Study on The Implementation of The Regulations of Terrorism Activities In Social Media

Angga Dewanto Basari
Student of Terrorism study program, Universitas Indonesia, Jakarta, Indonesia, debe2005@gmail.com

Muhammad Syauqillah
Lecturer of Terrorism study program, Universitas Indonesia, Jakarta, Indonesia, muhamsyasauqillah@ui.ac.id

Asep Usman Ismail
Professor of State Islamic University Syarif Hidayatullah, Jakarta, Indonesia, asep.usman@uinjkt.ac.id

Follow this and additional works at: https://scholarhub.ui.ac.id/jsgs

Part of the Economics Commons, Feminist, Gender, and Sexuality Studies Commons, International and Area Studies Commons, Islamic Studies Commons, Terrorism Studies Commons, and the Urban Studies Commons

Recommended Citation
Basari, Angga Dewanto; Syauqillah, Muhammad; and Ismail, Asep Usman (2020) "Study on The Implementation of The Regulations of Terrorism Activities In Social Media," Journal of Strategic and Global Studies: Vol. 3 : No. 2 , Article 6.
DOI: 10.7454/jsgs.v3i2.1035
Available at: https://scholarhub.ui.ac.id/jsgs/vol3/iss2/6

This Article is brought to you for free and open access by the School of Strategic and Global Studies at UI Scholars Hub. It has been accepted for inclusion in Journal of Strategic and Global Studies by an authorized editor of UI Scholars Hub.
Study on The Implementation of The Regulations of Terrorism Activities In Social Media

Cover Page Footnote

This article is available in Journal of Strategic and Global Studies: https://scholarhub.ui.ac.id/jsgs/vol3/iss2/6
STUDY ON THE IMPLEMENTATION OF THE REGULATIONS OF TERRORISM ACTIVITIES IN SOCIAL MEDIA

Angga Dewanto Basari¹*, Muhamad Syauqillah², and Asep Usman Ismail³

¹ Student of Terrorism study program, Universitas Indonesia, Jakarta, Indonesia*
² Lecturer of Terrorism study program, Universitas Indonesia, Jakarta, Indonesia
³ Professor of State Islamic University Syarif Hidayatullah, Jakarta, Indonesia

Abstract

The legal scope of the Terrorism Law and the Information and Electronic Transactions Law in Indonesia is considered as lacking to cover the problem of cybercrime in social media. Aside from literature review, this paper is also supported by data from direct interview with the Head of Counterterrorism Special Detachment 88 (Densus 88 AT) of Indonesian National Police. The data found out that the Terrorism Law is a repressive response towards terrorism crimes that have already occurred, but less preventive to future crimes. The existence of laws in Indonesia is often one step behind its crime. The difference of perception in seeing a crime also becomes a shortcoming for the legal apparatus, but becomes an opportunity for perpetrators of the crime. Prevention needs to be done as a form of monitoring and controlling the contents that could lead to the criminal acts of terrorism.

Keywords: terrorism, law, social media

* Corresponding author:
  E-mail: ¹debe2005@gmail.com* muhamadsyaquillah@ui.ac.id²
  Affiliation: Student of Terrorism study program, Universitas Indonesia, Jakarta, Indonesia*
1. Introduction

The development of technology, information and communication that occurs rapidly and without limits has impacted everyone in the process of life interaction. The development of this technology is related to the use of information technology that moves by using an internet connection network system. The positive impact of the development of internet technology is to facilitate the acceleration of the available communication and information to achieve the target. The dynamic social life in various events that happen in different parts of the world can be known in a matter of seconds. Current advances in science and technology, in addition to having a positive impact on human life, also brings negative impacts that could do harm to individuals, society, and/or country. One negative impact of the progress of science and technology is its misuse as a medium for committing crimes, especially cybercrime by certain people.

Changes in society in the way they consume media, from conventional mass media to digital (cyber), become a phenomenon in the current digital era. Even Though print media and electronic mass media still exist, the use of online media, such as social media and cyber mass media (online portals), has a high number of enthusiasts in Indonesia. Data from Hootsuit (We Are Social) states that as of January 2020, total internet access in Indonesia is around 174 million people, a rise from 2019 which was 150 million users. Indonesia is at the top three rankings in the growth of global internet penetration. The country is ranked third, preceded by India and China, with a population growth that accesses internet by 25.3 million new internet users in a year, escalated 17% in the past year.

From the number of internet users above, as of January 2020, social media penetration in Indonesia has reached 59% or more than half of the population of internet users in Indonesia. This number grew by 8.1% compared to last year, or equivalent to 12 million new social media users in a year. Popular online activities in Indonesia are social media and chatting applications. The most frequently used social media in Indonesia is Youtube, with the population of 88%, followed by WhatsApp, Facebook, and Instagram. From that number, the most users are the young generation (ages 18-34). The average duration of internet use in Indonesia is 7 hours 59 minutes and the duration of social media usage is 3 hours 46 minutes (Ramadhan, 2020).
The data above illustrates that social media is now a quite dominant service in cyberspace. Interestingly, the power of social media is inevitable given the vision of the internet in the beginning was to connect one person to another. Consequently, the use of social media is intensive and time-consuming. However, the explosive growth of these interconnected devices makes cyberspace a target that qualifies for cybercriminals. Given the high percentage of internet and social media penetration in Indonesia, it is no wonder Indonesia has the potential to become a target of cyber terrorism on social media.

