



A Case Study on Facebook Data Theft in Indonesia

Rudi Natamiharja

Faculty of Law, University of Lampung, Department of International Law
rudi.natamiharja@fh.unila.ac.id

Abstract

The rights to privacy as an individual fundamental right should be protected. Ironically, this right is deliberately delivered publicly in social media. And Facebook, the largest social media, keep more than 2.2 billion privacies data in the whole world. In early April 2018, one million personal data of Indonesian Facebook users was stolen by other parties. Mark Zuckerberg, as a founder and CEO, acknowledged that the Facebook data consisting of customer personal data had been stolen and used by other parties. It is one of the weaknesses and negligence of Facebook that needs to be addressed in the future. Indonesia government issued a warning letter to Facebook and required formal explanation concerning those recent cases. However, the Government's seriousness on the protection of personal data of its citizens is still questioned. How Indonesian regulations cover private data protection on their citizen and what steps should be taken to protect personal data in Indonesia? By using the International instrument and Indonesia legal instruments on the protection of privacy right, this article would give the answer what government Indonesian should do to undertake this situation. The research found that the regulation of privacy protection is sufficient yet the government has no determination to take account seriously on protecting the privacy right, and no sanction to the parties was involved. Socialization on the importance of personal data toward Indonesian society in Indonesia should be done, from the basic to the top level.

Keyword: *Right Privacy, International Law, Fundamental Rights*

How to cite: Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia", *Fiat Justisia*, 12 (3), (2018).

DOI: <https://doi.org/10.25041/fiatjustisia.v12no3.1312>

A. Introduction

The use of information technology in Indonesia has increased positively from year after year. Progress has been mentioned since the entry of the internet technology to the homeland since in 1988.¹ The harmony between the development of information technology with the media and telecommunications today has resulted in a growing variety of services and existing products. The convergence of these technologies is called telematics (telecommunications, media, and informatics). The use of the Internet in various fields in our lives not only makes things easier but also causes some problems, one of which is the legal problem. One of the legal issues which may occur are issues related to the protection of privacy rights. The right to privacy is the privacy rights possessed by a person of his or her privacy. This right becomes private because it involves information that cannot be owned or submitted to all party without the permission of the owner of that identity. Some experts express this basic understanding of the right to privacy.

Professor of public administration law from the University of Colombia, Alan Westin, defines the right to privacy as claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. The extent of privacy coverage usually makes the number of privacy settings in a country, both in type and level.² The notion and scope of other privacy concepts often referred to be the formulations developed by William Prosser, referring to at least four things: (a) Disturbance of a person's act of alienation or aloofness, or interference with his relationships (b) Disclosure of personal facts publicly embarrassing (c) The publicity that puts a person wrong in public opinion (d) Unauthorized control of a person's likeness for the benefit of others.³

In international legal instruments, freedom of privacy is recognized as inherent basic rights to every human being. This provision is contained in the

¹ Asih Antika, "Tahukah Kamu, Kapan Internet Pertama Kali Masuk Ke Indonesia", *Official website of Dewan Teknologi Informasi dan Komunikasi Nasional (WANTIKNAS)*, October 03, 2016, <http://www.wantiknas.go.id/2016/10/03/tahukahkamu-kapan-internet-pertama-kali-masuk-ke-indonesia/>, (accessed May 17, 2018)

² AF Westin, *Privacy and Freedom*, New York: Atheneum, (1967), pp. 7-8.

³ William Prosser, as quoted in DeCew, Judith, "Privacy", *The Stanford Encyclopedia of Philosophy* (Fall 2012 Eds), Edward N Zalta (ed). Can be downloaded at <http://plato.stanford.edu/archives/fall2012/entries/privacy/>.

