ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 88

1st International Conference on Innovation in Research (ICIIR 2018)

Privacy Related to Cyber Space Activities

Ni Putu Suci Meinarni, Emmy Febriani Thalib
STMIK STIKOM Indonesia
Denpasar-Bali, Indonesia
sucimeinarni@stiki-indonesia.ac.id

***Abstract*—Human Rights become an integral part in the various interactions that occur in cyberspace. Interaction between users of the virtual world is a distance interaction which is not necessarily meet in person. This can lead to potential lies or even the use of one's identity. Utilization of the intended identity is, using the identity of others with economic motives or certain crime motives. The principle of "The Right to be Let's Alone" is interesting in this study. Discussing issues that occur in cyberspace related to social phenomena related to privacy done through case studies of several phenomena contained on the internet and mapping the problem and conduct assessments with relevant legislation. Patterns of disturbance to human rights have similarities with one another, which in essence is the disruption of one's comfort in the virtual world. The cause of the above problems arises because, firstly, the lack of understanding that everyone has the right to privacy, the second actually happens the opposite, they are very upholding freedom of expression so as to forget there are other rights (person) is disturbed, and the third is the interest factor. E.g.: economic interests, spamming in the social media as a marketing purpose, etc.**

Keywords—privacy; human rights; cyber law

I. INTRODUCTION

Privacy in cyberspace (cyber space) is a human right that must be upheld for every cyberspace legal subject because it is a basic right that has a very important role related to human autonomy or authority and is protected by international and national law. Privacy on the initial concept of protection is referred to as the right not to be disturbed by others "the right to be let alone", meaning that every human being has the right to be alone, free from interference from others and others must do the omission. This right has a close connection with human nature as individual beings. Some things that are worth studying are related to the emergence of increasingly sophisticated applications related to privacy in cyberspace, including protection from spy, protection of personal data and privacy of positions. Even though every agreement related to the download automatically has given the application owner the opportunity to hack personal data or track the where about of the application downloader. National law regulations, bilateral agreements and international law regulations related to human rights are expected to be able to overcome problems related to these aspects of privacy.

Every service user/social media account is asked to register with a number of real data related to the account of the person concerned. The development of internet technology and marriage by collecting and using data does not merely change the concept of privacy and proclaims that there is a setback in its protection. Technology, especially social media indeed contributes greatly to changes in data control. But there should be innovations or changes in how to respond to these developments, one of which is to expand responsibility to various sectors, not only individuals as data holders, but also data collectors [1].

In the world of banking, online transactions related to banking have provisions that force every credit card owner to voluntarily provide some personal data. This can also potentially cause digital crime related to the use of credit cards.

The commitment of the Indonesian government to continue to encourage information transparency is also evident from its participation in global initiatives to encourage open governance, through the Open Government Partnership (OGP). However, even though the regulations and initiatives show very good progress, in the implementation there are still many inconsistent records, especially from government institutions in applying information disclosure obligations [2].

The government realizes that social aspects are unconsciously realized by the public that personal data is very risky, for example making a status on social networks whether it is photo data, family, etc., the privacy data has been consumed by the public all over the world directly [3]. This was conveyed at the National Urgency Seminar on Personal Data Protection Arrangements, at the Millenium Hotel, Jakarta, in 2013, but until now the Bill on the Protection of Personal Data has not yet been ratified. Based on the research background above, the writers interested to write about “Privacy Related to Cyberspace Activities“.

II. METHODS

The conducted study related to the writing of this article is included in the category/type of normative research, i.e. a library legal study or legal study which is based on secondary data [4]. The need of conducting this normative study was inexistence of law norm related to the problem of this research. The approaches of this study are The Statute Approach and Conceptual Approach. Collection of law material was conducted by documentation study. Data analysis was conducted by using qualitative analysis method and was presented qualitative descriptively and systematically [5].

III. Results and Discussion

A. Human Rights and Related Regulations

Regarding privacy, Western people have realized long ago about the basic rights possessed by humans. For example, a legal expert from Harvard University has written in a journal published in 1890 entitled: *The Right to Privacy*.

