevent cases of cybercrime in Addition, through this research is expected to be derived by an appropriate recommendations and accurate in tackling crime in the field of cybercrime is increasingly rampant today in line with the development of information and communication technology so rapidly.

III. RESULTS AND DISCUSSION

1. The Circumstance of Serious against Crime Cyber Crime in Indonesia

Action crime cybercrime application of articles of the Law on Information and electronic transaction against crime cybercrime. To analyze the theme of the subject in this study as follows: First, regarding the overview toward the crime cybercrime some of the things at issue is whether the definition and kalisfikasi crime cybercrime, how does the shape of the form and modus operandi, who the perpetrators and victims as well as how the public reaction to the crime. Second, regarding the settings and the application of the criminal law the Law the Information and electronic transactions. Things in mind about is how the adoption of the Law on Information and electronic transactions against crime cybercrime.

Information technology holds an important role, both in the present and in the future. Information technology is believed to bring profit and the interests of the large countries in the world. There are at least two ha1 that make information technology is considered so important in spurring the growth of the world economy. "According to Agus Raharjo that information technology is boosting demand for information technology products itself, such as a computer, a modem, a means to build a network of internet and so on. Second, is to facilitate business transactions, especially financial business in addition to business-general business other [4].

Crime and criminal computer can be defined as follows: [5]

1) Broad Definition: crimes and criminal a computer is a crime and criminal acts committed by the perpetrator against computer as a target with or without the use of the computer as a tool or using the computer as a tool against any target.

[1] Barda Nawawi Arief, Criminal Mayantara, the Development of the Study of Cyber Crime in Indonesia, Raja Grafindo Persada, Jakarta, 2007, pp.. 1

[2] https://qwords.com/blog/pengertian-cyber-crime/ Accessed on June 16, 2021. Hours. 9.45 PM

[3] Maskun, Cyber Crime, An Introduction, Kencana, Jakarta, 2013, pp. 29

[4] Agus Raharjo, Cyber Crime, Understanding dun Crime Prevention Efforts Tech,ctk. First, Citra Aditya Bakti, Bandung, 2002, pp.. 1

[5] Sutan Remy Syahdeini, Crime and Criminal Computer, Jakarta, Purtaka Utama Grafiti, 2009 , pp. 43

2) The Definition of narrow: crime and criminal a computer is a crime and criminal acts committed by the culprit using the computer as a tool against any target.

Currently, Indonesia has a Law that specifically governs cybercrime, but there are some positive law other applicable general and can be worn for the perpetrators of cybercrime especially for the cases of using the computer as a means of crime is Cyber Crime for an explanation as following:

a. The Definition Of The Concept Of Crime

The term Crime is more appropriate if our analysis of the approach of criminology. This approach is the presence of a strong relationship between crime and criminality with science criminologist. Criminology found by paul topinard, in the year 1830 s.d. 1911.

b. Classification Cyber Crime

1) **Theft Data:** Cybercrime activities this one is usually done to meet the interests of the commercial because there are others who want the confidential data of the other party.
2) **Cyber Terorism:** Cyber terrorism is an act of cybercrime which was much fought by the major countries in the world, including Indonesia.
3) **Hacking:** Types of cybercrime next is Hacking. Malicious acts are often done by the programmer professional is usually specifically targeting the weaknesses or loopholes of the security system to get an advantage in the form of material or personal satisfaction.
4) **Carding:** Carding is a term used to refer to the abuse of credit card information belonging to others.

A wide variety of shapes or variants are very detrimental to the life of the community or the interests of a nation and State in international relations. The form and modus operandi of Cyber Crime including:

1) **Theft Data:** This action of course is illegal entry into the criminal activities because it can cause loss of material resulting in the bankruptcy of an institution or company.
2) **Cyber Terorism:** The activity of cyber terrorism often threaten the safety of the citizens of the country or even stakeholders who organized the running of the government.
3) **Hacking:** If the view of the activities carried out, hacking actually does not always have a negative connotation because there is also a hacker positive that uses his abilities for the activities of beneficial and not detrimental.

