Legality of Indonesia Government’s Action in Blocking Telegram Application Due to Cyberterrorism Activities

By
HANI NUANZA UEMENINA
017201300010

A thesis presented to the Faculty of Humanities President University in partial Fulfillment of the requirements of Bachelor Degree in Law
2018
THESIS ADVISOR RECOMMENDATION LETTER

This thesis entitled “LEGALITY OF INDONESIAN GOVERNMENT’S ACTION IN BLOCKING TELEGRAM APPLICATION DUE TO CYBERTERRORISM ACTIVITIES” prepared and submitted by Hani Nuanza Uemenina in partial fulfillment of requirements for the degree of Bachelor of Law in the Faculty of Humanities has been reviewed and found to have satisfied the requirements for a thesis fit to be examined. We therefore recommend this thesis for Oral Defense.

Cikarang, Indonesia, April 4th, 2018

Sujana Donandi Sinuraya, S.H.,M.H
Advisor I

Zenny Rezania Dewantary, S.H., M.Hum
Advisor II
DECLARATION OF ORIGINALITY

I declare that this paper, entitle “Legality of Indonesia Government’s Action in Blocking Telegram Application Due to Cyber Terrorism Activities” is, to the best of my knowledge and belief, an original piece of work that has not been submitted either in whole or in part, to another university to obtain degree.

Cikarang, Indonesia, April 4th, 2018

Hani Nuanza Uemenina
PANEL OF EXAMINER APPROVAL SHEET

The panel of examiners declares that the thesis entitled “Legality of Indonesia Government’s Action in Blocking Telegram Application Due to Cyberterrorism Activities” that was submitted by Hani Nuanza Uemenina majoring in Law from the Faculty of Humanities was assessed and approved to have passed the Oral Examination on Cikarang, Indonesia, April 2nd, 2018.

Mr. Gratianus Prikasetya Putra, S.H., M.H.
(Chair - Panel of Examiner)

Mr. Sujana Donandi Sinuraya, S.H., M.H.
(Examiner I)

Ms. Zenny Rezania Dewantary, S.H., M.H
(Examiner II)
ABSTRACT

The crime regarding Telegram application accommodate cybercrime was one of the important issues in legal field. The legality related the blocking process of Telegram application by the government must be considered as one of the methods for preventing terrorist activities.

The method for this research is Normative, it is selected because of norm analyzing regarding to telecommunication technology and use telecommunication properly and correctly without any Radicalism of Processing Procedures and Analysis of Law Material. Using qualitative descriptive, will not only reveal the truth, but also to provide an understanding of the truth about the rules which governs Terrorism, Telecommunications, and Information Technology.

The result of this research found that: firstly, the Indonesia government considers it necessary to block telegram because in this application there is content that contains elements of Radicalism; secondly, telegram has paved the way for crimes related terrorism.

Keywords: Telecommunication, Cyberterrorism, Cybercrime, and Telegram
ABSTRACT

Kejahatan mengenai aplikasi Telegram mengakomodasi cybercrime adalah salah satu isu penting di bidang hukum. Legalitas yang terkait dengan pemblokiran aplikasi Telegram oleh pemerintah harus dipertimbangkan sebagai salah satu metode untuk mencegah kegiatan teroris.

Metode untuk penelitian ini adalah normative, hal ini dipilih karena analisis norma mengenai teknologi telekomunikasi dan menggunakan telekomunikasi dengan baik dan benar tanpa Prosedur Pengolahan dan Analisis Bahan Hukum dengan menggunakan deskriptif kualitatif, tidak hanya akan mengungkapkan kebenaran, tetapi juga memberikan pemahaman tentang kebenaran tentang aturan yang mengatur Terorisme, Telekomunikasi, dan Teknologi Informasi.

Hasil dari penelitian ini menemukan bahwa: pertama, pemerintah Indonesia menganggap perlu untuk memblokir telegram karena dalam aplikasi ini terdapat konten yang mengandung unsur-unsur Radikalisme, kedua, telegram telah membuka jalan bagi kejahatan terkait terorisme.

Kata Kunci: Telekomunikasi, cyber Terrorism, Cybercrime, dan Telegram
ACKNOWLEDGEMENT

Gratitude for the presence of Jesus Christ for His blessing, guidance, and who always giving me the courage and strengths in countering all obstacles, including in completing this entitled entitled “LEGALITY OF INDONESIAN GOVERNMENT’S ACTION IN BLOCKING TELEGRAM APPLICATION DUE TO CYBERTERRORISM ACTIVITIES”, as one of the conditions that should be fulfilled to complete this studies and obtain a Bachelor’s degree of Law.

There are many wonderful people who always support me and remind me to study and finish my bachelor degree. Through this part, I would like to express my humble appreciation, as follows:

1. Mrs. Dra. Fennieka Kristianto, S.H., M.H, MKn as head of study program of Law STUDY Program
2. Mr. Sujana Donadi Sinuraya S.H., M.H as my advisor 1 that has teaching me and helping me to write this study. Thank you for the knowledge which given and hopefully useful for me.
3. Mrs. Zenny Rezania Dewantary, S.H., M.Hum, as my advisor 2 that has teaching me and helping me to write this study. Thank you for the knowledge which given and hopefully useful for me.
4. My lovely family: my beloved father and mother thanks for your love for me, support me, and provide me advise whenever I needed especially in writing this thesis.
6. Florens Bertha Elirosa Ginting whom always pray for me and support me as my best cousin so the process of writing this thesis trial smoothly and there are not obstacles.
7. Thank You for my Bestfriends there out university life : Yosua Sihotang, Antonius Yoga, Putra Tarigan, Tristan Ginting, Martin Sembiring Kembaren, Kelly Tjiauw,
Fenando Ginting, Tannia Barus, Agung Prananta Tarigan, Ekin Sebayang, Theo Tarigan, Jeheskiel Bastanta Tarigan, and Feby Rosaphin Tarigan for supporting me, advising me, listening since my internship life until I already writing this thesis.

8. Thank You for My special Budi Utomo Purba for supporting me, advising me, listening since my internship life until I already writing this thesis.

9. Thank you for my bestfriend in university life: Chikita Sianipar, Rosima Rajagukguk, Alichia Diasuma Tarigan, Leonardo Rakinaung, Riski Darsani, Devina Hia, and Romi Saragih who had supporting me, and Edy Kalme Haganta Sinulingga laughing, and never stop to remind me to finish this thesis.

10. Thank you for all friends of mine in Church “Permata GBKP of Center Jakarta” for the prays.

11. Agustinus Ginting for advising me to not to be lazy for writing this thesis everyday so I can finish this on time.

12. To all President University’s Lecturers and my university friend, thank you for being one of my part of life. President University, the people which I met and the lesson were taught.

   Finally, thank you for all people which I can not mention one by one, but for all the contribution in helping me to write this thesis, for the support and pray which important for me. Thank you very much.

Cikarang, Indonesia, April 4th, 2018

Hani Nuanza Uemenina
# TABLE OF CONTENTS

- THESIS ADVISOR RECOMMENDATION LETTER ................................. i
- DECLARATION OF ORIGINALITY ............................................. ii
- PANEL OF EXAMINER APPROVAL SHEET ................................ iii
- ABSTRACT ........................................................................ iv
- ABSTRACT ........................................................................ v
- ACKNOWLEDGEMENT ........................................................... vi
- CHAPTER 1 ........................................................................... 1
  - Introduction ........................................................................ 1
  - 1.2 Problem Identification .................................................... 8
  - 1.4 Benefits of Research ....................................................... 9
  - 1.5 Research Method .......................................................... 9
  - 1.6 Research Framework .................................................... 11
- CHAPTER 2 ........................................................................... 12
  - Theoretical and Legal Aspects of Information Technology and Application Blocking by the Government ......................................................... 12
  - 2.1 Legal Provisions on Cyberterrorism and Telecommunications in Indonesia ................................................................. 12
  - 2.2 Definitions ..................................................................... 13
    - 2.2.1 Crime ....................................................................... 13
    - 2.2.2 Cybercrime ............................................................... 16
    - 2.2.3 Cyber Terrorism ......................................................... 18
    - 2.2.4 Telecommunication ................................................... 20
2.2.5 Social Media

2.2.6 Telegram Application

2.2.7 Privacy Policy

2.2.8 Electronic Information and Transactions

2.3 Legal Basis from National Law

2.3.1 Law No. 11 of 2008 concerning on Electronic Information and Technology

2.3.2 Law No. 36 Year 1999 concerning Telecommunication

2.3.3 Criminal in Indonesia Penal Code

2.3.4 Law No. 1 Year 2002 concerning Terrorism

CHAPTER 3

Cyberterrorism through Telegram Application

CHAPTER 4

LEGALITY OF INDONESIA GOVERNMENT’S ACTION IN BLOCKING TELEGRAM APPLICATION DUE TO CYBERTERRORISM ACTIVITIES

4.1 The legal basis for the Ministry of Communications and Informatics to block Telegram application

CHAPTER 5

Conclusions and Recommendation

5.1 Conclusions

5.2 Recommendation

REFERENCES

APPENDIX
CHAPTER 1
Introduction

1.1 Background

In this era of globalization there are a lot of social media used by people such as Friendster, Facebook, WhatsApp, Twitter, Path, Instagram, BeTalk, Bigo, Badoo, Tinder, Telegram, and much more. Moreover, all information can be accessed quickly by using data, Wi-Fi and as the advancement of telecommunication technology, media, and information, the Internet is as one now as the important media in human life.

The existence of internet applications has had a positive impact on our lives. The Internet also provides cheap and fast access and can be used at any time to get the information we want from around the world. But in addition to having a positive impact; the Internet can also have a negative impact. Thus the misuse of computers in a way that deviates from the main purpose can lead to what is called a computer crime.

Telecommunications is any transmission, delivery, and/or acceptance of any information in the form of signs, signals, writings, drawings, sounds, and noises through wire, optical, radio or other electromagnetic systems.\(^1\) A communication tool is any tool or equipment used in telecommunications. The principle and purpose of telecommunications itself are organized on the basis of principles of benefit, fair and equitable, legal certainty, security, partnership, ethics, and self-belief.\(^2\)

Telecommunication is organized with the\(^\) aim to support the union and unity of the nation, to improve the welfare and prosperity of the people in a fair and equitable way, to

---

\(^1\) Paragraphs (1) and (2) of Article 1, Articles 2 and 3 of Law No. 36 of 1999 concerning Telecommunication.

\(^2\) Ibid
support economic life and government activities, and to improve relations between nations.\textsuperscript{3}

According to Law No. 36 of 1999 regarding Telecommunications the Indonesian side is in conformity with the law No. 36 of 1999 on Telecommunications and the decisions are already contained in the press release of the Ministry of Communications and Information Technology No. 86 / HM / KOMINFO / 07/2017 concerning Recent Developments concerning banning of Telegram Access Applications.

The decision to block thousands of Telegram content was executed after considering the lack of goodwill on the part of Telegram since the 6th e-mail was sent from Tuesday dated July 11, 2017 to Thursday evening of July 13, 2017.\textsuperscript{4} In the absence of Telegram's response, the Ministry of Communications and Informatics decided to block the web version of Telegram service containing thousands of content of radicalism and terrorism.\textsuperscript{5}

On July 14, 2017 at 11.30 a.m., The Ministry of Communications and Informatics has ordered all Internet Service Providers (ISPs) to block 11 Domain Name System (DNS) associated with web-based Telegram services.\textsuperscript{6}

The Government of Indonesia submitted a claim to Telegram and the following are the 4 points demanded by the Government of Indonesia:
1. A Government Channel should be made in Telegram for communication purpose between Telegram Company and the Ministry of communication and Informatics of the Republic of Indonesia.