Universal Declaration of Human Rights. The Declaration has provided the legal basis for its member states in respect of the state's obligation to protect and respect the right of the individual's private citizens. This provision is explicitly stated in Article 3 and Article 17 of the Universal Declaration of Human Rights. Article 3 set the right of the person as follows: "Everyone has the right to life, freedom, and liberty as an individual. "While Article 17 to protect the freedom in two paragraphs, namely: (1) Everyone has the right to own property alone or jointly with others; (2) No one shall be deprived of his property arbitrarily.

Both the terms of the Universal Declaration of Human Rights above provide for the broad protection of the right to privacy. But this is the embryo of the emergence of more specific protection classified into two classes of protection, first against civil rights and political rights, the second is the protection of economic, social and cultural rights or known as "ECOSOC" originating from International Covenant on Economic, Social and Culture Rights. Furthermore, the International Covenant on Civil and Political Rights (ICCPR), which was born on December 16, 1966, through Resolution 2200A and entered into force on 23 March 1976 provides more protection for the rights of the human person. Indonesia has ratified the ICCPR on 28 October 2005 through the Law of the Republic of Indonesia Number 12 the Year 2005 on the Ratification of the International Covenant on Civil and Political Rights.

The State of Indonesia state based on the rule of law and it's obliged to embody this international provision in a positive, applicable and positive contribution to its citizens. The importance of this rule must be felt in everyday life. So that the people of Indonesia do not feel anxious personal data will be used or known to other parties that he does not desire. One example of cases of personal data protection in Indonesia is about the theft of users of social media data Facebook. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million users of Facebook, about 1 million of whom belong to users of Facebook in Indonesia. Indonesia is the third biggest country after the United States and the Philippines whose data are used.⁴

This data theft incident stems from the cooperation of Facebook and the application "thisisyourdigitallife." According to data compiled by Facebook Indonesia, 748 people have installed the application "thisisyourdigitallife" from November 2013 until December 2015. There are additional more than 1 million users who are affected by the friends of the user application. Then there are a total of 1,095,918 users whose data are stolen or 1,26 % of the

⁴ Oik Yusuf, "Data 1 Juta Pengguna Facebook Indonesia Dicuri", *Kompas*, April 05, 2018, <https://tekno.kompas.com/read/2018/04/05/10133697/data-1-juta-user-facebook-indonesia-dicuri>, (accessed June 12, 2018).

total affected users globally. The meeting between the Commission 1 of the House of Representatives and Facebook been held. House of Representatives worried about Facebook data will affect the Indonesian political year of elections and elections simultaneously 2019 because Cambridge Analytica reportedly ever used a Facebook user information related to US presidential elections in 2017 and where the underdog Trump has managed to win his fight with Hillary Clinton. The disappointment of the House against Facebook is the absence of law enforcement from Facebook to third parties (Cambridge Analytica).⁵ The government's irresponsiveness in taking action has sparked the question of whether the provision in Indonesia is sufficient to cover its citizens or whether it is the House of Representatives' reluctance to resolve the issue.

After the amendment of the The 1945 Constitution of the Republic of Indonesia (*Undang-Undang Republik Indonesia 1945*), Law Number 11 on 2008 of Information and Electronic Transactions or abbreviated as the ITE Law was established. Then some articles of the law have improved in 2016 which became known as the Law Number 19 Year 2016 on the Amendment of Law Number 11 on 2008 of ITE. The establishment of the ITE Law is a mandate of the 1945 Constitution of the Republic of Indonesia, including articles relating to personal data, rights to privacy. In the elucidation of Article 26 paragraph 1 of Law Number 19 Year 2016 it is stated that the definition of personal rights is, the right to enjoy private and free life, the right to be able to communicate with others without spying action, the right to monitor access to information about personal life and data someone. In Article 17 paragraph 3 of Regulation of the Minister of Communication and Informatics Number 12 of 2016, it is clearly stated that the Telecommunication Service Provider must keep the data and the identity of the customer confidential.

