The Virtual Jurisdiction to Combating Cyberterrorism in Indonesia

Danrivanto Budhijanto

Abstract

The neo-cyberterrorism crafting their actions by social media platform in a virtual world. There are terrorist materials that flooding from terrorist websites and chat-rooms, and spreads across social media all over the world. They also have high techs and outrages skill to communicate via an "end-to-end" encrypted messaging applications such as WhatsApp or Telegram. Cyberterrorist propagandas and execution attacks not only to bombing a place or public transportation around the city, but they are eager to disrupt international financial transactions, undermine air traffic control systems, alter the formulas of medication at pharmaceutical manufacturers, and sabotage utility systems by intercept and hacking the network and digital data platforms. The policy and legislation will not suit again to respond and combating cyberterrorism. Governments, tech internet industries, and netizen must interplay each their role to combating cyberterrorism with virtual jurisdiction principles. Governments and tech internet firms now broadly accept that they have a common interest in establishing global standards for exchanging data across borders in combating terrorism.

Keywords: cyberterrorism, virtual jurisdiction, legal convergence, messaging application, cyberlaw

Homo Informaticus in Virtual World

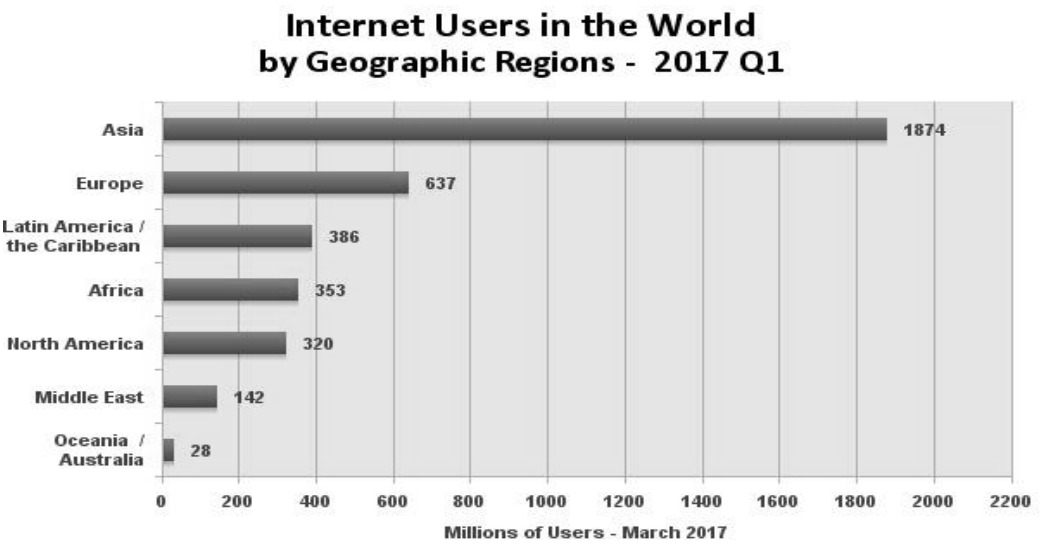
The social use of digital media today becomes a representation of the ultimate mankind evolution, from *Homo Erectus* to Homo *Informat-*

Danrivanto Budhijanto. The Virtual Jurisdiction to Combating Cyberterrorism in Indonesia. *Central European Journal of International and Security Studies* 12, no. 4: 61–80.

icus, [1,2]. humans who had been standing upright enough, to be a man who every waking up in the morning instantly update his or her status in a social media network. Especially with the increasingly extensive users of smartphones and easy access publicly of internet technology by Wi-Fi. Homo *Informaticus* evolution is what makes behavior and culture of people are transforming to the virtual world.

The use of internet technology in the world is a remarkable global phenomenon. Research from Internet World Stats (IWS) up to March in 2017 encountered the facts and data that internet users in the world are 3,739,698,500 of the total population of 7,519,028,970 inhabitants.[3] Most Internet users are in the region of Asia that reaches more than 1 billion users with 50.1% of the total internet users in the world that is 1,874,136,654, whereas in 2006 "new" a number of 364,270,713 users (1.539.6% growth since 2000-2017).

Europe's second largest internet user is 636,971,824 which, in 2006 was 290,121,957 users, followed by Latin America/Caribbean Islands of 385,919,382 whereas in 2006 there were 79,033,597 users, Africa with 353,121 users, 578 which jumped extraordinarily from 2006 which was only 22,737,500, and North America was 320,068,243 whereas in 2006 it was in the third position with 225,801,428 users (with only 8.6% growth since 2000-2017); The Middle East with 141,931,765 users where in 2006 a total of 18,203,500 users; and the last is the area of Oceania and Australia as many as 27,549,054 users compared with the year 2006 number 17,690,762 users.