\textsuperscript{3} Paragraphs (1) and (2) of Article 1, Articles 2 and 3 of Law No. 36 of 1999 concerning Telecommunication.
\textsuperscript{4} Press Release of Ministry of Communications and Informatics No. 86 / HM / KOMINFO / 07/2027 concerning Recent Developments concerning Blocking of Access to Telegram Applications.
\textsuperscript{5} \textit{Ibid}
\textsuperscript{6} \textit{ibid}
2. The Ministry of Communications and Informatics of the Republic of Indonesia demands an authority as Trusted Flagger against accounts or channels within Telegram in Indonesia.

3. The Ministry of Communications and Informatics of the Republic of Indonesia demands that Telegram open an official representative office in Indonesia.

4. For filtering issues, the Ministry of Communications and Informatics of the Republic of Indonesia will coordinate further to make improvements of the process, organization, technical and human resources. Pavel Durov addressed the blockade of Telegram by saying: "First, Pavel says that all public channels linked to terrorism have been blocked. This blocking is said to be in line with previous reports from the Ministry of Communications and Informatics.

Secondly, Pavel has contacted the Ministry of Communications and Informatics via e-mail to make personal communication. Pavel said "Direct communication helps us to work more efficiently to identify and block future terrorism propaganda,".

Thirdly, Telegram is forming a special team of moderators who understand Indonesian language and culture. That way, reports on terrorist content can be processed more quickly and accurately.

Pavel asserts Telegram is a secure platform with attention to user privacy through the encryption system. Nevertheless, he said that Telegram is not a friend of terrorists.

After PavelDurov explained that it had blocked all public channels relating to terrorism and telegram instead of the Federal Bureau of Investigation (FBI) terrorist friend explains that in general the notion of Cyberterrorism is:

---

7 See: http://jumalapps.co.id/article/12074 uploaded on July 26, 2017 and accessed on December 5, 2017 at 13:00 p.m.

8 Fatimah KartiniBohang, See: http://tekno.kompas.com/read/2017/07/16/10215597/3-upaya-telegram-agar-blokir-dicabut-di-indonesia uploaded on July 16, 2017 at 10.21 a.m. accessed on December 5, 2017 at 14.00 p.m.

9 Ibid
Like the two blades of a sword, technology can save people from destruction, but technology can also cause human destruction. Similarly, the development of technology has been entered all aspects of human life, including aspects of the legal scope, especially in the field of crime. Evil has entered into a new scope for development, a new world called cyberspace. Crime in this cyberspace is also known as cyberspace crime which is often referred to simply by the term cybercrime.

Didik M. Arief Mansyur and Elistris Gultom describe cybercrime as an attempt to enter and / or use computer facilities or computer networks without permission and unlawfully with or without causing any change and / or damage to the computer facilities entered or used. According to them cybercrime is a means for anyone who wants to break the law with or without causing changes and damage to computer facilities to launch his crime.

Cybercrime there are several forms of crime there that are forms of Carding Crime, cracking, unauthorized aces, and illegal contents, deliberate spread of the virus, Cyber Espionage, Sabotage and Cyberterrorism. Cyberterrorism is the most dangerous crime and most feared by the State because it can threaten the security of the State.

---

12 Ibid., p. 9.
13 Ibid., p. 10.
In the form of cyberterrorism activities as an attack, information technology is a tool and subject of attack. The attack of cyberterrorism, in order to fulfill the criteria as terrorism that can cause widespread fear, is in the form of direct attacks on computer systems that pose a threat to the lives of others. For example, disrupting aircraft control systems or hospital medical records, destroying buildings, and peace between countries.

However, a system is generally very complex and made to withstand attacks. Furthermore, there is no clear evidence that an attack on critical infrastructure over the internet has ever been committed by terrorists. Hence the computer is more often used as a tool to achieve terrorist goals than to be the object of attack. This is one of the second forms of cyberterrorism, a supporter in which terrorists use telecommunication media to launch their actions and to recruit members.

Terrorism is a crime against humanity and civilization and is one of the serious threats to the sovereignty of every State because it is an international scale that pose a threat to the security and peace of the world and harm the community, so that the eradication needs to be done in a planned and sustainable way so that human rights can be protected and upheld. Terrorists are the most dangerous criminals and feared by society. Terrorist crimes also destroy buildings, pose a threat to the security of a country and world peace so that continuous eradication is necessary to protect the human rights of many people.

The criminalization policy on terrorism propaganda can be reviewed under the Criminal Code as lex generalis and Law no. 11 of 2008 on Information and Electronic Transactions (IET Law). In relation to the Criminal Code, acts of terrorist propaganda are included in the criminalization policy of crimes against public order regulated in Paragraph

---


16 Indonesia, Law on Stipulation of Government Regulation in Lieu of Law no. 1 of 2002 on Combating Terrorism Crimes into Law no. 15, State Gazette No. 45 of 2003, Supplement to State Gazette no. 4284, General Explanation of Government Regulation in Lieu of Law no. 1 of 2002 on Combating Terrorism Crimes of Paragraph two.
When associated with IET Law, specifically for the dissemination of electronic information containing material for propaganda purposes and support for terrorism is covered by a criminalization policy of dissemination of information which generates a sense of hatred or hostility in Paragraph (2) of Article 28 in conjunction with Paragraph (2) of Article 45 of IET Law.

The reason for the blocking of Telegram is that it contains propaganda associated with radicalism, terrorism, hatred, invitation or means to assemble bombs, how to attack, disturbing images and so forth contrary to Indonesian laws and regulations. There are 11 Domain Name System (DNS) of Telegram, as follows: t.me, telegram.me, telegram.org, coretelegram.org, desktop.telegram.org, macos.telegram.org, web.telegram.org, venus.web.telegram.org, pluto.web.telegram.org, flora.web.telegram.org, and flora-1.web.telegram.org.17

The impact of the Telegram app blocking is that web versions cannot be accessed via computer. It further stated that this Telegram application may endanger the security of the country for failing to submit standard operating procedure (SOP) in handling terrorism cases.

The Director General of Informatics Applications also affirms that in carrying out the duties as mandated by Article 40 of Law. 19 of 2016 on Amendment to Law No. 11 of 2008 on Information and Electronic Transactions, the Ministry of Communications and Informatics always coordinates with State institutions and other law enforcement agencies in handling the blocking of content that violates Indonesian laws and regulations.18

17 Yoga Hastyadi Widiartanto, See: http://tekno-kompas.com/read/2017/07/14/20495927/ini-alasan-pemerintah-blokir-telegram.com, uploaded on July 14, 2017 at 20.49 p.m. and accessed on September 6, 2017 at 16:00 p.m.

18 Press Release of the Ministry of Communications and Informatics No. 84 / HM / KOMINFO / 07/2017 on Termination of Access to Telegram Applications.
The decision on the blocking of 11 web-based DNS of Telegram was done after the Ministry of Communications and Informatics sent a request via e-mail. Demand for thousands of terrorism and radicalism content spreading in 11 DNS was sent from 29 March 2016 to 11 July 2017. Regarding to that, the CEO of Telegram, PavelDurov, had previously apologized and admitted receiving a communication e-mail from the Ministry of Communications and Informatics on July 16, 2017. To solve the issue, the Ministry of Communications and Informatics invited PavelDurov plans to come to Indonesia.19

Based on the findings of the Ministry of Communications and Informatics and other related Ministries / Institutions there are contents that are is not in accordance with the legislation especially concerning the spread of radicalism and terrorism. Therefore the Ministry of Communications and Informatics sent a request to Telegram to clear the contents of all channels facilitated by the Telegram.20

Based on a description of the background of the problems above, the author is hereby interested in conducting research and study on "LEGALITY OF INDONESIAN GOVERNMENT’S ACTION IN BLOCKING TELEGRAM APPLICATION DUE TO CYBERTERRORISM ACTIVITIES".20

---

19 Press Release of the Ministry of Communications and Informatics No. 100 / HM / KOMINFO / 08/2017 on the Minister of Communication and Informatics and CEO of Telegram Discuss Terrorism Handling and Radicalization.

20 Press Release of the Ministry of Communications and Informatics No. 86 / HM / KOMINFO / 08/2017 on Recent Developments regarding Blocking Access to Telegram Application.
1.2 Problem Identification

Based on a description of the background of the problems above, then the subject matter is formulated as follows:

1. How is the legality of blocking Telegram application by the Government of Indonesia linked to terrorist activities using the Telegram application?
2. How does the existence of Telegram application accommodate cybercrime practice that can harm the State?

1.3 The Objectives of Study

The purpose of this study is to determine the legality of banning Telegram application by the Government of Indonesia according to Law No. 36 of 1999 regarding on Telecommunications (Supplement to the State Gazette of the Republic of Indonesia Number 3881 and State Gazette of the Republic of Indonesia Number 154 of 1999), Law no. 11 of 2008 (Supplement to the State Gazette of the Republic of Indonesia Number 4843 and State Gazette of the Republic of Indonesia Number 4843), crimes in the Criminal Code, as well as the government's reason is to prevent such crimes in Law No. 1 of 2002 regarding on Combating Terrorism Crime (State Gazette of the Republic of Indonesia Number 106 Year 2002).
1.4 **Benefits of Research**

This research is expected to produce benefits such as:

**Theoretical**

To find out what legal issues are occurring in the legality of banning Telegram application by the Government of Indonesia in relation to cybercrime, and as a contribution to the legal science of telecommunications, cyberspace information technology, and cybercrime.

**Practical**

This research is useful for giving input to the reader in order to know what laws and legal aspects are used in the legality of blocking Telegram by the Government of Indonesia and related institutions such as prosecutors and Indonesian legal institutions to handle cases related to cybercrime and to assist in the formulation of upcoming policies.

1.5 **Research Method**

As a normative science, the science of law has a way of working with the characteristics of sui generis.\(^{21}\) This research is a legal research that has a different method than other research. Legal research method is a systematic way in conducting for the research.\(^{22}\) Scientific logic in normative legal research is built on the scientific discipline and ways of

---

\(^{21}\) *Legal Research is Law Science is a science of its own kind in terms of work methods and scientific systems*, Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group; 2005).

legal normative law, the science of law which is the object of the law itself.\textsuperscript{23} The legal principle approach is not the goal of legal law research but is a necessary approach in determining which laws are appropriate to seek subjective laws (rights and obligations). Example: Legal principle “Lex specialist derogat legi generali”. The approach of this legal principle is used when there is a conflict between the special law and the general then the special ones apply. The other principles are a way of approach in obtaining the right law. Similarly, if it is said that normative legal research is to review the systematic laws and regulations.\textsuperscript{24}

The methodology of the present study uses a research approach:

\textbf{a. Statutory approach}

The study was conducted using a statutory approach, with the relevant rules and legal principles as the focus of the examination for the study.

This approach is done by reviewing all legislation relating to the issues (legal issues) that are being faced. This legislative approach, for example, is done by studying the consistency / conformity between the Constitution and the Law, or between the Laws one with other laws, etc.

\textsuperscript{23} Ibrahim, SH, M. Hum., and Dr. Johnny, \textit{the Theory & Mclode Normative Law Research}. (Malang: Bayumedia Publishing April; 2005), p. 47

b. Methodology of data analysis

This research is a qualitative research with research tool in the form of literature study by doing literature search. A research method that emphasizes the aspect of an in-depth understanding of a problem rather than looking at the problem for generalization research.

1.6 Systematic of Writing

After going through the process of data collection, data analysis, and research conclusions, the following is the systematic writing of research report:

Chapter 1: Introduction consists of background, research problems, research benefits, and research methods.

Chapter 2: Theoretical and legal aspects of information technology and application blocking by the government.

Chapter 3: Cybercrime via Telegram application.

Chapter 4: Legality of banning Telegram application by Government of Indonesia related to cybercrime.

