International Journal of Applied Business and Economic Research
Volume 16, Number 2, 2018, ISSN : 0972-7302
available at http: www.serialsjournals.com

SOME OF INDONESIAN CYBER LAW PROBLEMS

Dudu Duswara Machmuddin[1] and Bambang Pratama[2]

[1] *Langlanghuana University, Bandung, Indonesia*
[2] *Bina Nusantara University, Jakarta, Indonesia*

Abstract: Cyber regulation is very important to control human interaction within the Internet network in cyber space. On the surface, innovation development in science and technology facilitates human activity. But on the inside, innovation was controlled by new business model. In cyber business activities mingle with individual protection. By this condition, the law should keep the balance of the activities. Cyber law problems, were not particular country concern, but its global concern. This is a good opportunity for developing country to catch up with developed country. Beside this opportunity for talented people in law and technology is become necessity. This paper tries to describe cyber law in Indonesia. As a product of a developing country there are some of weakness that can be explained. Terminology and territory of cyber space become interesting to discuss, because this problems can give a broad view on cyber law in Indonesia.

1. INTRODUCTION

Information and Communication Technology (hereinafter ICT) exponentially has changed human life globally. Amazingly, ICT has various force driven new form of culture in society. Todays society is not only information of society, but also information of civilization, in which the world seen as a set of data that can be viewed, accessed, and share in a different ways [1].Behind the jargon of modern society, Zuboff also warn that the new civilization is a new model of capitalism, and therefore the law should respond to follow the change [2].

Zuboff and Unger message is very clear to develop new paradigm of law in order to create responsive law. This mean, that *jurist* must: think outside the box, holistically and interdisciplinary think, and have strategic thinking. However, in terms of legal thinking, Arief Sidharta [3]reminded that the law is not value-free, because the law has bound to the constitution of a country, and must start from applicable law as a legal basis.

In todays civilization, legal doctrine above reasonably true, because legal rule sometimes become barrier for technology development, especially in ICT. They said: the technologistsecretly waiting policy maker to sleep, then they can run the technology. If the rule makers awaken, they only become a burden. Law science (jurisprudence) as normology science is bound to the constitution on a country. This is the uniqueness; therefore, the value of Indonesian law is Pancasila as a philosophy of constitution.

In relation of ICT in law perspective, cyber law in Indonesia can be considered as a new study in law. But in practice demanding clear and fast policy to respon the dinamic of innovation. In global perspective, current law issues in developed country insisted developing country to respond, because interconnection of information do not differentiate country level. On the other hand, this is a good opportunity for developing country to catch. But in practice, lack of law expert in cyber become serious problems. The case of data protection is todays global issue in cyber law. In developed country, they already had robust legal framework to protect the data. But in Indonesia, legal standard for data protection and data treatment remain unregulate. This situation made the technologist set the rule self-regulated. In spite of ISO 27001 used as a standard data treatment in practice, but in legal perspective the rule is vague.

Indonesian cyber law was regulated by the Law No. 11/2008 regarding Information and Electronic Transaction (hereinafter ITE Law). Based on practice, there are two fundamental problems in ITE law. First; terminology problems, and second; cyber space problems. This two weekness must be clearly define, if is not, there are more problems occur. Most of cyber law case in Indonesia is defamation cases, in which the case mostly ignored the participant of the crime it self. For simple explanation in defamation case, the criminals can be more than one person, but the convicted always one person.

2. INDONESIAN CYBER LAW ANATOMY

Cyber law/ITE law in Indonesia was built by the convergence of three areas of law that become cyber law pillars, namely: telecommunications law, media law and law of informatics. If the law concept placed in the contestation of existing positive law, Indonesia has not recognized media law and law informatics. Media law and law informatics is associated with the field of intellectual property law and also associated with telecommunication law and press law. Based on the pillars of cyber laws, the principle must be inheritance into ITE law. But it is not in reality. Principle of law that only runs in particulars law is known as sectorial law principle[4].

Thus, it can be said that ITE law epistemologically unaccountable. Apart from legal systematic interpretation, urgency of cyber regulation in 2008 is extremely high, because there is no cyber regulation. But the consequences of this hasty decision, ITE law loose focus on information and electronic transaction. However, if we see ITE law statue, by its name, this law should have morefocus in information and electronic transaction, not regulate anything else, like defamation, interception, hate speech, and gamble.

3. SOME OF PROBLEMS IN INDONESIAN CYBER LAW

3.1. Cyber Terminology Problems

Before discussing about cyber law, common use of terminology is important to reach an agreement of legal meaning to enhance legal opinion [5]. Cyber terminology in Indonesia is very important to explain, because of disagreement among legal expert. Unfortunately, cyber terminology differences are also reflected in legislation. Refering to Black's Law Dictionary, 'cyber' terminology was uncovered inside the dictionary. Black's Law only explain cyber law, not cyber. However, regarding cyber concept, Blacks Law suggested concept of space in it[6]. Space in cyber concept indicate teritory, because the law prevail jurisdiction to apply (*ius constitutum*).