The total world internet users have achieved nearly 936% growth since 2000-2017. [4] Facts and data from IWS risen an understanding that the use of the Internet technology to be ultra-massive so its needed the identification and objective construction of information technology through the internet's five characters [5,6,7] that *First*, the internet has a global character and knows no national borders/borderless. *Secondly*, each and every internet user can communicate interactively end-to-end and even can perform activities of broadcasting (real-time video) with a relatively low even no-cost and able to independently encrypted (encryption) such as WhatsApp and Telegram. *Third*, no one can claim to be the "owner" of the internet which is a combination of hundreds of thousands of networks and platforms. *Fourthly*, the tremendous growth of Internet users and the rapid development of internet technology itself. *Fifth*, the Internet is not within the scope of a particular state or organizational government so that international cooperation is needed in the effort to overcome the emerging legal issues. Those points make Internet technology as something unique, so it needs to look for policy settings or laws that can be applied sufficiently for information technology activities in virtual jurisdictions.

The neo-cyberterrorism crafting their actions by social media platform in a virtual world. Their terrorist materials that flooding from terrorist websites and chat-rooms, and spreads across social media all over the world. They also have high techs and outrages skill to communicate via an "end-to-end" encrypted messaging application such as WhatsApp or Telegram. The threats of cyberterrorism identify online are twofold. The first is the extremist material that spews from jihadist websites and chat-rooms and spreads across social media, and the second is terrorists' ability to communicate via encrypted messaging apps. Together, they create an online echo chamber that amplifies anti-Western messages and helps propel a few individuals on their journey towards murder. [8,9,10,11].

Cyberterrorist propagandas and execution attacks not only to bombing a place or public transportation around the city, but they are eager to disrupt international financial transactions, undermine air traffic control systems, alter the formulas of medication at pharmaceutical manufacturers, and sabotage utility systems by intercept and hacking the network and digital data platforms. The policy and legislation will not suit again to respond and combating cyberterrorism. Governments, tech internet industries, and netizen must interplay each their

role to combating cyberterrorism with virtual jurisdiction principles. This paper discussing neo-cyberterrorism in virtual jurisdiction theory including neo-cyberterrorism framework in the theory of legal convergence, legal theory on information technology convergence, and the policy and legislation in Indonesia to combating cyberterrorism; neo cyberterrorism vs. information society including neo cyberterrorism vs. Indonesian legislation on cyberlaw, information constitutional rights in Indonesia, and cyberlaw revolution in Indonesia to combating cyberterrorism; and neo cyberterrorism vs. tech-internet platforms.

Neo-Cyberterrorism in Virtual Jurisdiction Theory

Neo-cyberterrorism framework in the theory of legal convergence

Legal Theory is sometimes mistakenly understood as the absolute domain of theorists and academics that only interact with concepts, paradigms, and principles. Often there is a dichotomy of Law Theory as Law in Theory or Law in Books with Legal Practice as Law in Actions or Law in Practices. Legal practitioners often avoid or sometimes "allergic" to the Theory of Law, unless the person is preparing a research for thesis or dissertation report. Globalization led to the convergence of the legal order or the legal system. Legal and economic experts have predicted that the legal order will move in a more adequate direction, they argue that the implications of globalization will force the legal order to converge so as to achieve economic efficiency. [12] This is because the relevant regulatory framework of a legal order will make a legal system alone will not be able to provide an optimal solution of emerging problems [13] Many jurists predicted a similar convergence would occur, especially the lawyers who adhered to the functionalist comparatists believed that the concept of legal unification was desirable and inevitable in a legal order. [14]

Need a more systemic and applicative understanding of the concepts known in the Theory of Law in Indonesia. Mochtar Kusumaatmadja carried the Development Legal Theory in the 1970's with the overall approach of principles, rules, processes, and institutions as the foundation of nation-building. [15] Then in 2009, Satjipto Rahardjo introduced the Progressive Legal Theory with a First understanding, that the law is always placed to seek the basis of endorsement of an act that upholds the procedural features of the basic law and the foundation of the rule; Secondly, that law in development is the instrumental na-

ture of the exchange with forces outside the law so that law becomes a means of social engineering. [16,17,18].

Romli Atmasasmita in 2012 published a book entitled Integrative Legal Theory, which understands the function and role of law as a means of unifying and strengthening the solidarity of society and bureaucracy in facing the development and dynamics of life, both within the scope of Republic of Indonesia and within the scope of international development. [19] Atmasasmita asserted that Integrative Legal Theory should be understood in the dynamic sense, not quo and passive status, but has the mobility of function and its role actively in accordance with the development of national and international society condition from time to time.

The Theory of Legal Convergence is a conceptual and theoretical understanding of authors of the convergence of technological, economic, and legal variables on human and digital relationships in the Digital Information Age, both at national, regional and international levels. [20] The paradigm of the convergence of the legal order can be made a deeper understanding by examining the concept of convergence and conception of non-convergence of law. An approach to finding a relation to the similarities or differences between legal systems, or comparing different legal systems is expected to explain the importance of the conception of legal convergence.