Chapter 5: The concluding section consists of conclusions and recommendation
CHAPTER 2
Theoretical and Legal Aspects of Information Technology and Application Blocking by the Government

2.1 Legal Provisions on Cyberterrorism and Telecommunications in Indonesia.

Basically, all laws aim to create a condition in the social life of society, both in the small and larger environment, in order that there is a harmony, order, legal certainty and so forth. Advances in information technology became the beginning of cybercrime. Although the progress of information technology become one of the supporting factors of society, but information technology can cause things that have negative effects. Indonesia currently has only one new law governing the behavior of activities in cyberspace. However, the current Law No. 11 of 2008 regarding Electronic Information and Transactions is still using the umbrella provision model so that the provisions on cybercrime are not regulated in its own legislation. Meanwhile, legislation that already existed before IET Law was born did set about the activities in cyberspace even though only a few articles.

The Negative impact in question is as stated by criminologists that crime is closely related to the development of society because crime is the product of society itself. There are three reasons why the attacks of electronic systems are growing day by day.

First, the global growth of the internet itself has caused the regulation of it is increasingly difficult. Secondly, there are millions of hacker-oriented websites that make it

\[\text{Ibid, p. 252.}\]

easier for people to acquire the knowledge they need to interrupt or destroy whatever they want.

Finally, the development of terrorist organizations found in various locations around the world has made it hard to track them down. Ease of access to the internet in addition to being used as a means of development and control, also used by criminals including terrorists with their deeds called cyberterrorism.

### 2.2 Definitions

#### 2.2.1 Crime

Crime is not an event of heredity (innate, inherited) nor is it a biological heritage.\(^{27}\) So crime is not innate or inherited from both parents but from self, biological inheritance done by self with both coercion and self-will.

According to a criminologist, Bonger, *a crime is a very anti-social act, which the State is consciously opposed to by punishment (criminal).*\(^{28}\) Furthermore, another criminologist, Sutherland, also argues that\(^{29}\):

“Criminal behavior is behavior in violation of the criminal law. No matter what the degree or morality, reprehensibility, or indecency of an act, it’s not crime unless it’s prohibited by the criminal law”.

The definitions given by Bonger and Sutherland both define crime as a forbidden act and a new feature of this risk is that new weapons are not physical but in the form of

---


software knowledge, a setting in which the attacks are virtual and the attacker never known and even hid during the attack.

Crime can be done by anyone both women and men with different levels of education. Crime can be done consciously, that is thought, planned, and directed to a certain purpose in a state of consciousness. Crime is an abstract conception in which the crime cannot be touched and seen except for the consequences it causes.

The definition of crime according to Kartono is that sociologically, crime is all speech, action, and behavior that is economically, politically and sociopathologically very detrimental to society, violates the norms of morality, and attacks the safety of citizens (whether it is contained in the law criminal or not).

In the life of society there are various kinds of crimes depending on the target of crime, as proposed by Mustofa quoted from Tri Andrisman's book, namely:

"Crimes against the body (murder, rape, persecution), crimes against property (robbery, theft, fraud), crimes against public order (drunkenness, gambling), and crimes against the security of the State".

A small part of the increase in crime in society itself is caused by some external factors. Much of this is due to the inability and lack of desire of people in society to conform to the norms prevailing in society.

According to Bidianto, "one of the causes of high crime rates in Indonesia is high unemployment; crime will increase if unemployment problems are not addressed immediately."

---

31 Ibid, p. 4
32 Tri Andrisman, Hukum Pidana dan Prinsip-Prinsip Dasar dan Dasar-dasar KUHP Indonesia, (Bandar Lampung: Fakultas Hukum UNILA; 2007), p.9
Actually, there are still many causes of crimes committed in Indonesia, for example: widespread poverty, lack of educational facilities, natural disasters, urbanization and industrialization, and environmental conditions that make it easier for people to commit crimes.

According to Sutrisno and Sulis\textsuperscript{33},

"the cause of crime can be seen from several factors namely the talent of the villain, the natural surroundings, and the spiritual element. The talent of a criminal can be seen by his mentality / spirituality where there are criminals whose mood is irritable his soul is weak and powerless to withstand external pressures. There are also those who have been born with spiritual disabilities since birth."

A spiritual flaw is that the criminal's faith is not so strong as to face a problem with someone, and the evil one is also often abused by others, including his family.

According to the Criminal Code, Crimes against State Security in Article 104 is defined as Assault with the intent to eliminate lives, or deprive the independence, or to abolish the ability of the ruling President and Vice-President. The perpetrator of this crime is punished by death penalty or life imprisonment or a jail sentence of a maximum of twenty years.\textsuperscript{34}

Wolfgang, Savitz and Johnston in The Sociology of Crime and Delinquency provide the definition of criminology as a collection of science of crime aimed at acquiring knowledge and understanding of the symptoms of crime by studying and analyzing scientifically the descriptions, uniformities, patterns, and causal factors related to crime, offender, and community reaction to both.\textsuperscript{35}

\textsuperscript{33} Adam Chazaw., \textit{Indonesian Law Lessons} (Jakarta: Raja GrafindoPersada; 2002), p.71
\textsuperscript{34} Criminal Code (KUHP) (Supplement to State Gazette of the Republic of Indonesia Number 3258)
\textsuperscript{35} Topo Santoso and Eva AchjaniZulfa, \textit{kriminalogi} (Jakarta: PT Raja GrafindoPersada; 2001), p. 9
2.2.2 Cybercrime

The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system.”36

According to Andi Hamzah, crimes in the field of computers in general can be interpreted as illegal users of computers.37 Further, he extended this definition by arguing that computer crime is any illegal activity that uses computers for criminal offenses. No matter how small the impacts or consequences caused by illegal or unlawful use of computers, it is still a crime. Moreover, according to him, computer crime is not a new crime but a common crime, as it may still be solved by the Criminal Code. Many argue that cybercrime is indeed real and different from traditional criminal methods and therefore requires new articulations of law and the formation of new investigative techniques.38

To distinguish computer crime and cybercrime is that the latter is done by utilizing computer technology related to the public information network i.e. the internet. Initial computer crimes, among others, are the attack on the system and network of telephone and money transfers using electronic devices.39 Since computers were initially centralized and unconnected, the chances of a computer crime were more limited to the abuse of the user's

37 Andi Hamzah, Aspek Kriminal dalam Komputer (Jakarta: SinarGrafika, 1990), p. 26
39 Muhammad Bagir, Task Protection and Security Techniques S1 / T1: Annex Investigation and Ethics (Jakarta: Megister Information Technology University of Indonesia, 2005), p. 2
authorization system. However, this understanding is growing more widely because today more computers are connected to the Internet network. So there is a wider act than just a computer crime, namely cybercrime

Cybercrime has a characteristic than conventional crime, among others:

1) Acts committed illegally, without rights or unethical occurs in cyberspace, so it cannot be ascertained the legal jurisdiction of which country applies to it;
2) The deed is done using any equipment that can connect to the internet;
3) Such actions result in both material and immaterial losses (time, value, service, money, goods, dignity, dignity, secrecy information) that tend to outweigh the crime conventional;
4) The culprit is the person who controls internet usage along with the application.

The Increase of computer crime should be a serious concern for any law enforcement agency or persons responsible for network security. The increasing of computer crime due to lack of oversight from the Government despite having Law No. 11 of 2008 concerning on Information and Electronic Transactions, Law No. 36 of 1999, Law No. 1 of 2002 concerning on Terrorism. Nevertheless, every electronic organizer must be held accountable if the information system they make is used by radical groups.
The quinquennial congresses have impacted criminal justice policies, as well as national procedures and professional practices throughout the world. The congresses are especially

---

40Ibid, p. 3
42 Sigid Suseno, Penegakan Hukum Pidana Terhadap Tindak Pidana Siber (Bandung Unpad Press, 2010), p. 3.
critical now, as the globalization of many contemporary problems, including crime, has made international collaboration an urgent priority.\textsuperscript{43}

2.2.3 Cyber Terrorism

Cyberterrorism is a form of planned and politically motivated activity with attacks on information, computer systems, computer programs, and data resulting in massive losses and innocent casualties committed by a group or individual.

In some international law literature, it is mentioned that cyberterrorism is already a part or form of cybercrime. By using internet terrorists can easily do the attack (cyber attack) because through the internet they cannot be identified. Many advantages obtained by terrorists when they do the attack (cyber attack) via the internet. Unlike terror that uses bombs where the terrorist must be on the scene, using the internet the terrorist can perform the action without having to be on the scene.

Cyber attacks occur in two forms, first to attack data and second to attack control system. The first form is used to steal, corrupt or alter data, and delete services. The second form focuses on the control system that will be used to manipulate or disable the physical infrastructure system. There are several possible targets of cyberterrorism, a computer network system owned by the government that is: financial network, power plant or system operated by using internet network.

Organizational networks and actions of national terrorism are limited to the territory of a particular country. Meanwhile, international terrorism is directed to foreign persons and assets, organized by governments or organizations in more than one country, and aims to

\textsuperscript{43} United Nations Office on Drugs and Crime See:
influence the policies of foreign governments. If viewed from the motives behind the occurrence of terrorism or the goal to be achieved by the perpetrator, terrorism can be divided into 3 forms as follows:

a) Political terrorism, a terrorism perpetrated by a person or a group systematically by using patterns of violence, intimidation, and aimed at generating public fear for political purposes;

b) Criminal terrorism, that is terrorism directed for political purposes, based on the interest of a particular group or community to fight for its purpose. Basically, this group performs terrorism based on certain ideology, religion, sect or view;

c) State terrorism, which is state-sponsored terrorist activity or conducted on behalf of the state in the form of state-sponsored acts of terror against a particular individual or group of people or against a particular nation or country.

Cyberterrorism is a picture of the growing world of terrorist crime that is increasingly more systematized and organized by the founders of terrorist organizations.

The Cyberterrorism National Police Agency (NPA) of Japan defines cyberterrorism as an electronic attack through computer networks against critical infrastructures that have potential critical effect on social economic activities of the nation.

The director of Central Intelligence Agency (CIA), George Tenet, said terrorist groups including Hezbollah, Hamas and Al-Qaeda use computerized files, e-mail and encryption to support their operations.

Gabriel Weimann said there are eight factors why there is a shift in the field of terrorism activities from the conventional to cyberterrorism, namely as follows:

---


46M. Cereijo, *Cuba the Threat II: Cyber terrorism and Cyber war, cited in Cyber terrorism – Global Security Threat* Mitko Bogdaboski and Drage Petreski
1) Easy to access. Cyberterrorism can be done remotely. This means that cyberterrorism can be done anywhere through remote control;
2) Regulation, censorship, and all forms of control by the government are few;
3) The potential for information dissemination is already globalized;
4) Anonymity in communicating. This is a common thing in the internet world. Most people interact on the internet using a fake name or commonly called a nickname;
5) Information flows quickly;
6) Low cost to develop and maintain the site. In addition, in implementing cyberterrorism that is generally required is only a computer device connected to the Internet network;
7) Multimedia settings facilitate the delivery of the intent and purpose of terror;
8) Abilities have been better than traditional mass media to present information.

2.2.4 Telecommunication

Telecommunications is any transmission, delivery, and / or acceptance of any information in the form of signs, signals, writings, drawings, sounds, and noises through wire, optical, radio or other electromagnetic systems.

The principle and purpose of telecommunications is that: 48

- Telecommunications are organized on the basis of principles of benefit, fair and equitable, legal certainty, security, partnership, ethics, and self-belief;
- Telecommunication is organized with the aim to support the union and unity of the nation, to improve the welfare and prosperity of the people in a fair and equitable way,

48 Law No. 36 of 1999 concerning on Telecommunications Articles 2 and 3.
to support economic life and government activities, and to improve relations between nations.\textsuperscript{49}

2.2.5 Social Media

Social media is abbreviated as media social, consisting of 2 (two) different words, that is media (tools, means of communication, intermediaries, connectors), and social (with respect to society or referring to the way people interact).