> *"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage".*

Which means privacy is upheld on the principle of justice and on the basis of moral health by promoting general comfort. So, as long as matters relating to privacy can be accepted in the community, the provisions of the law regarding privacy can be applied.

Then the term "The Right to Be Let Alone", so this right recognizes that there are related limitations on protection from undesirable disturbances in life. Privacy settings will give individual authority to negotiate with whom and how to interact with others.

International Human Rights Law has had great attention to digital privacy that takes concepts in various declarations regarding human rights and individual freedom. At the 2013 UN General Assembly, member states agreed on the right to privacy. Member States are asked to be transparent and responsible when collecting personal data. Therefore, protection of personal data is an extension of the protection of human rights.

The Universal Declaration of Human Rights (UDHR) is a document that is a milestone in the history of human rights [6]. This document was prepared by representatives of countries from various legal and cultural backgrounds from all over the world, and was declared by the General Assembly of the United Nations (UN) in Paris on December 10, 1948 as a general reference to the achievement of all nations and countries. In this declaration also for the first time Human Rights are fundamentally established to be protected universally.

Article 1 of the UDHR:

> *"All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."*

Which means that everyone is born free and has the same dignity and rights. They are endowed with reason and conscience and should associate with one another in a spirit of brotherhood.

Related to one's personal rights, stated in Article 12, namely:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

No one can be disturbed by his personal affairs, family, household or correspondence, nor is it permissible to violate his honour and good name. Everyone has the right to legal protection against such disturbances or violations.

Law of the Republic of Indonesia Number 39 of 1999 concerning Human Rights [7], in this Law what is meant by:

- Human rights are a set of rights inherent in the nature and existence of human beings as a task of the God's and a gift that must be respected, upheld and protected by the state of law, government, and everyone for the honour and protection of human dignity.
- The basic of human's obligation is a set of obligations that if it's not implemented, do not allow the realization of human rights.
- Discrimination is any direct or indirect limitation, harassment or exclusion based on human differentiation on the basis of religion, ethnicity, race, ethnicity, group, class, social status, economic status, language, political beliefs, which results in a reduction, deviation or the elimination of the recognition, implementation or use of human rights and basic freedoms in the lives of individuals and collectively in the political, economic, legal, social, cultural and other aspects of life.
- Torture is any act that is done intentionally, so that it causes great pain or suffering, both physical and spiritual to someone to obtain recognition or information from someone or from a third person, by punishing him for an act that has been done or allegedly carried out by someone or a third person, or threaten or force someone or a third person, or for a reason based on any form of discrimination, if the pain or suffering is caused by incitement from, with agreement, or the knowledge of anyone and or a public official.
- Children are every human being under the age of 18 (eighteen) years old and not married, including children who are still in the womb if it is in their interests.
- Human rights violations are any acts of a person or group of people including intentional or unintentional state apparatus or negligence which unlawfully reduces, obstructs, limits, and or revokes the human rights of a person or group of people guaranteed by this law, and does not obtain or it is feared that they will not get a fair and right legal solution based on the applicable legal mechanism.
- The National Human Rights Commission, hereinafter referred to as Komnas HAM, is an independent institution that is located at the same level in other countries that functions to carry out the study, research, distribution, monitoring and mediation of human rights.

From the 7 points above, there are elements that deserve to be underlined: human rights and obligations, discrimination and violations as well as state institutions tasked with providing human rights services.

Human rights protection in cyberspace is regulated in Law Number 11 of 2008 jo. Law Number 19 Year 2016 concerning Information and Electronic Transactions [8].

Arrangements regarding personal data protection in the Information and Electronic Transactions Act (ITE Law)

- Every person intentionally and without rights or unlawfully conducts interception or wiretapping of Electronic information and / or Electronic Documents in a particular computer and / or Electronic System belonging to another Person.
- Every person intentionally and without rights or unlawfully conducts interception of the transmission of Electronic Information and / or Electronic Documents that are not public in nature from, to, and in a particular Computer and / or Electronic System belonging to another person, whether that causes no change even those that cause changes, omissions, and / or terminations of Electronic Information and / or Electronic Documents that are being transmitted.
- Except interception as referred to in paragraph (1) and paragraph (2), interception is carried out in the context of law enforcement at the request of the police, prosecutor's office, and / or other law enforcement institutions that are stipulated by law.
- Further provisions concerning interception procedures as referred to in paragraph (3) are regulated by Government Regulations.