Legal theory on information technology convergence

The term "convergence" is understood to be the process of a condition that closely connects the technological change factor and the factor of increasing the scope of the economy directly, encountered by two or more products or services previously held by several separate corporate entities then organized by a single corporate entity the same one. [21] Understanding convergence in technology is that key converging technologies are generally classified as telecommunications or communication, computerized or computing, and content or content. [22] The convergence of information and communication technology (ICT) includes the integration of hardware and information technology software into telecommunication systems, network digitization, and Internet network enhancement. [23] Understanding convergence even includes things outside the technology, such as the symptoms of convergence between economic systems and the pattern of constitutional arrangements regarding the dynamics of the economy in society.

Information and communication technology (ICT) can be categorized into telecommunication technology, broadcasting technology, and information technology application. [24] In the sectorial industries of telecommunications (telecommunications/communication), computing (broadcasting) is indicated that causing the convergence of the three industries are several factors as follows:

a. Digitalization technology;
b. Declining prices of computing devices;
c. Reduced costs arising from the use of frequency or bandwidth; and
d. Competition of the telecommunications industry.

The technological change factor known as digitalisation/digitalization is a process of transitioning from analogue technology to digital technology and delivering information in an analogue format to binary format, it has enabled all forms of information (voice, data, and video) to be delivered across different network platform types. In the past, telephone networks were only designed for transmissions from two types of services limited to voice and data delivery, and broadcasting networks were restricted to one-way transmission for video viewing using the radio spectrum

Digitization has rapidly changed the conditions of the network platforms. The telecommunications and broadcasting networks become unified in its services. Telecommunication networks and broadcast networks today have the ability to carry two-way transmission simultaneously for voice, data, and video. Digital compression technology has also increased the capacity to carry information inside the network and allow more information to be transmitted over the same bandwidth or spectrum. The change in technology has led to the creation of new, interactive services, multimedia services such as video on demand, teleshopping, telebanking and interactive games as well as broadband, high-speed information and communication information systems (information superhighways).

Interactivity is a distinguishing characteristic of technological convergence in a network service both telecommunications and broadcasting. Further distinguishing characteristic of convergence is the user electronic devices that evolves overwhelmingly over time such as (TV, computer, mobile phone, smartphone) capable of delivering simultaneously services for voice, data and videos for its users.

Research Method

The research method used in this research is analytical descriptive that is by describing and analyzing data obtained in the form of secondary data and supported by primary data about various issues related to the policy and legislation responding and combating cyberterrorism in the framework of information and communication technology.

Related with the field of Legal Studies, the approach used in this study is a normative jurisdiction with emphasis on literature study to examine the meaning, purpose, and existence of policy and legislations responding and combating cyberterrorism. This research is reassurance by Legal History, the Comparative Law and the Legal Futurisctic methods. [25]

This study uses legal materials both primary and secondary law materials and tertiary law. [26] Primary Legal Material is a binding legal material in the form of norms or basic rules. Secondary Law Material is a legal material that provides an explanation of Primary Legal Material that can help analyze and understand the Primary Law Material in the form of research results, the writings of experts in the field of law both in national and international, and journals obtained through literature studies related with Cyberlaw, telecommunications law, broadcast media law, intellectual property law, and other fields of science related to policy and legislation responding and combating cyberterrorism. Tertiary Law Material is legal material provide guidance and information to Primary and Secondary Law Material that is dictionary law, a dictionary of information technology, encyclopedia. Data collection techniques used research stages in the form of Library Research and Virtual Research. [27]

The policy and legislation in Indonesia to combating cyberterrorism

Neo cyberterrorism vs. information society

The term "information" according to the linguistic is illumination; information; news or notice. [28] The definition of information is very rarely understood today. Often easily information is understood as the contents or contents of a daily document can be found. Information conveyed through printed media and electronic media is one such example. Indonesian society today is a community that is very hungry for any digital information that appears on the screen of the smartphone through social media, if not want to be said as "social media-junkies".

Indonesia's reformation era since 1998 pushed the movement of information into an almost uncontrollable freedom, where previously information became expensive and sometimes even non-halal (forbidden, sin). The amendment of several amendments to the 1945 Constitution and the enactment of Law Number 39 of 1999 on Human Rights contributed to the protection of fundamental rights for the people of Indonesia. Article 28F of the Second Amendment of the 1945 Constitution contains that "Every person shall have the right to communicate and obtain information to develop his / her personal and social environment, and shall have the right to seek, obtain, possess, store, process and convey information using any available channel."

Freedom of information is closely related to the understanding of personal rights or private rights or privacy rights. Freedom of information is a fundamental right that must come to an end when there is a line of embarkation on the protection of private rights. Therefore, the protection of the constitutional rights of information as contained in Article 28F of the 1945 Constitution should also be understood by other constitutional mandates which are also contained in Article 28J of the 1945 Constitution Paragraph (2) that stated "In exercising their rights and freedoms, everyone shall be subject to the restrictions laid down by law with the sole intent of ensuring the recognition and respect of the rights and freedoms of others and to fulfill fair demands in accordance with moral judgment, religious values, Security, and public order in a democratic society". Even in the United States, freedom of information is not permitted to violate the personal rights of any person. When the Freedom of Information Act was enacted in 1974, at the same time the Privacy Act was enacted by the United States Government. [29]

The international community itself gives recognition to the protection of private rights. Privacy is a human right, as contained in Article 12 of The Universal Declaration of Human Rights-1948, namely "No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack his honor or reputation. Everyone has the right to the protection of the Law such as interferences or attacks."