Kaplan & Haenlein\textsuperscript{50} formulates social media is an internet-based application that allows the creation and exchange of content created by users. Furthermore, according to Mayfield stated that \textsuperscript{51}:

"Social media is best understood as a group of new kinds of online media, which share most of the following characteristics: participation, openness, conversation, community, and connectedness".

Compared to conventional media, social media has many advantages: it is easy to use (user friendly), creates wider interaction, global reach, anyone can share information faster in real time, or can measure the effectiveness of information shared through the response that appears. The presence of social media affects the relationships between individuals. Then about how much profit we use social media is very dependent on ourselves each.

The advantages are obviously cheaper than via phone, in addition to establishing friendship, sharing information (faster), self-expression, self-image, and vent venture, to the

\textsuperscript{49}\textit{Ibid} Articles 3
\textsuperscript{51}Mayfield, A. 2008. What is social media? Available at http://www.icrossing.com/uk/sites/default/files_uk/insight_pdf_files/What%20is%20Social%20Media_iCrossing_ebook.pdf accessed 07 Februari 2018 at 8:00 p.m
business/online marketing. Reitz mentions the function of social media, namely: maintaining organizational identity, opportunities in building relationships, the ability to control issues management, and opportunities to promote CSR. 52

Social media has several characteristics that distinguish the conventional media. The social media character presented by Mayfield 53 is somewhat different from that of Musser and O'Reilly. Characteristics of social media according to Musser and O'Reilly 54, among others:

1) Allows web users to do more than just browse information;
2) Allows users to execute directly from the browser and then control the data on social media platforms;
3) Users can add value to the content they access this because social media is user friendly so it does not require special knowledge to use it;
4) A decentralized social media device in the absence of a control system;
5) Transparent and use technology standards grow rapidly into an open, building ecosystem;
6) Application to build open data and use componentsthe appearance of social media does not depend on the application on the 6th structure previously defined.

---


53 Op.cit

2.2.6 Telegram Application

Telegram is a free Russian-made app that allows people to exchange messages, photos and videos in the group up to 5,000 users. Its founders are Nikolai Durov and Pavel Durov. Telegram uses a self-made encryption technology called MTProto. The protocol is done directly by Nikolai Durov, one of the founders of Telegram. This technology is based on 256-bit AES encryption, RSA 2048 encryption, and Diffie-Hellman. This encryption technology is a proud work of Telegram owners to the extent that Telegram offers a huge amount of cash prizes to anyone who can afford to break into this application.

Wired is a monthly American magazine published in print and online editions, that focuses on how emerging technologies affect culture, the economy, and politics. Owned by Condé Nast, it is headquartered in San Francisco, California, and has been in publication since March/April 1993. Several spin-offs have been launched including: Wired UK, Wired Italia, Wired Japan and Wired Germany.

In its earliest colophons, Wired credited Canadian media theory Marshall McLuhan as its "patron saint". From its beginning, the strongest influence on the magazine's editorial outlook came from techno-utopian co-founder Stewart Brand and his associate Kevin Kelly.

From 1998 to 2006, wired magazine and Wired News (which publishes at Wired.com) had separate owners. However, Wired News remained responsible for republishing wired magazine's content online due to an agreement when Condé Nast

---


purchased the magazine. In 2006, Condé Nast bought Wired News for $25 million, reuniting the magazine with its website.

Wired contributor Chris Anderson is known for popularizing the term "the Long Tail", as a phrase relating to a 'power law' type graph which helps to visualize is the 2000s emergent new media business model. Anderson's article for "Wired" on this paradigm related to research on power law distribution models carried out by Clay Shirky, specifically in relation to bloggers. Anderson widened the definition of the term in capitals to describe a specific point of view relating to what he sees as an overlooked aspect of the traditional market space which has been opened up by new media.

The magazine coined the term "crowdsourcing", as well as its annual tradition of handing out Vaporware Awards which recognize "products, videogames and other nerdy tidbits pitched, promised and hyped, but never delivered". To Wired, Telegram's founder (CEO) Pavel Durov once said:

"Secure communications should be free for everyone, showing advertisements side by side with your personal communications are out of date, even immoral, we want to raise the standard of messaging technology to improve communication standards in terms of speed, security and functionality."

Telegram's uniqueness in terms of privacy and security makes this application reach up to 100 million users by 2016. Jade Parker, a senior researcher from the TAPSTRI research

---

58Manjoo, Farhad (July 14, 2008). "Long Tails and Big Heads, accessed on 2,2017 at 20:00 p.m.
group focused on internet use by terrorists, revealed that encryption that ensures confidentiality is not the only factor attracting terrorists to the Telegram platform.\textsuperscript{62}

Encryption is also applied by other service providers such as WhatsApp, though Telegram is still one step ahead as it provides many other facilities to make it easier for users to communicate both confidentially and openly from one individual to another and target a wider audience. The following are some of the reliability offered by Telegram, as follow:\textsuperscript{63}

a) Connection: can be used from remote places;

b) Coordination: able to become a means of communication group of more than 10,000 members;

c) Synchronization: chatting can be done by cross-device;

d) Messaging: can send various types of documents;

e) Encryption: can keep your personal and business secrets;

f) Deletion/destruction of messages: messages can be set according to time;

g) Storage: using cloud computing;

h) Privacy: messages in Telegram are strictly encrypted and can delete messages automatically;

i) Speed: Telegram sends messages faster than other applications;

j) Distribution: telegram server is the largest in the world to ensure the security and speed of messaging;

k) Document security: telegram makes the messages contained therein cannot be hacked.

Telegram Security has been subject to meticulous scrutiny of concern. Critics claim that the Telegram security model is undermined by the use of a specially designed

\textsuperscript{62}Oik Yusuf, See: \url{http://tekno.kompas.com/read/2017/07/15/08305697/mengapa-aplikasi-telegram-disukai-teroris-?page=all} uploaded on October 26, 2016 at 13.30 p.m and accessed on October 15, 2017 at 17.00 p.m.

\textsuperscript{63}Tempo.com, See: \url{https://nasional.tempo.com/read/891542/telegram-diblokir-kemenkominfo-digunakan-kelompok-radikal/} uploaded on July 14, 2017 at 20.01 p.m and accessed on October 17, 2017 at 19.21 p.m.
encryption protocol that has not been proven safe and does not enable secure conversations by default.  

Telegram also draws criticism for its widespread use by the Islamic State terrorist organization (NIIS). NIIS has recommended Telegram to its supporters and members, and by October 2015 they were able to multiply the number of their official channel followers to 9,000. Please note that client developers are required to adhere to the Safety Guidelines.

Telegram offers two types of APIs for developers. Bot APIs allow users to easily create programs that use Telegram messages for an interface. Telegram API allows users to create customized Telegram services. Users are welcome to use both APIs for free. API allows users to connect bot to telegram systems. Telegram Bots is a special account that does not require additional phone numbers to be prepared. This account serves as an interface for code that operates somewhere on the servers of telegram users.

To use it, users do not need to know anything about how the MTProto encryption mechanism works. The Telegram intermediary server will handle all encryption and communication with the Telegram API for the user. Users communicate with this server via a simple HTTPS interface that offers a simplified version of the Telegram API.

---

64 see :https://id.wikipedia.org/wiki/Telegram_(aplikasi), accessed on October 21, 2017 at 5.51 p.m.
65 "Isis Telegram channel doubles followers to 9,000 in less than 1 week", Yahoo News, accessed on October 21, 2017 at 5.51 p.m.
66 See: https://telegram.org/apps, accessed on October 21, 2017 at 6.03 p.m.
67 Ibid
68 Ibid
2.2.7 Privacy Policy

The Telegram users do not need to respond to all of this. Telegram is an open source project. Anyone can learn the API, the Protocol and the Source Code and make the right decision.

While it is not possible for most telegram users to use it, but five million new subscribers will have real reasons to use the self-destruct feature beyond a little text, and this is an amazing area. Following revelation, the NSA pulled data from applications including Angry Birds, on the increasing demand for a fast and secure form of information exchange. And although it has not added an audio message and voice call that will soon be enjoyed by WhatsApp fans, Telegram will follow later.69

2.2.8 Electronic Information and Transactions

Electronic information is the electronic data or a set of electronic data including, but not limited to, writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols or perforations that have been processed that have meaning or can be understood by those who are able to understand them.70

Electronic transactions are legal acts committed by using computers, computer networks, and / or other electronic media.71 The obligations and responsibilities of the electronic system administrators, namely:

69Rhiannon Williams See: http://www.telegraph.co.uk/technology/news/10658647/What-is-Telegram-the-new-WhatsApp.html uploaded on February 25, 2014 at 8.00 a.m GMT and accessed on October 12, 2017 at 7.00 p.m
70Article 1, of Law No. 11 of 2008 concerning electronic information and transaction
71Ibid Article 2
Every administrator of an electronic system shall administer electronic systems reliably and securely and shall be responsible for the operation of electronic systems as appropriate;

The administrator of the electronic system shall be responsible for the administration of electronic systems; and

The provision as referred to in paragraph 2 shall not apply in the case of proven force majeure, errors and / or omissions on the part of users of electronic systems.

Article 16 sets out the minimum requirements that must be met by the administrators of electronic systems in operating electronic systems, namely:

- Can redisplay electronic information and / or electronic documents in full according to the retention period specified according to the laws and regulations;
- May protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the administration of such electronic systems;
- Can operate in accordance with procedures and instructions in the administration of electronic systems, which is equipped with procedures or instructions that are announced with language, information or symbols that can be understood by parties related to the administration of electronic systems; and
- Have an ongoing mechanism to maintain the newness, clarity, and responsibility of procedures and guidelines.

The birth of digital technology has led to the integration and convergence in the development of information technology, media, and telecommunications (information, media, and communication). In line with developments in digital technology, the Indonesian people are more using digital technology than correspondence.

---

2.3 Legal Basis from National Law

2.3.1 Law No. 11 of 2008 concerning on Electronic Information and Technology.

According to Article 15 of Law No. 11 of 2008 concerning on the administration of electronic systems:

- Any administrator of electronic systems shall be reliable and secure and shall be responsible for the operation of electronic systems as appropriate;
- The administrator of the electronic system shall be responsible for administration of his or her electronic system;
- The provision as referred to in paragraph (2) shall not apply in the case of proven force majeure events, errors and/or omissions of the administrator of electronic system.

To the extent not specified otherwise by a separated law, any administrator of an electronic system shall operate an electronic system that meets the following minimum requirements:

a) can redisplay electronic information and/or electronic documents in full according to the retention period specified according to the laws and regulations;

b) may protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the administration of such electronic systems;

c) can operate in accordance with procedures and instructions in the administration of such electronic systems;

d) have an ongoing mechanism to maintain the newness, clarity, and responsibility of procedures and guidelines.
According to paragraphs (4) of Article 27, prohibited acts are:

“Any person who knowingly and unauthorizedly distributes and/or transmits and/or makes accessible electronic information and/or electronic documents with extortion and/or threatening content.”

Criminal provisions under paragraph (1) and (3) of Article 45:

(1) Anyone who fulfills the elements as referred to in paragraphs (1), (2), (3),(4) of Article 27 shall be liable to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000 (one billion rupiah);
(3) Anyone who fulfills the element as referred to in Article 29 shall be liable to a maximum imprisonment of 12 (twelve) years and / or a maximum fine of Rp2,000,000,000 (two billion rupiah).”