The rules of personal data protection are outlined in the Ministerial Regulation No. 20 of 2016 on Personal Data Protection (PDP) set on November 7, 2016, enacted and effective from 1 December 2016. In the rule, it is stated that Personal Data is certain personal data stored, cared for, and safeguarded by the truth and protected by its secrecy. In this rule, an electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal rules on the protection of personal data which must pay attention to aspects of the application of technology, human resources, methods, and costs. The owner of the personal data, is entitled to the confidentiality of his data; have the right to lodge a complaint in order to settle a private data clause; entitled to

⁵ A sample case can be found at <https://tekno.tempo.co/read/1080112/dpr-bert-facebook-besok-bahas-skandal-data>.

access to obtain historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system. Through the existing personal data rules in Indonesia, it can be concluded that the protection of personal data in Indonesia is insufficient because it has no comprehensive laws or rules regarding the protection of personal data protecting its citizens from data misuse. It is, therefore, necessary to create a Personal Data Protection Law that has clarity of rules on the recovery of victims. Citizens also need to be educated about digital privacy to understand the potential risks that exist and the right to protect privacy and personal data.

B. Problems and Methods

Based on the background described above, the first issue to be described in this paper is the extent to which regulations in Indonesia have covered the protection of personal data. The second issue, what the Government of Indonesia should take policies and steps in providing privacy data protection?

C. Discussion

1. Case Position Destruction Facebook Data

a. Data breaker Facebook in Indonesia

1) Position Case

In 2013, Cambridge University researchers named Aleksandr Kogan created a personality quiz app, "thisisyourdigitallife." Mark Zuckerberg revealed that the Kogan app is in use by around 300,000 people all of whom are willing to share their data as well as some data from their friends. Then Facebook changed the platform policy to limit the data accessible to the app a year later. Such changes make developers like Kogan unable to request friend data from users unless their friends also access the app.

In 2015, Facebook got information from the media that Kogan has shared its data on Cambridge Analytica. Kogan has violated Facebook's policies for illegally obtaining data so that the platform removes the Kogan app. Cambridge Analytica does not delete all data as they promised before. Facebook took action to block Cambridge Analytica from its services. Cambridge Analytica argues that they have deleted all the data. They even agreed to be audited forensically by the Facebook-appointed company, Stroz Friedberg, to confirm the incident.⁶ The misuse of data by Kogan is widely cited as the largest data theft in history. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million

⁶ Kustin Ayuwuragil, "Kronologi Pembobolan Facebook oleh Cambridge Analytica", *CNN Indonesia*, March 03, 2018, <https://www.cnnindonesia.com/teknologi/20180322194919-185-285163/kronologi-pembobol-facebook-oleh-cambridge-analytica>, (accessed June 10, 2018)

Facebook users, about 1 million of whom are owned by Facebook users in Indonesia. Indonesia is the third largest country after the United States and the Philippines whose data is utilized without seizing Facebook users.

2) Expert Opinion Regarding This Case

Cybersecurity expert, Pradama Persadha expertise from Indonesian Security Research Institute of Cyber and Communications assesses that Indonesia is difficult to act firmly against Facebook in case of data leakage involving data of more than one million users of social media applications owned by Indonesian citizens. This is because Indonesia does not have high bargaining power. Facebook Indonesia is currently still searching for data related to the leak and promised to conduct an internal audit as soon as the data is obtained even without detailing when the investigation was completed. This promise has previously been conveyed by representatives of Facebook Indonesia in a Public Hearing Meeting (RDPU) with the Commission 1 House of Representatives, in April. Commission 1 of the House gives a one-month deadline for Facebook to submit its internal audit results.⁷ The results will be used to measure potential hazards that could result from data leak incidents.