For example, a hacker who was given the task to track the whereabouts of a fugitive or a hacker who cooperate with the authorities to combat illegal activities in the digital realm.

The deeds that contained in Article 167, paragraph (1) and (2) of the criminal code, arise various questions if it is associated with the act of hacking. The question is; what a computer system a person's or an organization, or website in computer networks (the internet) can be categorized as object set forth in Article 167 of the criminal code? In other words, whether it can be equated enter the computer systems of others by entering into a yard or other people's homes? Whether the intercepted passwords can be equated with the use of false lock as set forth in the article? To answer the question then the judge should perform the interpretation of the deep, that its use in criminal law still raises debate.

4) **Carding:** The carder (pelaku carding) usually use access cartu credit other people to buy groceries online. Then, the goods igratisan such re-sale with cheap price to get money.

Crime digital how to carding usually often occur in a foreign country, while for users in Indonesia the number of cases recorded is not too big due to lack of credit card users who are fond of transacting in the virtual world.

2. The cause of the difficulty of the Completion of the Legal Protection of Victims of Crime cyber crime

As of this article is about the crime cybercrime application of articles of the Law on Information and electronic transaction against crime cybercrime. the settings and the application of criminal law. Normative juridical see how the principles of law and the synchronization of applicable law on the legal protection of a victim of cybercrime in Indonesia. The approach used is a conceptual approach (conceptual approach), the approach of legislation (normative approach), and the approach of the case law (case law approach). In this case concerning the legal protection of victims of crime cybercrime in Indonesia. The settings and the application of the criminal law Act-Information and electronic transaction law against crime Cyber Crime:

a) Phising

Phishing is a method to commit fraud to trick the target with the intent to steal the target account. The term is derived from the word “fishing” = “fishing” the victim to get caught up in the trap. Phishing can be said to steal the important information to take over the account of the victim for a particular purpose.

And who do Phishing will be charged:

1. Article 27 of the Law on Information and electronic transaction of the year 2008: Any person who knowingly and without the right to distribute and/or transmit and/or make accessible electronic information and/or electronic documents that have the charge of a violation of decency. The threat of criminal

article 45(1) of the criminal code. A maximum imprisonment of 6 (six) years and/or a fine of Rp1.000.000.000.00 (one billion rupiah). Also regulated in the criminal code article 282mengenai crimes against decency.

2. Article 28 of the Law on Information and electronic transaction of the year 2008 : Any person who knowingly and without the right to disseminate false news and misleading which resulted in the loss of consumers in electronic transactions.
3. Article 29 of the Law on Information and electronic transaction of the year 2008 : Any person who knowingly and without the right to transmit electronic information and/or electronic document that contains threats of violence or scare addressed personally (Cyber-Stalking). The threat of criminal article 45 (3) Any person who meets the elements referred to in article 29 shall be punished by a maximum imprisonment of twelve (12) years and/or a fine of not more Rp2.000.000.000, 00 (two billion rupiah).

b) Carding

Carding is the shop using the number and identity of other people's credit cards, which are obtained illegally, usually by stealing data on the internet. The title of the culprit is a Carder. Another name for the crime of this type is cyberfroud aka deception in the virtual world. This way you can shop for goods in the online shop free of charge, but it could be reported by the owner of the credit card and will be imprisoned. And who do Carding will be charged:

1. Article 31, paragraph 1: Any person who knowingly and without authority or unlawfully intercepting or eavesdropping on information electrical and / or electronic documents in a computer and / or electronic systems in specific property of others.
2. Article 31, paragraph 2: Any person who knowingly or without the right or unlawful interception or transmission elktronik and / or electronic documents that are not publikdari, to, and within a computer and / or electronic systems belonging to other people, both of which do not lead to changes, omissions, and or termination of electronic information and / or electronic documents transmitted.