2.3.2 Law No. 36 Year 1999 concerning Telecommunication

Telecommunication service is a service to fulfill telecommunication requirement by using telecommunication network. The administration of it is regulated in paragraph (2) of Article 7, paragraph (1) of Article 18, and Article 21 which reads:

Paragraph (2) of Article 7:

“In the administration of telecommunications, the following should be noted:

a. protecting the interests and security of the state;
b. anticipating technological developments and global demands;
c. done professionally and accountable;
d. Community participation.”
Article 18:

(1) The administrators of telecommunication services shall be note / record in detail the usage of telecommunication services used by telecommunication users.

(2) If the user requires a note / record of telecommunication services as referred to in paragraph (1), the administrator of telecommunications shall be obligated to provide it.

(3) The provisions on the registration / recording of the use of telecommunication services as referred to in paragraph (1) shall be governed by a Government Regulation.

Article 20:

“Every administrator of telecommunications shall give priority to sending, channeling and delivering vital information concerning:

a) state security;

b) the salvation of the life and possessions;

c) natural disasters;

d) danger; and/or

e) disease outbreaks.”

Article 21:

The administrators of telecommunications shall be prohibited from engaging in business activities in the administration of telecommunications that are contrary to public interest, morals, security or public order.
The telecommunication security itself is provided in paragraphs (1) and (2) of Article 39, Article 41, and paragraphs (1) and (2) of Article 42 which reads:

**Article 39:**

1) “The administrator of telecommunications shall be required to secure and protect the installation of telecommunication networks used for the administration of telecommunications;

2) The security and protection provisions as referred to in paragraph (1) shall be governed by a Government Regulation.”

**Article 41:**

“In order to verify the use of telecommunication facilities at the request of the users of telecommunication services, the administrators of telecommunication services shall record the use of telecommunication facilities used by the users of telecommunication services and may record information in accordance with applicable laws and regulations.”

**Article 42:**

1) “The administrators of telecommunication services shall keep confidential information transmitted and/or received by telecommunication service subscribers through telecommunication networks and/or telecommunications services which are administrated;

2) For the purposes of the criminal justice process, the administrators of telecommunication services may record information sent and/or received by the
administrators of telecommunication services and may provide the necessary information on:

a. Written request by the Attorney General and/or the Chief of Police of the Republic of Indonesia for specific criminal acts,
b. Investigator's request for a certain criminal act in accordance with applicable laws.”

The subject of the investigation is provided in paragraph (1) of Article 44 which reads:

“In addition to the investigators of the State Police Officers of the Republic of Indonesia, as well as certain Civil Service Officials within the Ministry whose scope of duty and responsibility are in the telecommunications field, are authorized as investigators as referred to in the Criminal Code to conduct investigations of criminal offenses in the telecommunications field.”

The subject of administrative sanctions is regulated in paragraphs (1) and (2) of Article 46 which reads:

(1) The administrative sanction as referred to in Article 45 shall be the revocation of permit.
(2) The revocation of permit as referred to in paragraph (1) shall be made after written warning is given.

The subject of a criminal act is provided in Article 57 which reads:

“The administrators of telecommunication services violating the provisions as referred to in paragraph (1) of Article 42 shall be subject to imprisonment of a
maximum of 2 (two) years and/or a fine of not more than Rp200,000,000 (two hundred million rupiah).

2.3.3 Criminal in Indonesia Penal Code

As is common in the legal system, the Dutch criminal law distinguishes between "misdrijven", namely a more serious crime that is broadly comparable to a very serious criminal offense called the term crime, and "overtredingen" (offense), or less criminal offense.

Crime is a term that can include insights relating to very diverse patterns of human behavior ranging from the veiled behind. Moeljatno said that the crime is "rechtsdeliten" which is an act which, although not regulated in the law, as a criminal debate has been perceived as onrecht, as an act contrary to the rule of law.73

The offense is "wetsdelikten", that is, the act of unlawfulness is known only after the law determines that. According to Andi Hamzah, crime is an offense that violates the interests of the law and also endangers concretely. The formulations of the crimes contained in the Criminal Code are all forms of deeds that meet the formulations of the provisions of the Criminal Code.74

As proof that the outline between recht and wetsdikikten is very difficult to determine and which is a necessity for any formation of legislation is to determine that a particular criminal act is entered into a crime or offense. If this determination does not exist then it cannot be tried before the court.75

73See: http://www.definisi-pengertian.com/2015/05/definisi-pengertian-tindak-pidana-kejahatan.html, accessed on October 18, 2017 at 10.00 p.m.
74Ibid
75Muladi dan Barda Nawawi Arief, Crime Theories and Policy, (Bandung: Alumni; 1984).
According to the second Book of Criminal Code on Indonesia Penal Code Article 104:

“Assault for the purpose of eliminating lives, or depriving of liberty or negating the ability of the President or Vice President to govern, shall be punished by death penalty or life imprisonment or imprisonment of a maximum of 20 (twenty) years.”

According to paragraph (1) of Article 55, paragraphs (1) and (2) of Article 56 and paragraphs (1) and (2) of Article 57 concerning on Participation in Crime, it is established that:

**Paragraph (1) of Article (55):** Sentenced as a criminal offender:

“Those who do, who enjoin to do, and who participate in doing the deed”

Paragraphs (1) and (2) of Article 56: Sentenced as a crime aide:

(1) Those that deliberately provide assistance when the crime is committed;
(2) Those that deliberately provide opportunities, means or information to commit a crime.

**Paragraphs (1) and (2) of Article 57:**

(1) “In the case of provision of assistance, the maximum criminal penalty, minus one third.
(2) If the crime is threatened with capital punishment or life imprisonment, then the maximum imprisonment of 15 years is imposed.”
2.3.4 Law No. 1 Year 2002 concerning Terrorism

The criminal act of terrorism shall be all acts which fulfill the elements of a criminal act in accordance with the provisions of this Government Regulation in Lieu of the Laws.

According to Article 6 on the Crime of Terrorism, stated:

“Anyone who deliberately uses violence or threats of violence creates an atmosphere of terror or fear of a widespread person or causes a mass casualty, by seizing independence or loss of life and property of others, or resulting in damage or destruction of strategic or environmental vital objects or public facilities or international facilities, shall be subject to capital punishment and life imprisonment or a minimum imprisonment of 4 (four) years and a maximum of 20 (twenty) years.”

The evidence of criminal investigation of terrorism crime based on Article 27 regarding on Investigation, Prosecution and Investigation in the court, the evidence including:

a) Evidence as referred to in the Criminal Code;

b) Other evidence of information that is spoken, transmitted, received, or stored electronically by optical means or something similar; and

c) Data, recordings or information that can be seen, read and / or heard, which may be issued with or without the aid of a device, contained on paper, any physical objects other than paper, or electronically recorded, including but not limited to:

- Writing, sound or image;
- Maps, designs, photographs or the like;
- Letters, signs, numbers, symbols, or perforations that have meaning or can be understood by people who are able to read or understand them.
CHAPTER 3

Cyberterrorism through Telegram Application

The Decree of the Minister of Communications and Informatics to block the 11 web-based DNS of Telegram was made after the Ministry of Communications and Informatics sent a request for Telegram to open chat via email. Demand to close thousands of terrorism and radicalism content spreading within the 11 DNS was sent by the government from 29 March 2016 to 11 July 2017. With regard to it, the CEO of Telegram, Pavel Durov, had previously apologized and admitted receiving a communication e-mail from the Ministry of Communications and Informatics on July 16, 2017. To solve the issue, the Ministry of Communications and Informatics invited Pavel Durov to come to Indonesia.  

On July 14, 2017, the Ministry of Communications and Informatics has requested that the Internet Service Provider (ISP) terminate (block) access to the 11 Domain Name System (DNS) owned by Telegram. This blocking must be done because the many channels in the service are propaganda of radicalism, terrorism, hatred, invitation or means to assemble bombs, how to attack, disturbing images, and others that are contrary to Indonesian laws and regulations.

There is a very strong reason why the government should block social media application of the Telegram. This application was used by terrorist groups as a means to confirm the establishment of new members. Telegram is also used to teach new members from how to make a bomb to how to blow it up. Expert Staff of the Ministry of

76 Press Release of the Ministry of Communications and Informatics No. 100 / HM / KOMINFO / 08/2017 on the Minister of Communication and Informatics and CEO of Telegram Discuss Terrorism Handling and Radicalization.

77 Press Release of the Ministry of Communications and Informatics No. 84 / HM / KOMINFO / 07/2017 on Termination of Access to Telegram Application.
Communication and Informatics for Legal Affairs, in a Discussion at the Auditorium of Pertamina University, South Grogol, Kebayoran Lama, South Jakarta, Saturday, July 29, 2017 says that, “Through Telegram application they teach how to make bombs and how to strengthen the hearts of the recruits as terrorists.” He also explained how the mode of terrorist groups to seek / recruit members through social media. In order for anyone interested in joining a terrorist group, they first create a radically-contented website. Then the link to the site is sent by the buzzer team and also the sympathizer via Facebook and Twitter account.\(^78\)

Those interested in joining will be indoctrinated through a more privacy-maintained chat app, Telegram. Ren confirms that "They communicate with each other on Facebook first. The candidate affixed like, then invited to communicate through a more secure route that is through Telegram."\(^79\)

The method of a terrorist group is to search for new members through social media. First, in order for anyone interested in joining a terrorist group, they create a radically-contented website first. Then, a link to the site is sent by the buzzer team and also sympathizers via Facebook and Twitter accounts. Those interested in joining will be indoctrinated through a more privacy-maintained chat app, Telegram.\(^80\)

The Minister of Communications and Informatics Rudiantara said,

"I have received an e-mail about apology from Pavel Durov, CEO of Telegram, apparently he is not aware of several requests from the Ministry of Communications and Informatics since 2016. Durov has followed up on what the Ministry of Communications and Informatics requested and he proposed a special communication to process the handling of negative content especially radicalism / terrorism. I respond

\(^78\) Tim Viva, See: http://www.viva.co.id/digital/940935-hati-teroris-diteguhkan-melalui-telegram-ungkap-kominfo uploaded on July 29, 2017 at 7.32 p.m and accessed on October 28, 2017 at 1.30 a.m.

\(^79\) Ibid

\(^80\) Ibid
to the proposal from PavelDurov and will follow up as soon as possible from the technical details so that the standard operating procedure (SOP) can be implemented immediately.” The 11 DNS that are blocked are as follows: t.me, telegram.me, telegram.org, coretelegram.org, desktop.telegram.org, macos.telegram.org, web.telegram.org, venus.web.telegram.org, plutoweb.telegram.org, flora.web.telegram.org, and flora-1.web.telegram.org. The impact of this blocking is that web version of Telegram service cannot be accessed via computer.\(^{81}\)

The policy aimed at screening for content that is radicalism and terrorism is a follow-up of the handling of issues that threaten the security of the country, especially with the start of geopolitical and geostrategic change in Southeast Asia, especially the events that occurred in Marawi, Southern Philippines.

The issue of state security is of particular concern to the President and the President supports the prosecution of content that could threaten the security of the country.\(^{82}\) And One case in Indonesia related to terror in MH Thamrin area, Central Jakarta, January 2016 agois the use of Telegram application. "Up to the bombing in Kampung Melayu, the last in Falatehan, which turned out to be from the communications they use that all use Telegram", said Tito in the National Monument Square, Central Jakarta, Sunday (16/07/2016).

In the case of Kampung Melayu, police found direct communication from terrorists through Telegram with BahrunNaim, a sympathizer of a group calling itself an Islamic

---

\(^{81}\)Press Release of the Ministry of Communications and Informatics No. 84 / HM / KOMINFO / 07/2017 on Termination of Access to Telegram Application.