Cyber terminology referred to the telecommunications law, in which etymologically derived from French words of *'telematique'*[7].Others expert said that cyber was formed by the convergence of ICT[8] that began in the early 1990s of electronic commerce or electronic commerce (e-commerce) [9]. Others expert argue that cyber terms also known with another name, that is; Information Technology law (Law of Information Technology), the World Law Maya (Maya World Law) and the Law of Mayantara, which is all the life in virtual (cyber/Internet) [10].As a result of this disagreement, inconsistency of cyber terms appears not only in ITE Law, but also in several legislation, namely: Intelligent Law (Law No. 17/2011) and law of Notaries (Law No. 2/2014).

The Three laws above are still applied until now, although contain terminology errors. This mistake consequently can bring error on substance. Sitompul found that 'cyber' term was not just a term, but it was born based on the concepts of cybernetics. The paradigm of this concept is to see information as an extension of the mind and the eye. Thus forming imagination and reality, including the new world [11]. Cyber terms also have equivalent words in Indonesian, which is '*siber',* not '*maya'* (unrealistic). The reason of 'maya' words is not appropriate because Indonesian dictionary define '*maya'* as imagination or fantasy. Telematics terms also inappropriate because telematics is short for three components: telecommunications, multimedia and informatics. Josua also argue that cyber terms must interpret extensively to get broad meaning. In respond to the situation, Indonesian Constitutional Court judge decided that to understand cyber is the media that use to do an activity that has impacted the lives of people in real world.

Josua arguments have similarity with constitutional court decision to use cyber terminology. Therefore, the next task is to find the constituent elements. In the case of

cyber element, according to Kang[12], there are four elements, that is: (1) temporal engagement, (2) communication Initiation, (3) audience scope, and (4) media richness. New type of communication that formed cyber world also have rules in it. Lessig argue in cyber there are two kind of law, namely code is law and legal code[13], which in principle to regulate human interaction not only with computer, but also inter-human communication.

By contrast, terminology disagreement of cyber arises from different view among legal experts. The most vulnerable argument is an argument that takes computer (tools) to inside the argument. In fact, to access the cyber space, the tool was a necessity. Therefore, inserting tools into the argument is disturbing the argument itself. By the proposition of legal expert above, cyberspace is a place/region/territory that generated by Interconnection of computer network. Therefore, fitting legal concept into cyber space is appropriate, and compatible with Cicero adagium *ubi societas, ibi ius.* If we understand cyber law is the law to regulate *netizen* (Internet user) to interact with other *netizen,* from the argument above, there are at least three reason to enhanced the argument: (1) cyber is common terminology globally, (2) the words cyber is not apple-to-apple with 'maya' words, because there is legal consequences in cyber, particularly in doing criminal offence (*schuld*), (3) to enter cyber space, require Internet and device connectivity, any action on offline computer considered as non-cyber crime.

The last line of the argument can be explain:if the crime use criminal law, there are two type of crime, namely: the crime using tools and cyber crime. In cyber crime, the use of computer is inevitable and done within Internet network. In the concept of crime using computer the action is not necessarily cyber crime if the action done without Internet connection. For example: a portable computer belonging to A taken by B. The crime committed by B is not the cyber crime. Even if A arguing there is stolen computer data, but the crimes can not classified as cyber-crime. The compliance of cyber element into B will appear if B stole computer data using computer network. This is the uniqueness of Indonesian cyber law, but in most developed country, the regulation can reach all of computer crime, because they cyber crime regime regulate computer related crime.

3.2. Space in Cyber

A philosophical foundation in freedom of expression has been mandated in 1945 Indonesian Constitution. As a democratic country, one of theindicators is legal guarantee on freedom of expression, freedom of speech and freedom of the press[14]. Indonesian laws regulate freedom of expression by wrapping it inside right to informed (to received, to process, to send, and to use information). So, the idea of freedom of expression is an activity using information. In its relation, individual information is vis-à-vis with another individual information; in which each of individual have the same rights. In this condition, the law turn up to solve individual conflict, by regulating them. In terms of information, they are three type information, which are: public information, private information, and national secrets information. The classification is not only based on juridical perspective, but also had similarity with privacy[15]. Solove also explain that in personal information a person have a right to express his/her idea, notion, data and fact[16].

Although, Soloves concept in privacy based on individualism philosophy, which is 'men are created free', but to have strong understanding in informational right, Indonesian law system limited individual right with public interest. In a real world regarding space, we know public and private space to deliver information. The question raised for public and private space is on how the law defined this concept in cyber space. To answer this question, lets take a closer perspective on communication theory, which was initiated by Edward T. Hall or known as Proxemics theory[17]. Halls theory can be described below.