It is difficult to find a universal definition to explain what is meant by "privacy". Privacy relates to the various forms of how a human gives access to others to obtain his personal information, partaking of private ownership and personal decisions. [30] Privacy is also understood as

a state to be free of public attention that may affect or interfere with one's actions or decisions. [31] In its recent understanding, privacy is not only protected by law but also by cultural, ethical and business/professional norms.

Personal rights or privacy rights (Privacy Rights) can be interpreted as an autonomous right owned by a person. Privacy or for a general right of personal autonomy, but the Supreme Court has repeatedly ruled that a right of personal autonomy is implied in the "zones of privacy" created by specific constitutional guarantees. In early definition, Privacy Right is the right to be let alone; the right of a person to be free from unwarranted publicity that right of privacy is the right to personal autonomy.

The U.S. Constitution does not explicitly provide for a right of privacy is generic term encompassing various rights recognized to be inherent in the concept of ordered liberty, and such right prevent governmental interference in intimate personal relationships or activities, freedoms of the individual to make fundamental choices involving himself, his family, and his relationship with others. The public has an obligation to create protection for rights violations in the form of disclosures, publicity and the disruption of personal and identity determination. In the United States, "privacy" and "privacy rights" have tremendous value.

The protection of personal rights or private rights will enhance human values; Enhance the relationship between individuals and their communities; Increase independence or autonomy to exercise control and gain appropriateness; Increase tolerance and keep away from discriminatory treatment and limit the power of government. Today informational privacy become importantly sensitive in the virtual world, as informational privacy is a private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others, esp. sensitive and confidential information [32]

The phenomenon of 'privacy' as described indicates one of the arguments of the importance of regulating the utilization of information and communication technology (ICT) in legal understanding. Increasing the application of information and communication technology (ICT) or also known as Information and Communication Technology (ICT), especially through telecommunication activities continuously transform local, national, regional and international economies into the networked economy which is the basis for the formation of the information society.

Big Data has a massive character and escalated because of the ease and speed of access to information technology or internet media. With just one touch it can spread the data widely and change in various formats in a short time. Government R.I. Seeks to encourage and protect social media personnel to stay safe and comfortable surfing in the virtual world, through legislation instruments namely Law Number 11 Year 2008 on Information and Electronic Transactions (UU ITE 2008) and Law Number 19 Year 2016 on Amendment to Law -Indonesia Number 11 Year 2008 on Information and Electronic Transactions (UU ITE 2016). Revision of the ITE Act in 2016 as evidence of the support of respected representatives of the people at the House of Representatives R.I. To the Government to exercise the rule of law and governance of virtual jurisdictions. The government is obliged to protect all Indonesian people in the virtual world or cyberspace. The state still has virtual jurisdiction that cannot be reduced and no one can commit a crime without being punished by law.

Neo cyberterrorism vs. Indonesian legislation on cyberlaw. Information Constitutional Rights in Indonesia

The recognition of independence expresses the mind and freedom of opinion as well as the right to obtain information through the use and utilization of Information and Communication Technology (ICT) objective to promoting the general welfare, and the intellectual life of the nation as well as providing a sense of security, justice, and legal certainty for users and Electronic System Providers. In the life of society, nation and state, the rights and freedoms through the use and utilization of ICT are conducted considering the limitations established by law with the sole intent of ensuring the recognition and respect for the rights and freedoms of others, and to fulfil the fairness accordance with moral considerations, religious values, security, and public order in a democratic society.

Law Number 11 Year 2008 as revised by Law Number 19 Year 2016 on Information and Electronic Transactions (Indonesian Cyber Law 2008 and 2016) is the first legislation in the field of Information Technology and Electronic Transactions as a much-needed legislative product and has become a pioneer that lays the foundation of the arrangement in the field of utilization of Information Technology and Electronic Transactions. However, in reality, the implementation of the Indonesian Cyber Law 2008 is experiencing problems.

Firstly, the Indonesian Cyber Law 2008 has been filed 4 (four) judicial review at the Constitutional Court with the Decision of the Constitutional Court Number 50/PUU-VI/2008, Number 2/PUU-VIII/2009, Number 5/PUU-VII/2010, and Number 20/PUU-XIV/2016.

The decision of the Constitutional Court Number 50/PUU-VI/2008 and Number 2/PUU-VIII/2009 ruled that defamation and defamation in the field of Electronic Information and Electronic Transactions is not merely a general crime but as an offense. The affirmation of the offense of complaint is intended to be in equilibrium with the principle of legal certainty and sense of social justice.

The decision of the Constitutional Court Number 5/PUU-VII/2010 contains the opinion of the Court that the interception and interception authority is very sensitive because on the one hand it is a limitation of human rights, but on the other hand, has the aspect of legal interest (interception as an instrument of enforcement Law-lawful interception). The opinion of the Court is meant to make the regulation concerning the legality of interception shall be established and formulated in accordance with the Constitution of the Republic of Indonesia Year 1945. The Constitutional Court is of the opinion that since the interception is a violation of human rights as stipulated in Article 28J paragraph (2) of the 1945 Constitution of the State of the Republic of Indonesia, so it is reasonable and appropriate that if the State wishes to deviate from the privacy rights of those citizens, the State must deviate in legislation instrument and not in the form of government regulation instrument.