Meanwhile, he said that the call to Facebook manager in Indonesia would not have a significant impact on the settlement and follow up of the case. Because currently, Indonesia does not have "bargaining power" to force Facebook to follow government rules. On the contrary, according to Pratama, this case should be momentum for Indonesia to start its independence in the field of social media application services, while exemplifying China that prohibits Google to operate in the country and has its microblogging site called Weibo. But he admitted it is still far to materialize considering Indonesia has no resources either Human Resources (HR) and infrastructure. For now, the least that the government can do is to urge the FB to minimize the impact of data leakage for example if it is used for political purposes such as in the United States.⁸

3) NGO Comments on the Hack Top of Privacy

⁷ Fatimah Kartini Bohang, "DPR Beri Waktu Facebook 1 Bulan", *Kompas*, April 17, 2018, <https://tekno.kompas.com/read/2018/04/17/16240047/dpr-beri-waktu-facebook-1-month>, (accessed June 10, 2018).

⁸ Quoted from <http://www.australiaplus.com/indonesian/berita/fb-indonesia-di-bareskrim/9674954>, (accessed May 26, 2018).

Sinta Dewi, Chairman of Cyber Law Center in Faculty of Law Padjadjaran University, stated that the interests of personal data protection regulations are increasing. This will be related to information technology business on security and data protection. It also becomes one of the necessities in ensuring the sustainability of the digital economy in the future.⁹ Deputy Director of Research Elsam Wahyudi Djafar, strengthen Sinta Dewi's opinion citing the resolution of the board of Human Rights in 2012 and 2013 adopted by the UN General Assembly which refers to Article 19 of the Covenant on Civil Rights and Political, states that: "the protection of all people when they are offline it will also apply when they are online "and" privacy protection on someone when they are offline it is also attached if they are online ". Under both resolutions, the UN encourages member states to revise its privacy-related national laws. Facebook's case according to Wahyudi Djafar, is an analytic data engineering that is not in line with the protection of the privacy of its citizens. If it persists, this practice will be perpetuated by affecting the preferences of the social choice of the social user with the consequences of excluding the rights of individual citizens. Hearing the explanation of experts from the civil society Vice Chairman of Commission I of the House of Representatives, Satya Widya Yudha acknowledges the urgency of this PDP Act. Even He also urged the Parliament to make laws for the PDP as a law a priority in the 2018-2019 national legislation. According to him, at this hearing, there was not a single fraction against the establishment of the PDP Law, so there is no reason for the House to postpone it.¹⁰

The Institute for Policy Research and Advocacy (Elsam) believes that closing Facebook access in Indonesia due to the misuse of user data by third parties is not the right solution. Deputy Director of Research Elsam Wahyudi Djafar encourages the implementation of audits with the government and Facebook to find out where the violations, what data is leaked, and what data is transferred. The issue of blocking or closing is according to him, usually depart from content issues, but for Facebook started from the issue of personal data of Facebook users. So do not have the right reasons if there is a Facebook shut down. When Facebook is closed, he fears it will limit the right of public information that has been able to communicate through Facebook and retrieve information from social media. In addition to a joint audit, it proposes a recovery mechanism against Facebook users who violated their privacy, then the obligations that must be charged to Facebook, such as updating terms of service or privacy policy to comply with privacy provisions. This is done so that the practices of alienation or misuse of data

⁹ Quoted from <http://elsam.or.id/2018/05/elsam-menghadiri-rapat-dengar-pendapat-umum-dari-panja-pengamanan-data-ponsel-komisi-i-dpr-ri/>, (accessed 10 June 2018).

¹⁰ *Ibid.*

do not happen again. Also, in the future, Facebook needs to be encouraged to educate its service users, not only do recording of data or content uploaded on Facebook for large-scale data collection.¹¹

In response to this Facebook case, Elsam sees the importance of placing human rights as the direction of its development. Human rights must be formulated in the form of a legal instrument as a guarantee of public protection. Normative forms are important for placing state responsibility and affirming the role of corporations in protecting people's privacy rights. This assurance of protection will ensure that technology and machinery work including artificial intelligence, for the benefit of data collection, will be in line with the principles of privacy protection.