B. General Data Protection Regulation (GDPR)

Data privacy and data protection are very closely interconnected, so much so that users often think of them as synonymous. But the distinctions between data privacy against. Data protection are fundamental to understanding how one complements the other. Privacy concerns arise wherever personally identifiable information is collected, stored, or used.

What's important to understand when comparing data privacy vs data protection is that you can't ensure data privacy unless the personal data is protected by technology. If someone can steal personal data, its privacy is not guaranteed, which puts you at risk for identity theft and other personal security breaches. But the opposite relationship isn't always true: personal data can be protected while still not being reliably private [9].

Other countries have already had rules regarding Data Protection of their Citizens as Australia has established the Privacy Act in 1988, while Singapore has established the Personal Data Protection Act in 2012.The European Union has a General Data Protection Regulation (GDPR) which has implemented the rules of personal data protection on May 25, 2018.GDPR is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) [10].

Regarding the personal data referred to in the GDPR, any related information regarding the identification of a person, either directly or indirectly, specifically referring to the person identified. This definition includes various personal identifiers to inform personal data, including names, identification numbers, location data or online identifiers, which reflect changes in technology and the way organizations collect information about people [8]. In the GDPR stated that personal data cannot be used if the owner of the data has not giving permission. For consumers, this policy provides protection for them so that their data is not used outside the realm of owner.

GDPR is the main law governing how companies protect the personal data of EU citizens. All companies that hold data on European Union citizens must comply with these regulations. In addition, the GDPR must also be adhered to companies outside Europe who want to take advantage of European Union citizen data, for example for the sake of distributing advertisements.

The EU struggle in forming the GDPR, namely an entity that protects personal data will involve countries that have a relationship in the "disclaimer". And GDPR is a reference for legislation in Indonesia if it feels necessary.

The purpose of the GDPR is to provide better protection for data privacy in today's digital economy by providing more freedom for individuals to their data and providing stricter regulations to those who manage or store them. And this regulation will be effective on May 25, 2018 throughout the world.

The GDPR requirements apply to each member country of the European Union, which aims to create more consistent protection for consumer and personal data in all EU countries. Some privacy keys and data protection requirements of GDPR include:

- Requires subject approval for data processing
- Identify collected data to protect privacy
- Provide notification of data violations
- Safely handle cross-border data transfers
- Require certain companies to appoint data protection officers to monitor GDPR compliance

In Asia, one of the country that also have a regulation likely GDPR is Japan. Japan has 2 regulations on this matter, namely the Act on the Protection of Personal Information on the protection of personal information in the private sector and the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure in the public sector administrative procedures.

Japan also has a special commission, the Personal Information Protection Commission Japan, which is in charge of protecting the rights and interests of individuals when entering personal data. South Korea also has regulations regarding personal data protection, namely Personal Information Protection Act (PIPA). Individual Koreans with a special Personal Information Protection Commission (PIPC) who is tasked with protecting the rights of individual privacy by reviewing and resolving policies related to personal data, coordinating differences between state institutions in

processing personal data, so that data information privacy and security rights remain awake.

In the ASEAN region, many countries have adopted and have regulations regarding Personal Data Protection. Like Malaysia, which has regulations on Personal Data Protection since 2010 with Personal Data Protection Act Number 709, a Personal Data Protection Commission has been formed.

Legal academician Yvonne McDermott argues that in the Big Data era there are four key values that must be upheld: privacy, autonomy, transparency and non-discrimination [11].

In 2016, the Ministry of Communication and Informatics issued a ministerial regulation on personal data protection in electronic systems as an implementing regulation of the 2008 Electronic Information and Transaction Law [8]. Given recent data breaches, the Government has issued a new draft personal data protection law.

Opportunities for abuse of citizen's personal data are increasingly open with so many rules that provide space for government and private institutions to collect and open personal data of citizens. There are at least 30 laws related to the collection of personal data of citizens who are still overlapping.