The decision of the Constitutional Court Number 20/PUU-XIV/2016 contains the opinion of the Court that in order to prevent any differences in interpretation of Article 5 paragraph (1) and paragraph (21) of the Indonesian Cyber Law 2008, the Constitutional Court stipulates that every interception must be a lawful process as a lawful interception. The Court in its ruling adds a word or phrase "in particular" to the phrase "Electronic Information and/or Electronic Documents". It is intended that there will be no interpretation that the decision will narrow the meaning or meaning contained in Article 5 paragraph (1) and paragraph (2) of Indonesian Cyber Law 2008, to afford legal certainty of the existence of Electronic Information and/or Electronic Document as legal evidence need to be emphasized in the Elucidation of Article 5 of the Indonesian Cyber Law 2008.

Secondly, the provisions of searches, seizures, arrests, and detentions provided for in the 1 Indonesian Cyber Law 2008 affectation

problems for law investigators because criminal offenses in the field of Information Technology and Electronic Transactions are so rapid and perpetrators can easily obscure acts or evidence of a crime.

Thirdly, the characteristics of cyberspace virtues allow for illegal content such as Electronic Information and/or Documents with content that violates decency, gambling, defamation or defamation, extortion and/or threats, disseminating false and misleading news (hoax) resulting in consumer losses in Electronic Transactions. Including as well as acts of spreading hatred or hostility based on tribe, religion, race, and class, and the sending of personally targeted violence or intimidating threats accessible, distributed, transmitted, copied, stored for re-dissemination from anywhere and anytime in electronic platform. Efforts to protect the public interest from all types of disruptions resulting from the misuse of Electronic Information and Electronic Transactions, it is necessary to affirm the role of the Government in preventing the dissemination of illegal content by taking action on the termination of access to Electronic Information and/or Electronic Documents, which have unlawful content inaccessible from Indonesia jurisdiction and the authority of the law investigator to request information contained in the Electronic Systems Provider for the interest of criminal law enforcement in the field of Information Technology and Electronic Transactions.

Fourth, the use of any information via the electronic media or electronic systems in regard to the personal data shall be made with the consent of the person concerned. It is, therefore, necessary to guarantee the fulfillment of personal data protection by requiring any Electronic System Provider to remove any irrelevant Electronic Information and/or Electronic Documents under its control at the request of the Person concerned by judicial appointment as known as "the right to be forgotten".

Based on above considerations and understandings it crucial to establish Laws on Amendments to Law Number 11 Year 2008 on Information and Electronic Transactions which reaffirm the provisions of the existence of Electronic Information and/or Electronic Documents in the Elucidation of Article 5, Electronic and/or Electronic Documents that are not relevant in Article 26, amend the provisions of Article 31 paragraph (41) concerning the delegation of arrangement of interception procedures into law, increasing the Government's role in preventing the dissemination and use of Electronic Information and/

or Electronic Documents have the illegal content prohibited in Article 40, amend some provisions concerning legal investigations relating to alleged criminal offenses in the field of Information Technology and Electronic Transactions in Article 43, and add to the elucidation of Article 27 paragraph (1), paragraph (3) and paragraph (4) to be more tuneful with the criminal law system legislated in Indonesia.

Cyberlaw revolution in Indonesia to combating cyberterrorism

The Republic of Indonesia Government authorizes power to the Ministry of Communications and Information Technology to discuss and draft the revision of Indonesian Cyberlaw 2008. Law Number 19 the Year 2016 as a revision of Indonesian Cyberlaw 2008 has been approved by the House of Representatives of the Republic of Indonesia (DPR-RI) for prompts are mostly highlighted only in terms of time of presence (Indonesian Cyberlaw 2016).

Since it was enacted in late November, with a political atmosphere that was warming after Muslim action on November 4 and by December 2, 2016, the revised Indonesian Cyberlaw 2008 was considered a legislative product to respond or even restrain the free speech. In fact, its name is a revision; the revised Indonesian Cyberlaw 2008 is not a completely new law. Moreover, the government uses for political purposes only briefly or to protect the interests of people and public interests.

If it is possible to reverse, the Indonesian Cyberlaw 2008 start out from the fact that the use of information technology should contribute to the enhancement of socio-economic welfare and encourage the achievement of the purposes of the state establishment. But not least, it raises the complexity of issues from the technical implementation such as the expanse of development, economics, law, and culture in society. Based on these understanding in Indonesian Cyberlaw 2008 was issued as the first legislation on Information Technology and Electronic Transactions as a pioneering legislative product in laying the basis of regulation and protection in the area of Information Technology and Transactions Electronics. But in its dynamic environment of Information Technology, it is necessary to fine-tune the needs and development of information society in Indonesia. Some legal cases based on Article 27 Paragraph 3 Indonesian Cyberlaw 2008 are often sued and questioned primarily regarding the threat of criminal sanctions set forth in Article 45 Paragraph 1 Indonesian Cyberlaw 2008.