The development of global network of computers or the internet has created a new world called cyberspace, a world of computer-based communication that offers a new reality, namely virtual reality. The term also produces various forms of cyber environments which later gave birth to a new term known as cybercrime. Basically, cybercrime includes traditional crime (which appears in a new form) and new crime that has never happened, so there are no rules that prohibit it. The types of crime between conventional and cybercrime is quite similar, just the dimensions used are different and the loss sometimes are not material (William, 2006). The scope of cyber terrorism seems to follow a general trend of the many real-world phenomena that are replicated online.

Cyber terrorism is known as a use of information and communication technology to facilitate the activities and objectives of terrorism crimes (United Nations Office on Drugs and Crime, 2019). According to data from the Ministry of Communication and Information Technology (2019), they have blocked contents that contained radicalism and terrorism as many as 10,499 contents during 2018. The contents consist of 7,160 contents on Facebook and Instagram, 1,316 contents on Twitter, 677 contents on Youtube, 502 contents in Telegram, 502 contents in file sharing, and 292 contents on website.

Cyber terrorism is a phenomenon that increasingly gains attention at present. One of the reasons is the concern that modern information and communication technology can be used to harm open societies. This also reinforces the idea that terrorists can enter cyberspace and use it as a domain for terrorism crimes (Akhgar, et. Al., 2014). According to Clifford (2006), problems that arise in combating cybercrime are inadequate laws, complexity in investigations, and prosecution of cyber criminals because they are in an online environment which is certainly difficult to trace on a global scale.
Seeing the conditions above, we need a set of rules that specifically regulate computer crime and legal protection against the use of information, media and communication technology in order to develop optimally.

Law No. 15 of 2003 is considered as a legal protection of terrorism which has been long “left behind” with the latest patterns of terrorism activities, especially those that use information and communication technology. After a long period of time, the revision of the terrorism law was finally passed in June 2018, becoming Law No. 5 of 2018 concerning Amendment to Law No. 15 of 2003 about the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism to become Law. The latest terrorism law has an effect on the enforcement of terrorism law, especially in the context of cyber crime.

Although the cyber world is a virtual world, laws are still needed to regulate people's attitudes and behavior, because virtual societies are basically people from the real world. Law No. 19 of 2016 concerning Information and Electronic Transactions only addresses the problem of legal irregularities that lead to cyber crime in general and does not lead to cyber terrorism, such as criminal acts related to illegal activities, interference, facilitating prohibited acts, and falsification of information or electronic documents. Referring to Chapter 1 of General Explanation of ITE Law No. 19 of 2016, as for the elements of crime which are regulated in broad outline only related to Electronic Information and/or Electronic Documents which have contents that violate decency/pornography, online gambling, insults and/or defamation, extortion, spreading of hoax, spreading of hatred, and spreading information and/or threats related to SARA/specific group. Thus, the implementation of regulations on cyber terrorism still relies on Law No. 5 of 2018 as a legal protection for cyber terrorism crimes.

On the other hand, Law No. 5 of 2018 concerning the Criminal Acts of Terrorism is more directed at law enforcement against the activities of radical groups on social media, and less directed on the issue of prevention. Cyber terrorism, which is manifested in various forms of activities, requires more specific provisions considering the adverse effects of cyber terrorism is more dangerous than cyber crime in general.

Several regulations, both at the national and international levels, have organized various aspects of activities on the internet and guaranteed freedom of expression. These
regulations include, among others, the Universal Declaration of Human Rights Article No. 19, the International Covenant on Civil and Political Rights (ICCPR) Article 4 which has been ratified through Law No. 12 of 2005, and The 1945 Constitution of the Republic of Indonesia Article 28E paragraph (3) which guarantees freedom of speech and expression. Then, Law No. 5 of 2018 and Law No. 19 of 2011 also guarantees freedom of information, expression and privacy. Unfortunately, these things are misused to carry out terrorism activities that could lead to threat of terror. The criminal acts of terrorism, especially cyber terrorism, has complex dynamics; the government policies, especially in terms of preventing terrorism, need to adjust to the changes.

2. Literature Review

There are several previous studies regarding the social reaction of the community to terrorism news or videos in cyberspace such as on social media. For instance, in experimental research on the impact of spreading terrorism videos online, the result shows that terrorism committed in cyberspace has the same impact as conventional terrorism in affecting the public's psychology, a sense of insecurity and a decreased trust in the government (Gross, Canetti, & Vashdi, 2017). Furthermore, analysis on social media data of the assassination of soldier Lee Rigby at Woolwich by two offenders who claimed to be God's (Allah SWT) army, found that social media played an important role as a source of major news information for the public in influencing public understanding and perception of terror attacks (The Economic and Social Research Council, 2015, p. 1).