Meanwhile, in the draft Personal Data Protection Bill will cover principles, mechanisms and sanctions. The plan, this bill will adopt some of the existing rules in GDPR (General Data Protection Regulation) such as data owner approval, accountability, appointment of personal data management data, to the right to delete and access.

The Draft of Law elaborates that general Personal Data means Personal Data that can be obtained from the public domain or has been disclosed under an identity document, e.g., name, identity card number, photo, telephone number, email address and birth date (noting that identity documents are widely used in Indonesia).

Also further regulations must be issued to clarify whether this will be an independent authority or a part of the Ministry of Communication and Informatics, which is the current authority that monitors general data protection matters.

IV. Conclusion and Suggestion

A. *Conclusion*

Indonesia already has regulations regarding Personal Data Protection but it is still fragmented in several sectors and overlaps so that it does not have a single and comprehensive regulation that can be applied to all sectors in a clear manner. Because the Ministry of Communication and Informatics which regulates Personal Data Protection does not regulate cross-sector.

B. *Suggestion*

- Experts in various sectors must collaborate with the Indonesian government to encourage and produce comprehensive personal data protection laws to protect citizens from the possibility of their data being used without permission or to discriminate against them.
- Personal data protection laws also have continued potential for the country's economy by creating safer business ecosystems. So that this condition will create business opportunities and also encourage more investment for companies in Indonesia.
- At the same time, citizens also need to be educated about digital privacy in order to understand the potential risks that exist and their rights to protect privacy and personal data. The need to always develop scepticism and prudence in every activity and online transactions, and be able to be realistic and mature in acting so that the information provided does not harm the users themselves.

References

[1] Elsam.or.id, "Memahami Konteks Privasi Dalam Kultur Asia Dan Tantangan Pemerintah Indonesia," 2017. [Online]. Retrieved from: http://elsam.or.id/2017/10/memahami-konteks-privasi-dalam-kultur-asia-dan-tantangan-pemerintah-indonesia/ [Accessed on 18-Jun-2018].

[2] I. for C. J. Reform, "Menyelaraskan Kebijakan Data Terbuka dan Perlindungan Hak Atas Privasi," 2015. [Online]. Retrieved from: http://icjr.or.id/menyelaraskan-kebijakan-data-terbuka-dan-perlindungan-hak-atas-privasi/ [Accessed on 18-Jun-2018].

[3] Kominfo.go.id, "Sesditjen IKP : Perlu segera UU Perlindungan Data Pribadi," 2013. [Online]. Retrieved from: https://kominfo.go.id/index.php/content/detail/1337/Sesditjen+IKP+%3A+Perlu+segera+UU+Perlindungan+Data+Pribadi/0/berita_satker [Accessed on 18-Jun-2018].

[4] S. Soekanto, Pengantar Penelitian Hukum. Jakarta: Universitas Indonesia Press, 2012.

[5] S.S.S. Mamudji, Penelitian Hukum Normatif; Suatu Tinjauan Singkat. Jakarta: PT. Rajagrafindo Persada, 2003.

[6] U. Nation, "Universal Declaration on Human Rights," 1948. [Online]. Retrieved from: http://www.un.org/en/universal-declaration-human-rights/ [Accessed on 16-Jun-2018].

[7] R. Indonesia, Undang-Undang tentang Hak Asasi Manusia. 1999.

[8] R. Indonesia, UU Informasi dan Transaksi Elektronik. 2016.

[9] R. Robinson, "Data Privacy VS Data Protection," 2018. [Online]. Retrieved from: https://blog.ipswitch.com/data-privacy-vs-data-protection [Accessed on 01-Aug-2018].

[10] F. News, "Pengertian GDPR," 2018. [Online]. Retrieved from: https://faktualnews.co/2018/05/25/pengertian-gdpr-dampak-tujuan-dan-sanksi-atas-gdpr/81866/ [Accessed on 15-Jun-2018].

[11] "The Conversation," 2018. [Online]. Retrieved from: https://theconversation.com/indonesia-sangat-memerlukan-undang-undang-perlindungan-data-pribadi-92607 [Accessed on 01-Aug-2018].