The intention to revise the Indonesian Cyberlaw 2008 has come to light since 2009. That is, only a year after the Indonesian Cyberlaw 2008 was enacted has come to the idea of the revision as a result of the numerous cases that triggered controversy in relation with the idea/mind expression in digital form. Since 2009 it is also the Revision Bill of Indonesian Cyberlaw 2008 is included in the listed of the 2010-2014 National Legislation Program on the initiative of the House of Representatives. In 2010 up to 2011, the Government of R.I. starting to discuss the bill to revised Indonesian Cyberlaw 2008 through an inter-ministerial team as well as the harmonization process in the Ministry of Justice and Human Rights. This process has been completed in 2012. But in 2013, the draft amendment to the Indonesian Cyberlaw 2008 was harmonized from the list of priority legislative discussions in 2014.

Once received the mandate from the Parliament, the Government of President Joko Widodo and Vice President Jusuf Kalla fully agree that such revision should be a priority to present more just rules and prevent criminalization of freedom of speech as well delivery fair opinion in a digital platform. On February 9, 2015, again the Revised Bill on Indonesian Cyber Law 2008 was submitted by the House of Representatives into a priority bill to be discussed in 2015 along with 36 other bills.

Finally, after going through various meetings and deep discussions of inter-ministerial and institutional harmonization, President Joko Widodo formally submitted the draft of Revised Bill on Indonesian Cyber Law 2008 to the Speaker of the House of Representatives R.I. with Presidential Letter No. R-79/Pres/12/2015, dated December 21, 2015. The Presidential Letter comprehends the governmental assignment of President R.I. to the Minister of Communication and Information Technology, and the Minister of Law and Human Rights, both individually and jointly to represent the President to discuss the Bill and get mutual consent with the House of Representatives.

On March 14, 2016, all political party legislative chambers in the First Commission on House of Representatives agreed to discuss the revision of Indonesian Cyber Law 2008 and come out of with the formation of the Working Committee to discuss in detail the contents of such revision. Mrs. Meutya Hafid, Vice Chairman of First Commission of the House who presided over the meeting at that time, confirmed that all political party legislative chambers had agreed to discuss the

revision of Indonesian Cyber Law 2008 to Working Committee level and form of such Working Committee with membership including representatives of all legislative chambers in First Commission of the House. The approval of the First Commission of the House included the importance of the discussion of the substantial norm namely the threat of criminal sanction Article 27 paragraph 3 of the Indonesian Cyber Law 2008. Mrs. Evita Nursanty as a member of First Commission of the House, in her general opinion, that in the revision need to be supported arrangements about the threat of punishment so that one cannot be arrested and detained on charges of fault. Nevertheless, there must still be a minimum penalty for the offender so as to afford a deterrent effect.

Subsequently, a series of meetings between the Government and Working Committee of First Commission was held in the form of working meetings, working committees, collaboration team, and drafting team. By such process, the team received much essential input and aspirations from non-governmental organizations (NGOs), academics, practitioners, and other society elements. Finally, the Bill has been finalized in the discussion of First Level on October 20, 2016, with the decision to agree to be forwarded to the next stage of Decision Making or Second Level Discussion in the House of Representatives Plenary Meeting.

The ultimate result happened at the Plenary Session on October 27, 2016, when the House of Representatives approved the Bill on the Amendment of Indonesian Cyber Law 2008 as Law. This above Law was officially signed by President Joko Widodo as Law Number 16 of 2016 and officially enacted on November 25, 2016.

Understanding the current situation, Indonesian Government is grateful that Indonesian Cyber Law have had the Law since 2008. Almost all of the Indonesian people are feeling lately, that the social media situation is filled with defamation, hoax, unfounded slander between the conflicting parties. The President himself took the initiative to hold a Specific Limited Administration Meeting at the end of 2016 to discuss the anticipated developments in social media related to these latest developments. During this time President Joko Widodo who is known as a very tolerant of freedom of expression in cyberspace, let alone He himself is also very familiar with and is an active communicator in, social media. However, with the increased tension and potential for social media outrage, the President felt important

as well and saw the need to strengthen law enforcement for anyone involved with independent judgment. The Government are even more grateful that thanks to the cooperation of the House of Representatives (especially the First Commission) and the assistance of thought from all stakeholders in the community, the new Indonesian Cyber-law 2016 was successfully revised on time as the pressure intensified to provide improved principles of justice which are better for Indonesian people.

There are at least 5 (five) important and new legislation norms that formulate the Indonesian Cyber Law 2016 relevant to the fulfillment of a wisdom of justice for people who use the virtual world as a place to express opinions, as follows:

First, to avoid imprisonment by reducing imprisonment from 6 (six) years to 4 (four) years. With this decrease in threats, the plaintiff parties and defendant(s) have the same legal position until it can be proven in the court litigation process. The defendant(s) need not be detained in advance because of the imprisonment under 5 years.