Afterwards, a study shows that there is a non-linear relationship between communication technology and terrorism. As communication technology and facilitates the flow of information in society, terrorism initially increases but then decreases. In particular, monitoring and arresting terrorists has become easier for law enforcement (Mahmood & Jetter, 2019, p. 152). In Indonesia itself, there is a problem of implementing legal synergy between the Indonesian National Police (POLRI) and the Indonesian National Armed Forces (TNI) regarding difference in vision and mission, in which POLRI thought that terrorism must be resolved through the criminal justice system while TNI believes that terrorism is a threat to state sovereignty which must be immediately eradicated (Darma, et. Al., 2018, p. 314).

Meanwhile, other studies show that there is an urgency to enact laws on social media terrorism for various countries, taking into account the right to freedom of speech, expression
and the right to privacy, which is one of the vital issues to establish human rights throughout the world (Hossain, 2018, p. 148). In compliance with this, Greenberg (2016, p. 174) also mentioned that in any counter-radicalization strategy, it is necessary to respect civil liberties (particularly the protection to freedom of speech) through policies at the government and private levels on how the collection of information is carried out, by who, and with what level of criminal responsibility, so there is transparency.

The issue of privacy on social media previously has been highlighted in Europe in the Open Source Intelligent (OSINT) trial, which is an open access technology that analyzing the information data from social media aims to identify lone wolf, child exploitation, copyright infringement, and public sentiment. The result of the research indicates that there are some risks of deprivation of public space on social media related to full access by the police to retrieve sensitive public information, no confirmation of the use of OSINT in the analysis of the police data, and the absence of laws and protocols in online policing, which can lead to criminalization of users (Trottier, 2015, p. 542).

Not only that, research on criticism of The U.K.’s Encouragement of Terrorism offence argues that, first, the concept of indirect encouragement to the acceleration of acts of terrorism is too vague and the scope of violations is too broad, so it is necessary to define clear boundaries of terms; second, the framing of the offence focus on the potential effects of the statements promoting terrorism, rather than on the purpose of the speaker or content creation, has detrimental consequences for freedom of speech and ideological discussion (Macdonald, 2019, p. 11).

3. Research Methodology

This study involves a big role of social media as a significant propaganda media for terror and the implementation of its laws and regulations in Indonesia. Based on this background, the writer is interested to identify the research questions about: "how does the implementation of regulations on terrorism activities on social media carry out?"

In discussing the problem, this study uses empirical juridical methods to see the implementation of normative legal provisions on cyber terrorism regulations on social media in practice in the field, then linked to the applicable laws and regulations. The data were analyzed descriptively in order to systematically compile a picture so that scientific conclusions were obtained which were the answers to the problems posed.
The data sources of this research include primary data and secondary data. Primary data obtained from interviews with the Deputy Chief of Counterterrorism Special Detachment 88 Anti-Terror, Police Brigadier General Marthinus Hukom, S.I.K and regulations of Law No. 19 of 2016 on the Information and Electronic Transactions and Law No. 5 of 2018 on the Eradication of Criminal Acts of Terrorism. The data was obtained by conducting semi-structured in-depth interviews with informant. Then, secondary data comes from academic literature studies.

4. Result and discussion

A. The Development of Terrorism Regulation in Indonesia

Counterterrorism in 1963 carried out through Law No. 11/PNPS/1964 concerning the Eradication of Subversion Activities. During both the old and new order regimes, this law was always used to ensnare terrorism which could be categorized as a subversion activity, in which the majority of the perpetrators were people from Islamic organizations, both on an individual scale and group of pilgrim organizations. The conceptualisation that could capture the criminal acts of terrorism as in Article 1 (1) and Article 19 paragraph (1), which includes actions that could overthrow, damage, or threaten the power of the state or legitimate government authority, disrupting the industry, production, distribution, trading, cooperation or transportation, and sabotage activities. Since its enactment, this subversion law has been challenged by various parties because the formulation of the criminal articles is unclear. In the reformation era, during the reign of President Megawati Sukarnoputri, this subversion law was finally revoked and declared no longer valid (Wiriadinata, 2015).

Since then, terrorism has been limited to be ensnared by articles in the Criminal Code (KUHP). However, the Criminal Code as an existing regulation at that time had not yet been specifically regulated and was not sufficient to eradicate terrorism. Several bombing incidents that occurred in a number of cities, especially the Bali Bombing, were the background for the establishment of a legal protection that regulates the eradication of terrorism. Therefore, the Indonesian government felt it was necessary to establish a Law about combating the terrorism crimes, namely by drafting a Government Regulation in Lieu of Law (Perppu) No. 1 and No. 2 of 2002, which on April 4, 2003 was passed into Law No. 15 of 2003 concerning the Eradication of the Criminal Acts of Terrorism. The use of Perppu No. 2 of 2002 is based on the consideration that the occurrence of terrorism in various regions in Indonesia has caused
material and immaterial losses as well as insecurity for the community. After becoming Law No. 15 of 2003, the regulation has become a legal provision and is coordinative in nature with other laws and regulations relating to combat the terrorism (Zulkifli. 2016).