State (ISIS), from Indonesia who is now in Syria.\(^3\) The government can look in the case of terror in MH Thamrin area, Central Jakarta, January 2016, bomb in Kampung Melayu until the stabbing of two members of the Mobile Brigade at Falatehan Mosque, KebayoranBaru.

In the case of the stabbing of the Mobile Brigade personnel at Falatehan Mosque, the alleged offender is known to plan an attack on the police in the presence of radical views exposed by radical groups in Telegram.

The flag rising of the ISIS in the office of the Kebayoran Lama Police Department occurred with the exposure of radical views presented by various terrorist groups through Telegram which was mentioned as Manjanik, Ghuroba, UKK and KhilafahIslamiyah Tito said “So far, many superior features have been boasted by Telegram, among them capable of loading up to 10,000 members and encrypted, meaning it is difficult to detect. So the Police requested that the Ministry of Communications and Informatics address this, one of which is closed.” \(^4\)

The Indonesian government also imposed the same law with the government residing in Marawi, Southern Philippines to a radical network that uses telegram applications by blocking telegram applications using existing laws in Indonesia.


\(^4\)BBC See: http://www.bbc.com/indonesia/indonesia-40624053, uploaded on July 17, 2017 and accessed on December 7, 2017 at 1.07 a.m.
CHAPTER 4

LEGALITY OF INDONESIA GOVERNMENT’S ACTION IN BLOCKING TELEGRAM APPLICATION DUE TO CYBERTERRORISM ACTIVITIES

4.1 The legal basis for the Ministry of Communications and Informatics to block Telegram application

The blocking of Telegram service is done from the decision of the Counter-Terrorism team led by the Ministry of Communication and Information. Not just blocking Telegram services. But the owner of the Telegram app service is being stopped when there is content related radicalism. 85

Minister of Communication and Informatics has legal basis to block Telegram application that is: Law No. 11 of 2008 on Information and Electronic Technology, Law no. 1 of 2002 on Terrorism, and Law no. 36 of 1999 on Telecommunications, as well as Criminal Code, because the Telegram party violates all these laws and regulations. Telecommunications Law, as well as Criminal Code, because the Telegram party violates all these laws and regulations. Telecomunications Law, as well as Criminal Code, because the Telegram party violates all these laws and regulations. Until now, there is no regulation that regulates using of social media includes telegram, Articlee 40 ofLaw No. 19 of 2016 the changes of Law No. 11 of 2018 stated:

(1) The government regulates the using of Technology Information and Electronic Transaction in accordance with the regulation and law;
(2) The government shall protect public interes from any kind of disturbance resulting from the misuse of Electronic Information and Electronic Transactions that disrupt public order, in accordance with the provisions of legislation;
(2a) The Government shall be obliged to prevent the dissemination and use of Electronic Information and / or Electronic Documents which have a content prohibited in accordance with the provisions of legislation.
(2b) In doing the prevention as referred to in paragraph (2a), the Government is authorized to terminate the access and / or order to the Operator of Electronic System to make the termination of access to Electronic Information and / or Electronic Document having unlawful content.
(3) The Government shall stipulate institutions or institutions possessing strategic electronic data which shall be protected.

Where the content of the telegram itself has a charge that the State is prohibited and such acts may threaten the security of the State so on that basis the government shall block the telegram. Whereas the use of social media is not forbidden by the government if social media users pose a threat to the State government should act, in this case the use of telegram may pose a threat to the state then the government must close up to the responsibility of the telegram

Law no 11 of 2008 is made to recall and consider that national development is an ongoing process that must always be responsive to the various dynamics that occur in society. Information globalization has placed Indonesia as part of the world's information society so that it requires the establishment of arrangements on the management of Information and Electronic Transactions at the national level so that the development of Information Technology can be done optimally, evenly, and spread to all levels of society in order to educate the nation.
The rapid development and advancement of Information Technology has led to changes in human life activities in various fields that have directly affected the birth of new forms of legal action; that the use and utilization of Information Technology should be continuously developed to maintain, maintain and strengthen national unity and integrity based on the Laws and Regulations in the national interest.  

Ministry of Communication and Informatics through a press release held yesterday said. If Telegram is used as a nest of Terrorists, especially ISIS. Party Ministry of Communication and Informatics admitted if there are already about 17 thousand radical pages scattered in the Telegram instant messaging application.  

The government also argues if Telegram presents a variety of radical content that can undermine diversity. Telegram is also called a favorite application of terrorists because of its advantages are considered anti-tapping and anti-piracy.  

The uniqueness of this Law as it applies to any person who commits a legal act as provided for in this Law, both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, which has legal consequences in the jurisdiction of Indonesia and/or outside the territory Indonesian law and harm Indonesia's interests. So that it can be interpreted and has a scope that is different and wider than the existing law in dealing with the Cyber Crime problem, because the meaning of the use of the articles in the existing law was biased.  

---

86 See:
https://books.google.co.id/books?id=Qx_dCwAAQBAJ&pg=PA361&lpg=PA361&dq=Perkembangan+pesat+dan+kemajuan+Teknologi+Informasi+telah+menyebabkan+perubahan+dalam+aktivitas+kehidupan+manusia+di+berbagai+bidang+yang+secara+langsung+mempengaruhi+kelahiran+bentuk+bentuk+tindakan+hukum+baru+bahwa+penggunaan+dan+pemanfaatan+Teknologi+Informasi+harus+terus+dikembangkan+untuk+memelihara+memelihara+dan+memperkuat+persatuan+dan+integritas+nasional+berdasarkan+pada+Hukum+dan+Peraturan+untuk+kepentingan+nasional&source=accessed April 4th, 2018 at 22:35 p.m.

Principles and Objectives This Act is the utilization of Information Technology and Electronic Transactions carried out based on the principle of legal certainty, benefits, prudence, good faith, and free choice of technology or technology neutral. So, it can be interpreted that the use of information technology and electronic transactions is expected to be guaranteed with legal certainty, have benefits, full of caution, good faith, and the freedom of choice of technology and neutral.

The provisions referred to in paragraph (2) shall referred to in paragraph (2) article 15 of Law No. 11 year 2008 concerning on Electronic Information and Technology shall not apply in the presence of evidence for force majeure, errors and / or omissions from the administrators of electronic systems. In this case also including.

Based on Article 16, any administrator of the electronic system shall operate an electronic system that meets the following minimum requirements:

a. Can display electronic information and / or electronic documents in full according to the retention period specified according to the laws and regulations;

b. May protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the administration of such electronic systems;

c. Can operate in accordance with procedures and instructions in the administration of such electronic systems;

d. Have an ongoing mechanism to maintain the newness, clarity, and responsibility of procedures and guidelines.

According to paragraphs (4) of Article 27, prohibited acts are:

“Any person who knowingly and unauthorizedly distributes and / or transmits and / or makes accessible electronic information and / or electronic documents with extortion and / or threatening content.”

---

88 Law No. 19 Year 2016 concerning on Amendment Law No. 11 Year 2008 concerning on Infomatic a and Electronic Transaction Article 3
In articles 15, 16 and 27 electronic system providers shall be responsible, display electronic information and/or electronic documents, protect the availability, integrity, authenticity, confidentiality and accessibility of Electronic Information, electronic organizers shall also have an ongoing mechanism for maintaining novelty, clarity and responsibility of the procedures or instructions made by the electronic system providers, and any person who knowingly and without right to distribute and / or transmit and / or make accessible Electronic information and/or Electronic Documents with extortion and/or threatening charges, the organizer electronics shall comply with all procedures set forth in the article and if not following such procedures the organizer may be threatened with criminal acts pursuant to sections 15, 16 and 27.

Based on Telecommunication law, telecommunication development and operation has demonstrated an increasingly important and strategic role in supporting and encouraging economic activity, strengthening defense and security, enhancing the life of the nation, facilitating government activities, strengthening national unity and unity within the framework of the archipelago, and strengthen national resilience and improve relations among nations. Changes in the global environment and the rapid development of telecommunications technology led to fundamental changes, created a new telecommunication environment, and changes in perspective in telecommunications, including the convergence of information technology and broadcasting, so it is deemed necessary to reorganize the national telecommunications.

Based on Law No.36 of 1999 concerning on Telecommunications Article 7 paragraph (2) in the operation of telecommunications, note the following matters:

a) Protecting the interests and security of the State
b) Anticipate technological developments and global demands
c) Conducted professionally and accountable
d) Community participation
In the case of telegram blocking, the government observes that the telegram violates Paragraph (3) of Article 27 stated:

“Any person who knowingly and unauthorized distributes and/or transmits and/or makes accessible electronic information and/or electronic documents with extortion and/or threatening content, if the telegram does not telegram application blocker that there is a network of radical in telegram application, will be enforce blocked by the Indonesian government as already contained in the press release.”

Being the basis of the government's telegram blocking because the government saw Law No. 36 of 1999 on Telecommunications article 7, paragraph 2, could be a strong basis for blocking telegram because radical groups use telegram to undermine the security of the State and the interests of others.

Based on Article 18 paragraphs (1), (2) and (3):

1) The provision of telecommunication services shall record / record in detail the use of telecommunication services used by telecommunication users;

2) If the user requires a record / recording of the use of telecommunication services as referred to in paragraph (1), the telecommunication operator is obliged to provide it; 3.

The provisions concerning the recording / recording of the use of telecommunication services as referred to in paragraph (1) shall be regulated by a Government Regulation

Telegram parties must record / record if the government requires the telegram must provide if not given the government is obliged to give sanctions and if there is no response the government must call the telegram as the government in the case of blocking telegram to hold accountable if not provide recording / recording.
Article 20 provides that *every administrator of telecommunications shall give priority to sending, channeling and delivering vital information concerning:*

a. state security;
b. the salvation of the life and possessions;
c. natural disasters,
d. danger, and/or disease outbreaks.

The telecommunication security itself is provided for in paragraphs (1) and (2) of Article 39, namely: (1) The administrator of telecommunications shall be required to secure and protect the installation of telecommunication networks used for the administration of telecommunications. (2) The security and protection provisions as referred to in paragraph (1) shall be governed by a Government Regulation.

Furthermore Article 41 stated that:

“*in order to verify the use of telecommunication facilities at the request of the users of telecommunication services, the administrators of telecommunication services shall record the use of telecommunication facilities used by the users of telecommunication services and may record information in accordance with applicable laws and regulations.*”

Paragraphs (1) and (2) of Article 42 provide that:

1) “*The administrators of telecommunication services shall keep confidential information transmitted and/or received by telecommunication service subscribers through telecommunication networks and/or telecommunications services which are administrated.*”
2) For the purposes of the criminal justice process, the administrators of telecommunication services may record information sent and / or received by the administrators of telecommunication services and may provide the necessary information on: a. written request by the Attorney General and/or the Chief of Police of the Republic of Indonesia for specific criminal acts, b. investigator's request for a certain criminal act in accordance with applicable laws.

The investigation is provided in paragraph (1) of Article 44:

“In addition to the investigators of the State Police Officers of the Republic of Indonesia, as well as certain Civil Service Officials within the Ministry whose scope of duty and responsibility are in the telecommunications field, are authorized as investigators as referred to in the Criminal Code to conduct investigations of criminal offenses in the telecommunications field.”

In the case of investigations all Indonesian National Police investigators and civil servants are responsible for investigating cases of telegram blocking and if the Attorney General and or the Chief of Police of the Republic of Indonesia request recording evidence for the investigation process in a particular crime and in the process of further investigation for now the case of telegram blocking by the Indonesian government which again handled by The Ministry of Communications and Informatics and Police, telegram organizers have also been called and apologize to the Indonesian government and the telegram has lowered the colleagues who understand the rules in Indonesia, language, and Indonesian culture for telegram not so blocked.