Second, adding provisions on "the right to be forgotten" to the provisions of Article 26 of the Indonesian Cyber Law 2016. In the future, the Operator of Electronic Systems shall remove the irrelevant Electronic Information which is under its control at the request of the person concerned based on the court's award and provide such of motion procedural.

Third, protect the public from illegal and unlawful content with two ways, namely protection in terms of access restrictions and in terms of education. In terms of content, the government always gets input from various parties, especially related to pornographic content and gambling.

Fourth, is to accommodate the decision of the Constitutional Court by altering the procedural of lawful interception or intercepts, from those previously stipulated in a Government Regulation to be regulated in legislation instrument.

Fifthly, the declaration that legal evidence of the interception result is an interception conducted in the context of law enforcement at the request of law enforcement officers.

Law Number 19 of 2016 on Amendment of Law Number 8 the Year 2011 on Information and Electronic Transactions authorized and enacted by the Government R.I. on November 25, 2016 as published in the State Gazette of the Republic of Indonesia Year 2016 Number 251

and documented in Supplement to the State Gazette of the Republic of Indonesia Number 5952.

Neo cyberterrorism vs. tech-internet platforms

The Virtual Jurisdiction to Combating Cyberterrorism

Governments, tech internet industries, and netizen must interplay each their role to combating cyberterrorism with virtual jurisdiction principles. Governments and tech internet firms now broadly accept that they have a common interest in establishing global standards for exchanging data across borders in combating terrorism.

Fears that the internet is promoting and enabling Islamist terrorism are not new. But they have become sharper since 2014 when IS established its "caliphate" in parts of Syria and Iraq. It has put much more effort than its older rival, al-Qaeda, into creating sophisticated online propaganda, which it uses to recruit, promote its ideology and trumpet its social and military achievements. It puts as much attention into digital marketing as any big company, says Andrew Trabulsi of the Institute for the Future, a non-profit research group, "It's a conversion funnel, in the same way, you would think of online advertising." [33]

IS's media operation was portrayed in a report published in 2015 for the Quilliam Foundation, a counter-extremism think-tank in London. "Documenting the Virtual Caliphate" described an outlet that released nearly 40 items a day, in many languages, ranging from videos of battlefield triumphs and "martyrdom" to documentaries extolling the joys of life in the caliphate. Each *wilayat* or province of the caliphate has its own media team producing local content. Unlike al-Qaeda, which aims its messages at individual terror cells, IS uses mainstream digital platforms to build social networks and "crowdsource" terrorist acts. [34]

Its Twitter supporters play whack-a-mole with moderators, setting up new accounts as fast as old ones are shut down. Some accounts broadcast original content; others promote the new accounts that replace suspended ones; others retweet the most compelling material. [35] When the Islamic State's releases a new recruitment video, its supporters spring into action. Rita Katz of the SITE Intelligence Group, a Washington-based firm that tracks global terror networks, analyzed what happened to "And You Will Be Superior", a 35-minute video released in March that follows suicide-bombers, from a doctor to a disabled fighter to a child. [36] Translators, promoters, social-media leaders and link-creators joined together to promote it across the internet. One of these groups, the Upload Knights, creates hundreds of links

daily across streaming and file-sharing sites. Ms. Katz found that in the two days after the film's release, it distributed the video with 136 unique links to Google services (69 for YouTube, 54 for Google Drive and 13 for Google Photos). [37]

Conclusion

Further progress will require joint action by internet firms and governments. The fear laws along the lines of one recently acted in Germany that would see those fined vast sums unless they speedily remove any content that has been flagged as hate speech. They also have a growing commercial interest in cracking down on terrorist content, which hurts their brands and could cut revenue. In recent months some of YouTube's clients pulled their ads after realizing that they were appearing next to extremist videos. Greater legal certainty, less confrontation and more co-operation between governments and firms will not drive jihadist propaganda off the internet altogether. But they should clear the worst material from big sites, help stop some terrorists—and absolve tech firms from the charge of complicity with evil.

Acknowledgment

All materials in this article are based on references from scholarly writings in the form of books, scientific journals, research reports, dictionaries and other writing documents in which all copyright inherent is fully protected by law for its author(s).

Notes

1 Der Spiegel Magazine, 5/2006
2 Dong L and Keshavjee K (2016), 'Why Is Information Governance Important For Electronic Healthcare Systems? A Canadian Experience,' ***Journal of Advances in Humanities and Social Sciences*** 2(5), p. 250-260.
3 Internet World Stats Miniwatts Marketing Group (2017), 'Internet World State,' available at: www.internetworldstats.com/stats.htm (accessed 15 January 2018).
4 Internet World Stats Miniwatts Marketing Group (2017), 'Internet Usage Statistic,' available at: www.internetworldstats.com/stats.htm (accessed 15 January 2018).
5 Danrivanto Budhijanto (2017), '***BIG DATA: Legislasi dan Regulasi***,' Bandung: LoGoz Publishing, pp. 25-27.
6 Kongmanus K (2016), 'Development Of Project-Based Learning Model To Enhance Educational Media Business Ability For Undergraduate Students In Educational Technology And Communications Program,' ***Journal of Advances in Humanities and Social Sciences*** 2(5), p. 287-296.