Law no. 15 of 2003 asserted that terrorism is a criminal act that has political tendency, so that its eradication in the scope of bilateral and multilateral cooperation could be implemented more effectively. The suspect or defendant receives special protection for their rights (safeguarding rules) and also stipulates the threat of particular minimum sanctions to strengthen the deterrent effect for the perpetrators of terrorism crimes (Zulkifli, 2016). The investigation was carried out by Special Detachment 88, known as the Counterterrorism Special Detachment. This special detachment is part of the National Police to execute actions related to operationalization in the field (Zaidan, 2017).

The prevention and eradication of criminal act of terrorism financing is a step that is needed to cut off the development of terrorism groups. Therefore, Law No. 8 of 2010 on the Prevention and Eradication of Criminal Act of Money Laundering and Law No. 9 of 2013 on the Prevention and Eradication of the Criminal Act of Terrorism Financing were made (Windiani, 2017). To oversee financial transaction activities that are suspected to fund terror groups, the Financial Transaction Reports and Analysis Center (PPATK) strengthened the regulation by issuing Presidential Decree No. 13 of 2018 concerning the Principle on Recognizing Beneficial Ownership of Corporations in the Prevention and Eradication of Money Laundering and Criminals Act of Terrorism Financing.

After the terror attacks and bombing on Jalan MH Thamrin, Central Jakarta, on January 14, 2016, all leaders of state institutions at the time agreed that the prevention of terrorism acts must be improved. The Coordinating Minister for Political, Legal, and Security Affairs at the time, Luhut Binsar Panjaitan, asked the DPR to revise Law No. 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism so that the Revision of the Counterterrorism Law is included in the 2016 Priority National Legislation Program (Supriyadi, 2016). Ultimately, the Law concerning the Eradication of Criminal Acts of Terrorism No. 5 of 2018 Amendment to Law No. 15 of 2003 on the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism has been applied as Law.

According to Article 1 paragraph (2) of Law No. 5 of 2018 on the Eradication of Criminal Acts of Terrorism, Terrorism is:
"An act that uses violence or threats of violence which creates widespread atmosphere of terror or fear, resulting in mass casualty, and/or cause damage or destruction to vital strategic objects, the environment, public facilities, or international facilities with ideological, political, or motive for security disturbances."

The US Department of Defense defines terrorism as a strategy in using politically motivated violence to inflict fear with the aim to intimidate the government on political, religious or ideological grounds (Howard et al, 2009). Terrorism emerges because of the existence of radical thoughts that arise due to the spread of radical narratives to targeted people/groups. The thoughts could be in the form of hatred towards the government, the police, and non-Muslims (especially Christians) who are considered to have discriminated Muslims (Riyanta, 2016). The triggers are partly due to religious, ideological, ethnic conflicts, and economic disparity, as well as the obstruction of public communication to the government or because of the idea of separatism and fanaticism (Weinberg et al, 2009).

In the context of terrorist groups affiliated with ISIS, they authorize acts of violence and the content of propaganda spread through doctrine. They consider the doctrine to originate from the teachings of the holy book which they perceive as an obligation to change the religion and belief of all people in the world to become Muslims, both persuasively and repressively. The purpose of uniting all people in the world as Muslims is to establish a caliphate (state) that applies Islamic law. The authorization to implement acts of violence arises when there are parties who oppose the goals of these terrorist groups. Those who oppose to the goals are considered as enemy, therefore, committing acts of violence against them is deemed right (Bernholz, 2017).

**Cyber Terrorism**

On an important note, there is a significant comparison of differences in terms of authority or scope between the old regulations of the terrorism law and the new one. There is no article that regulates terrorism activities in electronic form, such as on social media, in Law No. 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. Meanwhile, in the new Law No. 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, terrorism activities in electronic form are regulated in Article 12B paragraph (3) which reads,

"Any person who intentionally makes, gathers, and/or distributes writings or documents, both electronic and non-electronic for use in training as referred to in
paragraph (1) shall be sentenced to a maximum imprisonment of 3 (three) years and a maximum of 12 (twelve) years."

The latest terrorism law has an effect on the enforcement law of terrorism, especially in the context of cybercrime. Based on the applicable legal principle, the provision of the new regulation erases the enactment of the previous law governing the same legal material and special provisions that override general provisions. Law No. 5 of 2018 concerning the Criminal Acts of Terrorism has ruled out Law No. 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism and Law no. 19 of 2016 concerning Electronic Information and Transactions as the general regulations that regulate cybercrime because it does not yet include cyber terrorism.