Accordance with Article 104, Article 55 paragraph (1), Article 56 paragraphs (1) and (2), and 57 paragraphs (1) and (2) whose contents are as follows:
Article 104 of Criminal Code concerning Crime stated:

“assault with the intent to eliminate lives, or deprive the independence, or to abolish the ability of the ruling President and Vice-President. The perpetrator of this crime is punished by death penalty or life imprisonment or a jail sentence of a maximum of twenty years.”

Article 55 regarding on Sentenced as a criminal offender:

“those who do, who enjoin to do, and who participate in doing the deed.”

Article 56 provide that: Sentenced as a crime aide:

(1) “Those who deliberately provide assistance when the crime is committed;
(2) Those who deliberately provide opportunities, means or information to commit a crime.”

Furthermore, in paragraphs (1) and (2) of Article 57 it is stipulated that: (1) In the case of provision of assistance, the maximum criminal penalty, minus one third. (2) If the crime is threatened with capital punishment or life imprisonment, then the maximum imprisonment of 10 years is imposed.

a. In addition to the criminal code of terrorism is also subject to sanctions contained in Law No. 1, 2002 on Terrorism which in which terrorists have used violence or threat of violence to the community because it caused an atmosphere of terror that makes people fear of widespread and cause victims who are mass by depriving their independence and also resulting in the destruction of vital objects in the environment or public facilities and terrorists may be subject to penal sanctions contained in Lately, the mode
of terrorist acts has begun to vary, such as the Kampung Melayu bombs, the last in Falatehan, the propaganda of radicalism, terrorism, hatred, the invitation or the means of assembling bombs, the way of attacking, disturbing images and others, invitation in Indonesia, which turned out to be from the communication they use all of them using Telegram, these threats can happen anytime and anywhere, and threaten the safety of everyone's soul at this time there is no safe place and can be said to be free from the threat of terrorism, stabbing Brimob personnel at Masjid Falatehan, the alleged perpetrator was known by plotting an attack on the police since being exposed to radicalism by radical groups in Telegram all terrorist acts could be criminalized according to Presidential Regulation No. 1 of 2002 on Terrorism and within article 6 of Indonesia Penal Code which states:

“any person who deliberately uses violence or threat of violence creates an atmosphere of terror or fear of a widespread or massive victim, by seizing independence or causing destruction or destruction of strategic vital objects or the environment or public facilities or facilities international, sentenced to death or life imprisonment or imprisonment of a minimum 4 (four) years and a maximum of 20 (twenty) years.

And in article 27 of the Investigation, Prosecution and Inspection in court proceedings namely the evidence of criminal investigation of terrorism which contains about evidence as referred to in the Criminal Code;

a) Other evidence of information that is spoken, transmitted, received, or stored electronically by optical means or something similar; and
b) Data, recordings or information that can be seen, read and / or heard, which may be issued with or without the aid of a device, contained on paper, any physical objects other than paper, or electronically recorded, including but not limited to:

1. Writing, sound or image;
2. Maps, designs, photographs or the like;
3. Letters, signs, numbers, symbols, or perforations that have meaning or can be understood by people who are able to read or understand them.

The administrators of telecommunications must provide services to the government so that the latter may open access if state security problems occur such as registration/recording of the use of telecommunication facilities. The administrator of telecommunications must participate in protecting the interests and security of the state, anticipating technological developments and required to do so professionally and accountably in court if necessary in certain offenses in accordance with applicable law.

4.2 The existence of Telegram application in Indonesia accommodates cybercrime practice can harm the state.

The existence of telegram applications in Indonesia can facilitate Radical groups to communicate in secret because the telegram app has a Private Chat feature. In a private chat nobody can see the chat of telegram users including the government, consequently the government cannot trace the network of radicalism and difficult to capture the network.

The telegram is temporarily blocked until the Telegram party makes an apology, comes to Indonesia to account for it, and provides contacts that can be contacted if something similar happens and addition to the existence of telegram applications can facilitate radical groups there are several Terms that are used for the law that regulates activities in the virtual space is the law of the internet; the law of information technology; the telecommunication law; and lexinformatica.89

Telegram has not been blocked anymore causes by the Ministry of Communication and Informatics and made several agreements. *First*, telegram will allocate its resourcing in Indonesian. There will be a representative from Telegram in Indonesia to handle the issues and to keep the government easier to coordinate with Telegram. *Second*, Telegram entrust especially for their representative to communicate with the Ministry and provide a special channel to the Ministry in handling negative content especially terrorism and radicalism.

Telegram also promised to create a kind of script program, to do the filtering on the platform. In addition, Telegram is also agreed that there are standard procedures if there are negative content of radicalism and terrorism in Telegram. These is including the handling of radicalism and terrorism content requested by the Ministry of Communications and Information Technology at the same time.

Emergence of cybercrime cases in Indonesia has been a threat to security stability and public order with an escalated high enough. The government with its legal instruments has not been able offsetting the crime techniques done with computer technology especially in connection with Internet or Cyber Media (internetwork).

Unlawful lawsuits in the cyber world are not easy to overcome if only relying on conventional positive law.

The scope of cyberlaw with a special *(sui generis)* regulatory setting for activities within cyberspace includes, among others:

1) Copyright;
2) Brand (Trademark);
3) Defamation or Defamation;
4) Insults, defamation, SARA (Hate Speech);

---

90 *Ibid*, p. 130
5) Attacks on computer facilities (Hacking, Viruses, Illegal access);
6) Internet development regulation (Regulation Internet Resource);
7) Privacy Rights;
8) The Precautionary Principle (Duty of Care);
9) Criminal offense (Criminal Liability);
10) Procedural, Procedural issues;
11) Electronic Contracts and Digital Signatures;
12) Pornography;
13) Theft;

In practice, according to Teguh Arifiyadi the challenges encountered in the cyber world are encryption, anti-forensics, internet speed, and large data.

"In addition, the criminals who hide in difficult to reach websites or better known as the term deepweb also become one of the challenges that will be removed in the future," he said.\(^{93}\)

Understanding of the general principle of good governance hereinafter abbreviated as AUPB is a principle used as a reference for the use of Authority for Government Officials in issuing decisions and / or actions in government organizers.\(^{94}\)

In the case of telegram the government has followed the General Principles of Good Governance because the government has made efforts to telegram no longer used by

\(^{93}\)Kementrian Komunikasi dan Informatika See : https://www.kominfo.go.id/content/detail/10533/dari-ekonomi-digital-blokir-konten-hingga-wannacry/0/berita_satker_upload September 05, 2017, accessed February 14, 2018 at 04:52 a.m.

\(^{94}\)Administrasi Pemerintah, See : http://pemerintah.net/asas-asas-umum-pemerintahan-yang-baik-aupb/ accessed April 3\(^{rd}\), 2018, at 03:32 a.m
terrorist groups and that the State of Indonesia can be safe from terrorist groups and the
government has exercised authority over its obligations under Article 8 paragraph (2):\textsuperscript{95}

- Laws and Regulations;
- General Principles of Good Governance

And the Government in blocking Telegram is in accordance with Article 10 paragraph
(1) namely General Principles of Good Governance referred to in Law Number 30 Year
2014 About the Administrative State includes the principle:

- Legal certainty;
- Utilization;
- Impartiality;
- Accuracy;
- No abuse of authority
- Openness;
- Public interest; and
- Good service.

\textsuperscript{95} Ibid
CHAPTER 5
Conclusions and Recommendation

5.1 Conclusions

Based on the discussion that has been described in the previous chapters, then in this chapter some conclusions of research and discussion of material that has been done will be described. The conclusions that can be taken are as follows:

1. The Indonesian government considers it necessary to block Telegram because in this application there is content that contains elements of Cybercrime, such as: Distribution of crimes through Telegram application in accordance with
   - Article 104 of Criminal Code concerning crimes, paragraphs (1) and (2) of Article 56 and paragraphs (1) and (2) of Article 57 concerning on Participation in Crime;
   - Law No. 36 of 1999 concerning on Telecommunications in:
     - paragraph (2) of Article 7 concerning the administration of telecommunications;
     - paragraphs (1), (2), and (3) of Article 18;
     - Article 20 and Article 21 concerning on the Rights and Obligations of Administrators and Communities;
     - paragraphs (1) and (2) of Article 39;
     - Article 41;
     - paragraphs (1) and (2) of Article 42 concerning on Telecommunications Security;
     - paragraph (1) of Article 44 on investigations;
     - paragraphs (1) and (2) 46 concerning on Administrative Sanctions, Article 57 on Criminal Provisions,
Law no. 1 of 2002 concerning on Terrorism in Article 6 on the Criminal Act of Terrorism, Article 27 on Investigation, if Telegram blocking is still implemented then businesspeople cannot invest in Telegram and also to companies that provide features used to download Telegram, and for businesspeople who already provide Telegram application can lose due to blocking of Telegram application.

Telegram has paved the way for crimes related to terrorism for the examples:

a) Case of terror in MH Thamrin area, Central Jakarta, January 2016; the case of the stabbing of the Mobile Brigade personnel at Falatehan Mosque, the alleged offender is known by way of planning an attack on the police;

b) Case of bomb in Kampung Melayu Ad all cases are indicated by terrorist networks using Telegram, and they all have something to do with ISIS network groups that use the view of radicalism.

c) Telegram has been unblocked by the government of Indonesian and agreed on the agreement. If there is the same thing happen, telegram will responsible to ministry of communication and informatics

5.2 Recommendation

Based on the conclusion, author give recommendation to:

a) The government should be consistent in addressing the blocking of the Telegram application.

Whereas in the opinion of the government writer inconsistent blocking telegram, the telegram looks blocked in reopening because of the statement from Pavel Durov as telegram CEO stating that there will be no more content containing radical elements and if in the future there is radical content then telegram will block application in Indonesia and
according to author with revelation alone is not enough. According to government authors have to make specific rules about the use of social media so that in later days radical elements are not found anymore in the content of social media usage.

b) The government should strengthen the Legal Mafia Eradication Task Force in Indonesia so as not to be left behind from other countries and further enhanced the quality of this agency so that crime in cyberspace can be reduced and even overcome.
REFERENCES

BOOKS


A. M., Kaplan, & M. Haenlein. 2010. “*Users of the World, Opportunities of Social Media*”


Chazawi, Adam. 2002. *Indonesian Law Lessons*, Jakarta: Raja Grafindo Persada


Suhariyanto, Budi. 2013. *Information Technology Crime (cybercrime)*, Jakarta: PT Raja Grafindo Persada


**LAW AND REGULATION**

Indonesia Penal Code

Law No. 36 of 1999 concerning on Telecommunication

Law No. 11 of 2008 concerning on Electronic Information and Transaction

Law no. 1 of 2002 concerning on Terrorism

As stated in the Decree of the Minister of Communications and Informatics No. 290 Year 2015

Indonesia, Law on Stipulation of Government Regulation in Lieu of Law no. 1 of 2002 on Combating Terrorism Crimes into Law no. 15, State Gazette No. 45 of 2003, Supplement to State Gazette no. 4284, General Explanation of Government Regulation in Lieu of Law no. 1 of 2002 on Combating Terrorism Crimes of Paragraph two.