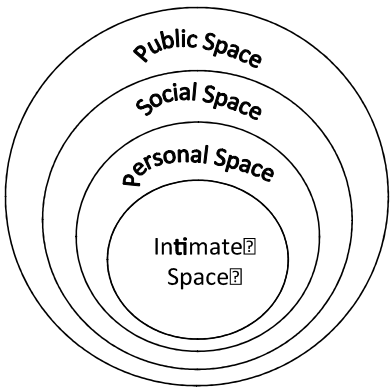

Figure 1: Proxemics Theory

Halls separates communication by determines the sphere with its relationship. Halls concept, is very useful to classifying legal action clearly. For example: if someone in an intimate sphere humiliate someone else dignity, this action cannot be categorize as defamation. The reason if this arguments because of intimate sphere is not public sphere, and the law prerequisite public sphere in order if defamation offence.

In cyber space territory, defamation offence also must fulfilled public sphere, or done in public space. Ludlow framing this concept by explaining that public space in cyber is a space that's not required invitation or password to enter[18].However, of course, Ludlow opinion was necessary must be seen case-by-case, because in social media, the situation is far more complicated. Regardless, the important thing from Ludlow is in cyber space the concept of communication sphere also can be used.

Within legal perspective, defamation was also regulated in ITE Law. But this norm was taken to judicial review court, because it was feared become highly ruled and harm the democracy spirit. The constitutional court, decided that cyber defamation, basically same with a defamation in non-cyber. But in practice, unfortunately defamation norm mostly used to criminalize by particular person.

To strengthen argumentation, there are at least three cases that can be serve as an example. (1) Prita Mulyasari vs. Omni International Hospitals (2009), (2) satay seller vs. Indonesian President, Joko Widodo (2014), and (3) the National Narcotics Agency (BNN), Indonesian Republic Police (POLRI), Indonesian National Army (TNI) vs. Harris Azhar (The Commission for Disappeared and Victims of Violence/KONTRAS) (2016). These three cases drew public attention, because they are victims. Some of research data claimed they are hundred victims of defamation in, but the exact number was never showed.

The most important things in cyber defamation is the fulfillment of the norms element of public spaces. For example, social media, Tweeter, urged that all of Tweeter users arein public space when they Tweet, that's why Tweeter user must very careful to write in Tweeter. Regarding this concept, Facebook imposed another concept or give option for user to set type of his/her writing in Facebook, whether send in public or private space. So the treatment in Facebook is casuistic, depend on the cases.

4. CONCLUSION

As a part of the innovation dynamic, cyber phenomenon is hard to catch by the law-maker to formulate robust legal framework. Some of the developed country may see cyber law as a simple space to rule with some adjustment of law concept, but in developing country like Indonesia, the degree of difficulty is several times more difficult. ITE law was an example of law product in Indonesia that trying to catch a developed country. The key is ITE law are the conceptual of technology as an object of the law must be clearly defined. If the concept was right, then the norms will also be clear to determine.

REFERENCE

Shoshana Zuboff (2015). "Big Others: Surveillance Capitalism and The Prospect of an Information Civilization," *Journal of Information Technology*, p. 77.

Roberto Mangabeira Unger (2007). *Free Trade Reimagine*. New Jersey: Princeton University Press.

Bernard Arief Sidharta (2000). *Refleksi tentang Struktur Ilmu Hukum*. Bandung: CV. Mandar Maju.

Gabriel Hallevy (2010). *A Moern Treatise on The Principle of Legality in Criminal Law*. Berlin: Springer-Verlag.

Hilman Hadikusuma (2013). *Bahasa Hukum Indonesia*. Bandung: PT. Alumni.

Bryan A. Garner, Ed. (2009). *Black's Law Dictionary*. Dallas, USA: Thomson Reuters.

Edmon Makarim (2003). *Kompilasi Hukum Telematika*. Jakarta: PT. Raja Grafindo Persada.

Danrivanto Budhijanto (2010). *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi, Regulasi dan Konvergensi*. Bandung: Refika Aditama.

Shinta Dewi (2009). *Cyber Law, Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran.

Ahmad M. Ramli (2004). *Pengaruh Teknologi Informasi Terhadap Eksistensi Hak Kekayaan Intelektual dan Urgensi Hukum Siber (cyber law) dalam Sistem Hukum Nasional*. Bandung: Refika Aditama.

Josua Sitompul (2012). *Cyberspace, Cybercrime, Cyber Law, Tinjauan Aspek Hukum Pidana*. Jakarta: PT. Tata Nusa.

Jerry Kang (2000). "Cyber-Race," *Harvard Law Review*, pp. 1148-1147, March.

Lawrence Lessig (2006). *Code Version 2.0*. New York, USA: Cambridge Center.

Amir Efendi Siregar (2014). *Mengawal Demokratisasi Media: Menolak Konsentrasi, membangun Keragaman*. Jakarta, Indonesia: PT. Kompas Media Nusantara.

Paul M. Schwartz and Daniel J. Solove (2011). *The PII: Privacy and a New Concept of Personality Identifiable Information*.: NYW Law Review.

Daniel J. Solove (2004). *The Digital Person - Technology and Privacy in the Information Age*. New York: New York University Press.

Edward T. Hall (1966). *The Hidden Dimension*. New York, USA: Garden City.

Peter Ludlow (2001). *Crypto Anarchy, Cryberstates, and Pirate Utopias*. USA: Massachusetts Institute of Technology.