Considering the global nature of cyber terrorism crimes at the international level and does not only relies on each country, investigation agencies must cooperate and have international relations so that the investigation process can be carried out quickly, effectively, and rightly. The international legal instruments related to cybercrime is the Convention on Cyber Crime on November 23, 2001 in Budapest (Suharyo, 2010). Certain countries have Law of cyber terrorism as well. For example, India with the Law of Information Technology of 2000, Pakistan with the Law of Prevention of Electronic Crimes of 2016, and Kenya with the Law of Computer Misuse and Cyber Crimes in 2018.

Legal instruments about managing information and electronic transactions and their arrangements are included in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on the Information and Electronic Transactions. There are several revisions in the new IET Law. The amendment is contained in Article 27 paragraph (3) which adds an explanation of the term "distribute, transmit and/or make Electronic Information accessible" and emphasize that the provision is a complaint offense. The next amendment is the reduction of criminal penalty in 2 (two) provisions in Article 29 concerning the provision regarding search, seizure, arrest and detention. Then, changes were also made to Article 31 paragraph (4) regarding the delegation of the procedure preparation for interception into law, Article 5 paragraph (1) and (2) related to the provision on the existence of Electronic Information and/or Electronic Documents, the synchronization of procedural law in Article 43 paragraphs (5) and (6) with the provisions of the procedural law in the Criminal Code, and to strengthen the role of the Civil Servant in Article 43 paragraph (5). Another change was made in adding the provisions regarding "the right to be forgotten" in the Article 26 concerning the
elimination of Electronic Information that is no longer relevant, and the last, the change to strengthen the role of the government in protection to the misuse of information and electronic transactions in Article 40 (Ministry of Education and Culture Higher Education Institution, 2016).

Changes were made in view of the characteristics of cyberspace that allows illegal content, which in Chapter 1 of General Explanation of IET Law No. 19 of 2016 such as Information and/or Electronic Documents with contents that violate decency, gambling, defamation, extortion, spreading hoax, spreading hatred, threats or SARA elements can be accessed, distributed, transmitted, copied, stored for further dissemination from anywhere and anytime.

The IET Law regulates several general cybercrimes in detail, but does not yet regulate cyber terrorism crimes in general. The contents in the IET Law only regulates violations related to decency, gambling, insults, and/or defamation, extortion, and/or threats, but does not yet regulate contents related to cyber terrorism, especially those that lead to propaganda and radicalization.

**B. The Problems of Handling Cyber Terrorism**

The specific characteristics of the internet and social media explain why it is so effectively used by extremist organizations. The easiness and cheap price of the internet access, the existence of anonymity, the absence of traces of perpetrators and eyewitnesses in the virtual world, the use of fictitious/fake identities, as well as the unlimited virtual world are made an advantage for cyber criminals to carry out their actions in reaching a broad target group, but at the same time, also to certain target groups. The simplicity of messaging through social media also makes it suitable to broadcast live reports of ongoing attacks from the battlefield, as done by Al-Shabaab in the Westgate attack in Nairobi, Kenya, in September 2013 (Ginkel, 2015).

Based on the direct interview with the Deputy Chief of Counterterrorism Special Detachment 88, Police Brigadier General Marthinus Hukom, S.I.K. on April 15, 2020, the existence of laws in Indonesia was often a step behind its crime. That means, a law was often drafted after a crime has occurred, which is more of a repressive move than preventive. This terrorism law is no exception. In fact, according to Hukom, acts of terror in Indonesia have
occurred more or less since 1999. For example, the Christmas Eve bombing in 2000, the Atrium and the Santa Anna Church bombing in 2001, as well as several bombings in Ambon and Poso in 2002. Bali Bombing 1 on October 12, 2002 became a turning point for the Indonesian government to issue regulations on criminal acts of terrorism in the Government Regulation in Lieu of Law No. 1 of 2002 before it became Law No. 15 of 2003. For approximately 15 years, from 2003 to 2018, there was no change in the development of this terrorism law. Although, if examined further, the variety of terrorism crimes always follows technological developments. Until finally in 2018, the use of social media went massive. Terrorists no longer carry out propaganda through books, writings or lectures, as they have begun to play their role through social media.

Another problem is that there is often a difference of perception in seeing the crime. Interviewer Police Brigadier General Marthinus Hukom gave an example of how the expression of hatred (hate speech) in Indonesian law is included as a crime. However, American law does not categorize hate speech as a form of crime due to the strong existence of freedom of speech. This is a difficulty when facing a legal process using social media as evidence. It means that the weakness is not only in Indonesian law, but also the result of perspective differences in freedom of speech on the law in each country. As a result, this becomes a shortcoming for the legal apparatus, but becomes an opportunity for perpetrators of the crime.

Then, according to Hukom, there are general crimes which are accommodated in the IET Law. However, if we refer to the perspective of terror through the said Law, then it is against the formal law or procedural law that already exists in the terror law. For that reason, the Law of Terrorism No. 5 of 2018 accommodates the crimes of Information and Technology which indeed happened at that time, but have not been accommodated in Law No. 15 of 2003.