Law No. 19 Year 2016 concerning on Amendment Law No. 11 Year 2008 concerning on Infomatic a and Electronic Transaction Article 3
JOURNAL

Federal Bureau of Investigation (FBI), cited by Adam Savino, Cyber Terrorism,

http://www.cybercrimes.net/Terrorism/ct.html, upload on February 15, 2006, and Accessed October 16:00 p.m

Gabriel Weimann, www.terror.net, Now Modern Terrorism Uses the Internet,

http://www.usip.org/pubs/specialreports/srr116.pdf/2017/10/10>, Accessed August 12, 2018 at 2.00 a.m

Mayfield, A. 2008. What is social media? Available at http://www.icrossing.com/uk/sites/default/files_uk/insight_pdf_files/What%20is%20Social%20Media_iCrossing_ebook.pdf, accessed 07 February 2018 at 8:00 p.m


Manjoo, Farhad (July 14, 2008). "Long Tail and Big Heads", accessed on 2,2017 at 20:00 p.m

61


http://jumalapps.co.id/article/12074 uploaded on July 26, 2017 and accessed on December 5, 2017 at 13:00 p.m


INTERNET

https://id.wikipedia.org/wiki/Telegram_(aplikasi), accessed on October 21, 2017 at 5.51 p.m

https://telegram.org/apps, accessed on October 21, 2017 at 6.03 p.m

http://www.definisi-pengertian.com/2015/05/definisi-pengertian-tindak-pidana-kejahatan.html, accessed on October 18, 2017 at 10.00 p.m

Admintrasi Pemerintah, See: http://pemerintah.net/asas-asas-umum-pemerintahan-yang-baik-aupb/ accessed April 3rd, 2018, at 03:32 a.m

See: https://books.google.co.id/books?id=Qx_dCwAAQBAJ&pg=PA361&lpg=PA361&dq=Perkembangan+pesat+dan+kemajuan+Teknologi+Informasi+telah+menyebabkan+perubahan+dalam+aktivitas+kehidupan+manusia+di+berbagai+bidang+yang+secara+langsung+mempengaruhi+kelahiran+bentuk-
bentuk tindakan hukum baru; bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk memelihara, memelihara dan memperkuat persatuan dan integritas nasional berdasarkan pada Hukum dan Peraturan untuk kepentingan nasional.


**ELECTRONIC NEWSPAPER**

Kompas, *3 Upaya Telegram agar Blokir Dicabut di Indonesia*
http://tekno.kompas.com/read/2017/07/16/10215597/3-upaya-telegram-agar-blokir-dicabut-di-indonesia. uploaded on July 16, 2017 at 10.21 a.m accessed on December 5, 2017 at 14.00 p.m

Kompas, *Telegram dan WhatsApp Sama-sama Pakai Enkripsi, Apa Bedanya?*
http://tekno.kompas.com/read/11110067/telegram-dan-whatsapp-sama-sama-pakai-enkripsi-apa-bedanya?-page. uploaded on 15/07/2017 at 11.11 a.m, and accessed on August 1, 2017 at 13.00 p.m

Kompas, *Mengapa Aplikasi Telegram Disukai Teroris?*
http://tekno.kompas.com/read/2017/07/15/08305697/mengapa-aplikasi-telegram-disukai-teroris?-pageall uploaded on October 26, 2016 at 13.30 p.m and accessed on October 15, 2017 at 17.00 p.m

Tempo.co, *Telegram Diblokir, Kemenkominfo: Digunakan Kelompok Radikal*
https://nasional.tempo.com/read/891542/telegram-diblokir-kemenkominfo-digunakan-kelompok-radikal/. uploaded on July 14, 2017 at 20.01 p.m and accessed on October 17, 2017 at 19.21 p.m
The Telegraph, What is Telegram: the new WhatsApp? http://www.telegraph.co.uk/technology/news/10658647/What-is-Telegram-the-new-WhatsApp.html, uploaded on February 25, 2014 at 8.00 a.m. GMT and accessed on October 12, 2017 at 7.00 p.m


Kementrian Komunikasi dan Informatika See:
https://www.kominfo.go.id/content/detail/10533/dari-ekonomi-digital-blokir-konten-hingga-wannacry/0/berita_satker, uploaded September 05, 2017, accessed February 14, 2017 at 04:52 a.m


BBC Indonesia, Seberapa efektif blokir Telegram untuk cegah aksi terorisme? http://www.bbc.com/indonesia/indonesia-40624053, uploaded on July 17, 2017 and accessed on December 7, 2017 at 1.07 a.m

Pebriansyah Ariefana See:
OTHER

Press Release of the Ministry of Communications and Informatics No. 84 / HM / KOMINFO / 07/2017 on Termination of Access to Telegram Applications.

Press Release of the Ministry of Communications and Informatics No. 100 / HM / KOMINFO / 08/2017 on the Minister of Communication and Informatics and CEO of Telegram Discuss Terrorism Handling and Radicalization.

Press Release of the Ministry of Communications and Informatics No. 86/HM/KOMINFO/07/2027 Concerning Recent Developments About Blocking Access to Telegram Application.
Press Release of the Ministry of Communications and Informatics No. 84/HM/KOMINFO/07/2027
Concerning Termination of Access to Telegram Application

On July 14, 2017, the Ministry of Communications and Informatics has requested that the Internet Service Provider (ISP) terminate (block) access to the 11 Domain Name System (DNS) owned by Telegram. This blocking must be done because the many channels in the service are propaganda of radicalism, terrorism, hatred, invitation or means to assemble bombs, how to attack, disturbing images, and others that are contrary to Indonesian laws and regulations.

The 11 DNS that are blocked are as follows: t.me, telegram.me, telegram.org, core-telegram.org, desktop.telegram.org, macos.telegram.org, web.telegram.org, venus.web.telegram.org, pluto-web.telegram.org, flora.web.telegram.org, and flora-1.web.telegram.org. The impact of this blocking is that web version of Telegram service cannot be accessed via computer.

"Currently we are also preparing for the complete closure of the Telegram application in Indonesia if Telegram does not prepare Standard Operating Procedures (SOPs) for handling unlawful content in their applications This step is taken as an effort to maintain the integrity of the Unitary State of the Republic of Indonesia" the Director General of Informatics Application, Samuel A. Pangerapan said.
It further stated that this Telegram application may endanger the security of the country for failing to submit standard operating procedure (SOP) in handling terrorism cases.

The Director General of Informatics Applications also affirms that in carrying out the duties as mandated by Article 40 of Law. 19 of 2016 on Amendment to Law No. 11 of 2008 on Information and Electronic Transactions, the Ministry of Communications and Informatics always coordinates with State institutions and other law enforcement agencies in handling the blocking of content that violates Indonesian laws and regulations.

Jakarta, July 14, 2017
Public Relations Bureau

Ministry of Communications and Informaticn
Press Release of the Ministry of Communications and Informatics No. 100/HM/KOMINFO/08/2027 Concerning Minister of Communications and Informatics and CEO of Telegram Discusses Terrorism Handling and Radicalization

Minister of Communications and Informatics Rudiantara held a meeting with Telegram CEO Pavel Durov at the Office of the Ministry of Communications and Informatics, Tuesday (1/8/2017). This meeting discussed the handling of terrorism issues and radical content that developed in the Telegram platform. This is a follow up of the policy of the Ministry of Communications and Informatics to disable the 11 Domain Name System (DNS) of web-based services of Telegram. The decision taken on July 14, 2017 was once reap criticism from Telegram users in Indonesia. "I appreciate Telegram who is very responsive in addressing this issue", Rudiantara said.

Related to the handling of terrorism issues, Telegram's CEO, Pavel Durov, also has the same commitment. "Telegram is very concerned about the threat of global terrorism, especially to countries like Indonesia, it is important for the Government of Indonesia and Telegram to make a Joint Statement related to this", Durov explained.

As a follow up of this commitment, the Ministry of Communications and Informatics and Telegram agreed to organize and manage the process. Because to face of the threats of terrorism and radicalism, the speed of acting is needed. To that end, both Rudiantara and Pavel Durov agreed that the process will be discussed in a meeting involving the technical team.

The Director General of Informatics Application, Samuel A. Pangerapan, added, "Because of the goodwill and commitment of Telegram to manage and deal with issues that threaten the country through the spread of terrorism issues and content of radicalization, in
accordance with the procedures adopted, the 11 web-based DNS of Telegram will be restored soon. This week will be restored soon", Semmy asserted.

**Chronology of Telegram Blocking**

The decision on the blocking of 11 web-based DNS of Telegram was done after the Ministry of Communications and Informatics sent a request via e-mail, demand for thousands of terrorism and radicalism content spreading in 11 DNS was sent from 29 March 2016 to 11 July 2017. However, all the requests are not addressed. Regarding to that, the CEO of Telegram, PavelDurov, had previously apologized and admitted receiving a communication e-mail from the Ministry of Communications and Informatics on July 16, 2017. To solve the issue, the Ministry of Communications and Informatics invited PavelDurov to come to Indonesia.

Jakarta, August 1, 2017
Public Relations Bureau, Ministry of Communications and Informatics

Related News
Press Release of the Ministry of Communications and Informatics No. 86/HM/KOMINFO/07/2027 Concerning Recent Developments about Blocking Access to Telegram Application

Based on the findings of the Ministry of Communications and Informatics and related Ministries / Institutions there are content that is not in accordance with the legislation especially concerning the spread of radicalism and terrorism. Therefore the Ministry of Communications and Informatics sent a request to Telegram to clear the contents of all channels facilitated by the Telegram. The Ministry of Communications and Informatics has sent emails six times since March 29, 2016 to July 11, 2017 to Telegram. All these emails have been sent and received by Telegram but all the requests have not been addressed. The decision to block thousands of Telegram content was executed after considering the lack of goodwill on the part of Telegram since the 6th e-mail was sent from Tuesday dated July 11, 2017 to Thursday evening of July 13, 2017. In the absence of Telegram's response, the Ministry of Communications and Informatics decided to block the web version of Telegram service containing thousands of content of radicalism and terrorism. The Ministry of Communications and Informatics has ordered all Internet Service Providers (ISPs) to block 11 Domain Name System (DNS) associated with web-based Telegram services. Before making a decision on blocking, the Ministry of Communications and Informatics once again coordinates with all stakeholders addressing the issue of radicalism and terrorism.
Statement of Telegram’s CEO

On Sunday, July 16, 2017 at 7:00 a.m., Telegram CEO on behalf of the Telegram team expressed his apologies and admitted receiving a communication email from the Ministry of Communications and Informatics even though he had previously said he had not received an email report from the Ministry of Communications and Informatics. Furthermore Telegram CEO is committed to open communication channels with the Ministry of Communications and Informatics.

Minister of Communications and Informatics Rudiantara said, “I have received an e-mail about apology from Pavel Durov, CEO of Telegram, apparently he is not aware of several requests from the Ministry of Communications and Informatics since 2016. Durov has followed up on what the Ministry of Communications and Informatics requested and he proposed a special communication to process the handling of negative content especially radicalism / terrorism. I respond to the proposal from Pavel Durov and will follow up as soon as possible from the technical details so that the standard operating procedure (SOP) can be implemented immediately.”

Based on the Telegram CEO's statement, the Ministry of Communications and Informatics followed up with an answer to ask Telegram to prepare technical and administrative teams to support the process of communication and coordination more intensely. The Ministry of Communications and Informatics greatly appreciates Telegram's response, intention, and desire to build cooperation with them.

Follow-up Actions

After communication from Telegram to the Minister of Communication and Informatics, the follow-up is done in the form of technical SOP preparation (process, human resources, organization, etc.):
1. The Government Channel is likely to be made in order to communicate with the Ministry of Communications and Informatics more quickly and efficiently.

2. The Ministry of Communications and Informatics will request to be authorized as Trusted Flagger against accounts and channels in Telegram services.

3. The Ministry of Communications and Informatics will ask Telegram to open representatives in Indonesia.

4. For the process of content filtering governance, the Ministry of Communications and Informatics continues to make improvements in the process, organizing, technical, and human resources.

   The policy aimed at screening for content that is radicalism and terrorism is a follow-up of the handling of issues that threaten the security of the country, especially with the start of geopolitical and geostrategic change in Southeast Asia, especially the events that occurred in Marawi, Southern Philippines. The issue of state security is of particular concern to the President and the President supports the prosecution of contents that could threaten the security of the country.

Jakarta, July 17, 2017

Public Relations Bureau

Ministry of Communication and Information.