c) Deface

Deface is a technique to replace or insert a file on the server. This technique can be done because there is a hole on the system security in an application. It aims to change the display on the website of the victims with the appearance of which is owned by si defacer. Deface also a criminal act because knowingly you do changes on the web someone without permission. And the actors Deface will be subject to the Information and electronic transaction law about the defacer. In the Law on Information and electronic transaction discuss the issue of hacking is mainly about access to someone else's computer without permission. It is regulated in article 30 and article 46 of the punishment that will be received. The following is the content of the article:

Article 30

1. Any person who knowingly and without authority or unlawfully accessing a Computer and/or Electronic Systems belonging to other People in any way.
2. Any person who knowingly and without authority or unlawfully accessing a Computer and/or Electronic Systems in any way with the aim to obtain Electronic Information and/or Electronic Documents.
3. Any person who knowingly and without authority or unlawfully accessing a Computer and/or Electronic Systems in any way to violate, break through, beyond, or hacking into security systems (cracking, hacking, illegal access).

Article 46

1. Any person who meets the elements referred to in Article 30 paragraph (1) shall be punished by a maximum imprisonment of 6 (six) years and/or a fine of at most 600.000.000, 00 (six hundred million rupiah).
2. Any person who meets the elements referred to in Article 30 paragraph (2) shall be punished with imprisonment of 7 (seven) years and/or a fine of at most 700.000.000, 00 (seven hundred million dollars).
3. Any Person who meets the elements referred to in Article 30 paragraph (3) shall be punished by a maximum imprisonment of 8 (eight) years and/or a fine of at most Rp.800.000.000, 00 (eight hundred million rupiah).

d) Bruteforce, Exploiting, The Spread of Malware and Techniques Ilegal Gaining Access Other

Bruteforce is the engineering hacking hacked account, login, system, and lain2 by using the method of matching a sentence from the list wordlist that belongs to the hacker to get access forcibly.

Exploiting is a hacking technique using a loophole / bug in the system the better it Operating System, Web Application, Desktop Application, dan Mobile Application to break through and gain access in the system forcibly.

Malware is a malicious program that is used to damage the system, data theft, and to the action of tapping.

These kinds of Malware are as follows RAT is a Remote Administration Trojan is a malicious program to perform the activity of tapping the

keyboard/keylogger, tapping the webcam, and even a RAT is able to perform the activity data theft and take over control of the system is infected by her. Virus is a malicious program to damage the computer Worm worm is a type of one of the variants of the virus just this worm spread to the entire directory of sensitive systems and can spread quickly if not handled directly by the sysadmin and antivirus and other application programs. Ransomware is a malicious program that is holding the data of the victim if the person is exposed to ransomware then his data will be encrypted and that victims must pay to the diffuser ransomware to be the public key to unlock the encryption.

A Backdoor is a program access management that belongs to the hacker if a hacker already successfully entered into the system then he's going to plant a backdoor to control access, the system, and even the hacker can configure the system that was hacked by him as if like a Sys Admin or the owner of the system.

A Botnet is a robot internet or a malicious program that is her nature to make the system of the victim becomes a part of the military forces of the hacker's botnet is most often used hackers is DDOS (a Distributed Denial of Service) is by way of infecting as many devices computer system and make her as a tool to attack the other party.

Sanctions for perpetrators in Article 30 of the LAW the Law the Information and electronic transactions. The chapter contains three variants of the offense that makes the hacker may be subject to criminal law, i.e. intentionally and without right:

a. Access a computer or electronic system,
b. Access a computer or electronic system with the aim to obtain electronic information,
c. Beyond, to break, to violate, the security system from a computer or electronic system to be able to access a computer or electronic systems.

The threat to the violation of Article 30 of the Law on Information and electronic transaction is a maximum imprisonment of 8 years and/or a fine of at most Rp 800 million according to the stipulated in Article 51 paragraph 1 of the Law on Information and electronic transaction. The provisions of the investigation in the Information and electronic transaction law and its amendments shall also apply to criminal investigations of cyber in the broadest sense. For example, in a criminal tax, before a search warrant or seizure to the bank server, the investigator should pay attention to the smooth running of public services, and protect the interests of maintaining public services as set out in the Information and electronic transaction law and its amendments. If by turning off the server bank will interfere with public services, such actions should not be performed.