C. The Dilemma between Restrictions on Access and Features of Social Media and Restrictions on the Freedom of Expression

The Network Enforcement Act, known as NetzDG in Germany, requires social media companies to remove content containing hate speech and other illegal content that came into force from January 1, 2018. Reporting from Human Rights Watch, (2018), based on 22 provisions of criminal law, this regulation requires social media platforms such as Facebook,
Instagram, Twitter and YouTube to immediately remove illegal contents; from insults to public officials or institutions to threats of violence, with threat of fines up to 50 million euros.

At least, countries such as Russia, Singapore and the Philippines have directly referred to this law as a positive example in considering similar laws for removing illegal contents on social media. In addition to these countries, there are several other countries that limit the expression of speaking online by forcing social media companies to act as the censors. Venezuela approved The Law against Hate for Peaceful, Coexistence and Tolerance, which imposes high fines on social media platforms who do not remove contents which include propaganda that calls for war or national, racial, political, and other hatreds (AP News, 2017). In Europe, the Governments of the United Kingdom and France have drawn up joint action plans to develop the identification and elimination of online content which is considered by the authorities to be a terrorism, radical or hateful contents contained in the 'French-British Action Plan'. Also, reporting from The Guardian (2018), the Prime Minister of the United Kingdom, Theresa May, also called on social media platforms to improve identification and elimination of terrorism contents.

Meanwhile, according to Human Rights Watch, this new law is considered to be fundamentally flawed because it can result in unaccountable and excessive censorship. This law places a burden on social media companies to make difficult decisions about possible violations of the law, under conditions that encourage restrictions on the expression of content that could be legal. In addition, this law fails to provide a role for judicial oversight or legal effort if a company decision violates a person's right to speak or access information. This law sets a dangerous precedent for governments of other countries who seek to limit online expression by forcing companies to censor on behalf of the government. The Global Network Initiate, a coalition of non-governmental organizations, academics, investors and companies who committed to advancing freedom of expression and online privacy, states that this law “transfers decisions” about freedom of expression to private companies (Human Rights Watch, 2018).

In Indonesia, the government had limited features to send photos and videos on the WhatsApp, Facebook, Twitter, LINE and Instagram. The Ministry of Communication and Information Technology (Kominfo) decided on May 22, 2019, in connection with the demonstration that was carried out by a group of people in front of the Election Supervisory Body (Bawaslu) related to the results of the 2019 General Election. The Minister of
Communication and Information at that time, Rudiantara, stated that the limitation of downloading and uploading media features is done so that the public is not easily provoked by rallies and prevents the spreading of hoaxes. According to the government, the decision to restrict access to social media and chat applications is in accordance with the Information and Electronic Transactions Law (IET Law). Reporting from Liputan 6, a spokesperson for Facebook Indonesia confirmed that it will continue to coordinate with the Indonesian government regarding restrictions on this feature (Jeko, 2019a).

At the same time, according to the ICJR, this restriction is contradicting the right to communicate and obtain information and freedom of expression. Human is a social creature who cannot live alone. We need friends, groups and opinions to improve our life. This has been guaranteed and regulated in the 1945 Constitution, Article 28E paragraph (3), which states, “Each person has the right to freely associate, assemble, and express his opinions.”

In the Universal Declaration of Human Rights, it also regulates the freedom of the individual in expressing his opinion, namely article number 19 which reads,

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”

Later on, reporting from Liputan 6, ICJR deemed that the government was mistaken in limiting access and social media features and chatting applications without prior notice. Article 4 of the International Covenant on Civil and Political Rights (ICCPR) which has been ratified through Law No. 12 of 2005 gives the authority to the state to impose human rights restrictions when the state is in an emergency. The emergencies can occur due to factors from domestic (internal) or foreign (external) in the form of military/armed threats or can also be unarmed threats, such as bomb terror and other emergency situations. In emergencies that threaten the life of the nation, the constitution gives the power to the president or the government to assess and determine whether the state is in an emergency or not (Jeko, 2019b).

Based on the General Comment No. 29 Article 4 of the ICCPR, there are two basic conditions that must be met in order to limit human rights. First, the situation must be an emergency that threatens the life of the nation. Second, the President must officially determine that the country is in an emergency situation through a Presidential Decree. In this
case, clear indicators of restrictions on the actions of human rights should be determined so as not to open up opportunities for abuse at the expense of broader interests. Hence, it is an inappropriate action of the government to restrict access and features of social media and chat applications without prior announcement (Jeko, 2019b).

This is in line with the ‘Program on Extremism: Social Media, Terrorist Content Prohibitions and The Rule of Law’ (MacDonald, 2019), which states that the right to freedom of speech is important in the context of counterterrorism. A clear communication about the restrictions on the prohibition of contents that promote terrorism is important. This is not only useful to ensure that users are given information on their rights and responsibilities for the use of social media platforms and allows them to make decisions based on information about the content they will upload, but also, to limit and guide the policy of the content moderator, thereby, limiting the risk of inconsistent decision making—or even inappropriate.