7 V Charoensuk and D Jaipetch (2017), 'Attitudes toward English: A study of first-year students at King Mongkut's University of Technology North Bangkok,' ***Journal of Advances in Humanities and Social Sciences*** 3(1), p. 42-57, 2017.
8 Terror and the Internet (2017), 'The Economist,' p. 52-54.
9 Purba CS and Martono D (2017), 'Local Act Draft Model On Development, Control, And Telecommunication Tower Supervision,' ***International Journal of Humanities, Arts and Social Sciences*** 3(5), p. 231-240.
10 Destiwati R (2015), 'Smoking On Campus: A Review Of Communication Among Student Smokers,' ***International Journal of Humanities, Arts and Social Sciences*** 1(3), p. 127-129.
11 Achaleke HF (2018), 'Integrated Learning Of Integrated Marking Communication In Ubon Ratchathani University Thailand,' ***Journal of Advanced Research in Social Sciences and Humanities*** 3(1), p. 31-36
12 Ian Brown and Christopher T. Marsden (2013), '***Regulating Code: Good Governance and Better Regulation in the Information Age***,' Cambridge: MIT Press Ltd, pp. 89-90.
13 Gregory N. Mandel (2007) 'History Lessons for a General Theory of Law and Technology', ***Minnesota Journal of Law in Science and Technology*** 8(20), p. 2-3.
14 Ian Brown and Christopher T. Marsden (2013), '***Regulating Code: Good Governance and Better Regulation in the Information Age***,' Cambridge: MIT Press Ltd.
15 Mochtar Kusumaatmadja (1976), '***Hukum dan Masyarakat dan Pembinaan Hukum Nasional***,' Bandung: Lembaga Penelitian Hukum dan Kriminologi Fakultas Hukum Universitas Padjadjaran-Penerbit BinaciptaKusumaatmadja.
16 Sudikno Mertokusumo (2012), '***Teori Hukum***,'Yogyakarta: Penerbit Cahaya Atma Pustaka
17 Azhar M (2015), 'The Concept Of Religious Democracy As A New Political Philosophy For Countries With Moslem Predominant,' ***Journal of Advances in Humanities and Social Sciences*** 1(1), p. 19-28.
18 Kim H (2016), Political correctness on David Mamet's Oleanna,' ***Journal of Advances in Humanities and Social Sciences*** 2(3), p. 195-203.
19 Romli Atmasasmita (2012), ***Teori Hukum Integratif: Rekonstruksi terhadap Teori Hukum Pembangunan dan Teori Hukum Progresif***, Yogyakarta: Genta Publishing, pp. 47.
20 Danrivanto Budhijanto (2015), ***Teori Hukum Konvergensi***, Bandung: Refika Aditama, pp. 31.
21 Special Issue Ten (2013), 'Breakthrough Technologies,' ***MIT Technology Review*** 116(3).
22 Eric Schmidt and Jared Cohen (2014), ***The New Digital Age: Transforming Nations, Businesses, and Our Lives***, New York: Alfred A. Knopf.
23 Your Connected Life (2017), ***MIT Technology Review***, Special Edition October.
24 Danrivanto Budhijanto (2010), ***Hukum Telekomunikasi, Penyiaran, dan Teknologi Informasi: Regulasi dan Konvergensi***, Bandung: Refika Aditama.
25 Sunaryati Hartono (2006) ***Penelitian Hukum di Indonesia pada Akhir Abad Ke-20***, Bandung: Alumni
26 Soerjono Soekanto (1986), ***Pengantar Penelitian Hukum***, Jakarta: UI-Press. Hanitijo Soemitro (1990), ***Metodologi Penelitian Hukum dan Jurimetri***, Jakarta: Ghalia Indonesia, Jakarta.

27 Cnossen C and Sith Veronica M (1997) 'Developing Legal Research Methodology to Meet the Challenge of New Technologies', ***The Journal of Information, Law and Technology*** 2.

28 WJS Poerwadarminta (1999), ***Kamus Umum Bahasa Indonesia***, Jakarta: Balai Pustaka.

29 Bruce Schneier (2016), ***Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World***, New York: WW Norton & Co.

30 Klaus Schwab (2017), ***The Fourth Industrial Revolution***, New York: Crown Publishing Group Division of Random House Inc.

31 Bryan A. Garner (1999), ***Black's Law Dictionary***, St. Paul: West Publishing Co.

32 Garner (1999), 'Black Law,'

33 Why ISIS Has All the Money It Needs (2015), 'Bloomberg Businessweek,' The Puzzle of Political Islam (2017), 'The Economist'

34 How Platforms Change Strategy (2016), 'Harvard Business Review,'

35 Terror and the Internet (2017), 'The Economist'

36 Common Purpose: Closing the Prosperity Gap (2017), 'Strategy + Business,' Autumn.

37 The Economist (2017), 'Your Connected Life' ***MIT Technology Review Terror and the Internet'***.