As for the procedure for demanding in the criminal proceedings against the deeds of the criminal cyber, can be simply described as the following: [6]

1. Victims who feel their rights are violated or through the power of the law, came instantly create a report of the incident to the POLICE investigator on the unit/section Cybercrime or to the investigator PPNS on the Sub-Directorate for Investigation and Prosecution, the Ministry of Communication and Information technology. Furthermore, the investigator will conduct an investigation can proceed with the investigation process over the case concerned the Law of Criminal procedure and the provisions of the Law on Information and electronic transaction.
2. After the investigation process is complete, then the case file by the investigator will be delegated to the attorney general to do the prosecution in advance of the court. If the conduct of the investigation is PPNS, then the results of the investigation submitted to the public prosecutor through a POLICE investigator.

In addition to the Information and electronic transaction law, regulation that became a cornerstone in the handling of cases of cybercrime in Indonesia is the regulation implementing the Law on Information and electronic transaction and also the technical regulations in the investigation in each agency investigator.

Should we use the internet and the science of IT wisely, don't get hooked to that last because it could be that you would not be able to use the internet for many years. According to the Strecher (1971: Be 59-66) law Enforcement is not something that can be seen as a stand-alone, but always exchange activities with the community that served him, or by citing Parsons we refer to as relational. Thus may, if accepted, that the changes in society caused by the use of modern technology, especially in the form of coverage in the speed and power damage, will provide its influence themselves against law enforcement in the community. Especially in the relationship with the work of law enforcement in this case, many centered on the work of the police. In addition, to prevent the onset of cyber crime is also required equipment forensic computing appropriate to evidence the crime and ha1 is no less important again need to also prepared a Police investigator to be educated and able to investigate cyber crime and cooperation with law enforcement who are outside the country.

6 https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia/ Accessed on June 8, 2021' Hours. 19.35 AM

IV. CONCLUSION

The law on Information and Electronic Transaction in Indonesia has the potential to be effective, because it is supported by people who tend to always use the technology of electronic information as a basic need in addressing the development of the modern times. However there some barriers which is said to interfere with the effectiveness of Laws Information and Electronic Transactions in Indonesia, among others, first, in the effectiveness of regulation of the absence of the settings against the criminal acts of fraud using a computer, the second, in the effectiveness of the purpose of the legislation is said to have not been able to achieve the goals that are loaded in it, need to do some revamping the system in the life of society as the subject of law and as a user of the means of technology of electronic information. The completion of the cybercrime earliest use how persuasive, then harmful, improving the quality of law enforcement in the settlement of case, make the law as a basis for any action that created the existence of equality before the law and the rule of law.

By knowing the above information hopefully we can be more vigilant so that the crimes that occurred in the virtual world this does not happen to You until whenever and wherever.

REFRENCES

- Agus Raharjo, Cyber Crime, Understanding dun Crime Prevention Efforts Tech,ctk. First, Citra Aditya Bakti, Bandung, 2002.
- Barda Nawawi Arief, Criminal Mayantara, the Development of the Study of Cyber Crime in Indonesia, Raja Grafindo Persada, Jakarta, 2007
- https://qwords.com/blog/pengertian-cyber-crime/ Accessed on June 16, 2021. Hours. 9.45 PM.
- https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia/ Accessed on June 8, 2021' Hours. 19.35 AM
- Maskun, Cyber Crime, An Introduction, Kencana, Jakarta, 2013
- Satjipto Rahardjo, Makalah Penegakan Hukum Suatu Tinjauan Sosiologis; Penerbit Sinar Baru, Bandung; 1983.
- Sutan Remy Syahdeini, Crime and Criminal Computer, Jakarta, Purtaka Utama Grafiti, 2009.