5. Conclusion

The IET Law No. 19 of 2016 currently only limited to discussing general cybercrimes, and does not cover cybercrime terrorism. Meanwhile, the regulation on terrorism is specifically regulated in the Terrorism Law No. 5 of 2018 and there has been a special agency that handles the criminal acts of terrorism, namely the National Counterterrorism Agency (BNPT), as stipulated in the said law. Unfortunately, the terrorism law is only a repressive response to terrorism crimes that have already occurred; it is not a preventive one. Thus, this does not break the chain of radicalization in the spread of the terrorism through social media.

The Ministry of Communication and Information Technology is guided by international laws that regulate the freedom of information and expression which always promotes the rights to maintain individual’s privacy. As a result, the Ministry does not have complete control over access and features on social media as it is the right of each company that governs its policies, including the anonymity policy on social media that is presented on social media platforms.

The responsibility in monitoring and controlling the contents of radicalism can have a gray effect if carried out by each social media provider, because there are no benchmarks and will have an impact on social and religious issues. Therefore, in this case, the solution is to
have a collaboration between the Ministry of Communication and Information Technology, BNPT, and Densus 88. Kominfo should provide access to BNPT and Densus 88 to oversee and control terrorism activities in social media, so that the benchmarks and tactics can be legally accounted for. As an example, Kominfo, Densus 88, and BNPT can coordinate intensively in controlling the contents with radical issues and terrorism on social media through the steps of early detection of social media accounts and press-like media that are considered worrying. In addition, efforts can also be made by improving the verification protocol when creating accounts on social media. The aim is to prevent the emergence of fake accounts that are used by terror groups, in relation to the problem of anonymity in cyberspace.

Another recommendation for cooperation is for the Ministry of Communication and Information Technology, the National Counterterrorism Agency, the Counterterrorism Special Detachment 88, relevant ministries, social media platform companies and mass media, relevant government/non-government agencies, and community leaders to work together to make counter-narratives of radical and terrorism propaganda made by terror groups. The parties can be involved by carrying out their respective roles simultaneously and integrated. This can be done online (posting writings, pictures or videos on social media and creating websites that contain counter-narrative contents, online literacy training for the public to distinguish radical media) and face-to-face (seminars, workshops, general lectures) which calls for the importance of de-radicalization in Indonesia, so that the objectives of the spreading of terror and fear in terrorism acts fail or can be resisted by the response of internet users in Indonesia.
References

Books
Akhgar, B. et.al. (2014). Cyber crime and cyber terrorism investigator’s handbook. London: Elsevier.

Clifford F, Gray and Erik W Larson. (2006). Project Management: The Managerial Process. McGraw Hill

Eddyono, S.W. et. al. (2016). Catatan kritis atas RUU pemberantasan terorisme tahun 2016, Institute for Criminal Justice Reform.

Howard, R.D., Sawyer, R.L., & Bajema, N.E. (2009). Terrorism and counterterrorism: Understanding the new security environment, 3rd Ed. USA: McGraw-Hill.

MacDonald, S. (2019). Program on extremism: Social media, terrorist content prohibitions and the rule of law. Washington DC: George Washington University.

The Economic and Social Research Council. 2015. Economic and Social Research Council Annual Report and Accounts 2017-2018. Economic and Social Research Council.Polaris House.North Star Avenue.Swindon SN2 1UJ.www.esrc.ukri.org

Widodo E., Supriyadi. 2016. Catatan Kritis Atas RUU Pemberantasan Terorisme Tahun 2016. Institute for Criminal Justice Reform. Jakarta Selatan.

Weinberg, L., Pedahzur, A., & Perliger, A. (2009). Political parties and terrorist groups. Oxon: Routledge.

Articles
Darma, et. al. (2018). Kebijakan formulasi hukum pidana dalam penanggulangan tindak pidana terorisme di Indonesia. Jurnal Daulat Hukum, 1(1), 305-316.

Economic & Social Research Council. (March 2015). Security, terrorism and social media. Evidence Briefing. Swindon, UK: The Economic and Social Research Council.

Gross ML, Canetti D, Vashdi DR. The psychological effects of cyber terrorism. Bull Atom Sci 2016;72:284–91.

Ginkel, van B. (2015). Responding to cyber jihad: Towards an effective counter narrative. International Centre for Counter-Terrorism–The Hague Research Paper, 1-19.

Greenberg, K.J. (2016). Counter-radicalization via the internet. The ANNALS OF The American Academy, 668, 165-179.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49-58.

Hossain, M.S. (2018). Social media and terrorism: Threats and challenges to the modern era. South Asian Survey, 22(2), 136-155.

Macdonald, S. (2019). Social media, terrorist content prohibitions and the rule of law. The George Washington University Program on Extremism, 1-14.
Mahmood, R. & Jetter, M. (2019). Communications technology and terrorism. *Journal of Conflict Resolution, 64*(1), 127-166.

Bernholz, Peter. 2017. Totalitarianism, Terrorism and Supreme Values," Studies in Public Choice. Springer, number 978-3-319-56907-9, December.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies* 2015, 18(4-5), 530–547.

Windiani, R. (2017). Peran Indonesia dalam memerangi terorisme. *Jurnal Ilmu Sosial*, 16(2), 135-152.

Wiriadinata, W. (2015). Peranan aparat penegak hukum dalam penanggulangan terorisme di Indonesia. *Jurnal Hukum dan Pembangunan*, 45(2), 209-228.

Tafoya, William. 2006. *Cyber Crime and Cyber Terrorism (What's New in Criminal Justice)*. Paperback Press.America

Zaidan, M.A. (2017). Pemberantasan tindak pidana terorisme (pendekatan kebijakan kriminal). Paper is presented in the National Seminar of Law, Universitas Negeri Semarang, Semarang.

**Government Documents**

French-British Action Plan. (n.d). [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619333/french_british_action_plan_paris_13_june_2017.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619333/french_british_action_plan_paris_13_june_2017.pdf) accessed on April 29, 2020.

Ministry of Education and Culture Higher Education Institution. (Desember 1, 2016). *Pengesahan RUU perubahan UU ITE menjadi UU no.19 tahun 2016*. [https://lldikti12.ristekdikti.go.id/2016/12/26/undang-undang-nomor-19-tahun-2016-tentang-perubahan-uu-ite.html](https://lldikti12.ristekdikti.go.id/2016/12/26/undang-undang-nomor-19-tahun-2016-tentang-perubahan-uu-ite.html) accessed on April 30, 2020.

Suharyo. (2010). *Laporan penelitian penerapan bantuan timbal balik dalam masalah pidana terhadap kasus-kasus cybercrime*. Jakarta: Badan Pembinaan Hukum Nasional Departemen Hukum dan HAM.

**Thesis**

Zulkifli. (2016). Konseptualisasi dan kontekstualisasi deradikalisasi (soft power) dalam penanganan terorisme dihubungkan dengan undang-undang nomor 15 tahun 2003 tentang pemberantasan tindak pidana terorisme. Tesis. Bandung: Universitas Pasundan, Bandung.

**Laws and regulations**

The Information and Electronic Transactions Law No. 19 of 2016.

The Criminal Procedure Code, No. 8 of 1981.

The Eradication of the Criminal Acts of Terrorism Law No. 5 of 2018 concerning Amendment to Law No. 15 of 2003 about the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism to become Law.
The Eradication of the Criminal Acts of Terrorism Law No. 15 of 2003 about the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002.

**Interview**

Basari, Angga D. (15 April 2020). Personal Interview.

**Internet**

AP News. (November 2017). *Venezuela assembly passes new law clamping down on media*. Accessed via https://apnews.com/d0083a0ce86441358b702e8b53c4eb44 on April 29, 2020.

Ramadhan, B. (February 2020). *Data internet di Indonesia dan perilakunya tahun 2020*. Accessed via https://teknoia.com/data-internet-di-indonesia-dan-perilakunya-880c7bc7cd19 on April 29, 2020.

Human Rights Watch. (2018). *Jerman: Cacat dalam undang-undang media sosial - NetzDG adalah respon keliru terhadap pelecehan daring*. February 14, 2018. Human Rights Watch. Accessed via https://www.hrw.org/id/news/2018/02/14/317098 on April 29, 2020.

Jeko I.R. (Mei 2019a). Akses dan fitur media sosial dibatasi, ini jawaban facebook. *Tech News*. Accessed via https://www.liputan6.com/tekno/read/3973134/akses-dan-fitur-media-sosial-dibatasi-ini-jawaban-facebook on April 29, 2020.

Jeko I.R. (Mei 2019b). ICJR: Pembatasan akses media sosial harus berdasarkan hukum. *Tech News*. Accessed via https://www.liputan6.com/tekno/read/3975635/icjr-pembatasan-akses-media-sosial-harus-berdasarkan-hukum on April 29, 2020.

Ministry of Communication and Information Technology. (May 2019). BNPT: *Internet jadi media penyebarluasan terorisme*. Ministry of Communication and Information Technology. Accessed via https://www.kominfo.go.id/content/detail/18602/bnpt-internet-jadi-media-penyebarluasan-terorisme/0/berita_satker on April 30, 2020.

Riyanta, S. (2016). *Skenario kontra narasi radikalisme di Indonesia*. Accessed via https://www.academia.edu/27215010/Skenario_Kontra_Narasi_Radikalisme_di_Indonesia on April 27, 2020.

United Nations Office on Drugs and Crime. (June 2019). *Module 14: Hacktivism, terrorism, espionage, disinformation campaigns & warfare in cyberspace*. United Nations Office on Drugs and Crime. Accessed via https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html 30 April 2020.

The Guardian. (January 2018). My calls on social media giants to do more to tackle terrorism. *Business*. Accessed via https://www.theguardian.com/business/2018/jan/24/theresa-may-calls-on-social-media-giants-to-do-more-to-tackle-terrorism on April 29, 2020.