It can be concluded that the government has done various actions to solve the case of personal data protection data theft Protection of this Facebook, but the action is not sufficient because until now there has been no settlement from the Government and Facebook. The law in Indonesia implicitly provides for the guarantee of the right to privacy. Unfortunately, the legal regulation has not been properly outlined in the level of legislation. Countries with low data protection laws such as Indonesia may be subjected to irresponsible companies for theft of personal data for their benefit.

4) The Government Undertook Measures

Minister of Communications and Informatics, Rudiantara, said his side keeps escorting the effort to hold Facebook accountable. Because of the possibility of account data in Indonesia abused that is to affect the results of elections next year (2019). The government has sent a letter to Facebook related to the theft of Facebook data in Indonesia to request confirmation and explanation of the case. The government can also press Facebook to immediately close access to applications that allow the theft of personal data users. The company should not submit to the account owner to actively disable the leak-prone application. Facebook needs to be responsible for the privacy of its users. The Ministry of Communication and Informatics does not stand alone but also cooperates with the police. The Ministry of Communication and Informatics only takes care of administrative sanctions, while for criminal sanctions the process is carried out by the police. Relate leaked data social media platform Facebook, Rudiantara rate the process is not easy because Facebook is pursued quibble pending audit results from the authority in the UK, namely Information Commissioner Office (ICO).¹²

¹¹ Antara, "Data Bocor, Elsam: Menutup Facebook Bukan Solusi" Tempo, April 11, 2018, <https://bisnis.tempo.co/read/1078332/data-bocor-elsam-closing-facebook-not-solution>, (accessed May 26, 2018).

¹² Quoted from https://www.kominfo.go.id/content/detail/13163/rudiantara-bakal-insiasi-regulasi-soal-konten-medsos/0/sorotan_media, (accessed May 26, 2018).

b. Another Case Concerning the Violation of the Right to Privacy

1) Facebook Case in Singapore

More than 65,000 Facebook users in Singapore experience the theft of Facebook data.¹³ The Personal Data Protection Commission (PDPC) says that they are in close contact with Facebook and are looking into this issue. PDPC is concerned that the people of Singapore will be affected by the theft of this Facebook data. SCL Group, the holding company of Cambridge Analytica, has opened an office in Singapore. So far Singapore connection has been developed, but News Lens News have evidence of the relationship between the protagonists of scandals involving Cambridge Analytica and Singapore, including academics Singapore who has worked with the Ministry of Defense, Office of the Prime Minister of Singapore, and the Interior Ministry, which oversees the police Singapore, the security and intelligence services. The leading trio of Singapore academics has access to Facebook data collected in the same way as the app developed by Dr. Aleksandr Kogan, a professor of psychology at Cambridge University who collected data that was later utilized by Cambridge Analytica and may be familiar with the methodology used to utilize the data for political gain. Also, Nigel Oakes ' first company, Behavioral Dynamics Institute (BDI), also has links with the Ministry of Defense, while SCL Group and BDI seem to have maintained its presence in Singapore. News Lens news agency also has asked the Ministry of Defense, Ministry of Home Affairs, and the Prime Minister's Office to ensure that the Singapore government never has access to data from the Facebook application " myPersonality ", or engages in utilizing the data collected for academic research purposes, obtained illegally from Facebook by Cambridge Analytica on 65,000 Singaporeans, to develop an Audience Target analysis targeting Singaporean society. Facebook users in Singapore say that although they do not take drastic steps to boycott Facebook, they are now more aware of what they will share.¹⁴

2) Yahoo Case Data Theft in 2017

According to Verizon Communications, which Yahoo acquired in 2017, as many as 3 billion in Yahoo users' email accounts hacked from 2013 to 2014 and that means that all email accounts hacked. This case was recorded as the largest hacking case in history. Marissa Mayer, Yahoo's former CEO

¹³ Quoted from <https://international.thenewslens.com/article/93805>, (accessed May 26, 2018).

¹⁴ Neo Chai Chin and friends, "65,000 Singapore users may be hit in Cambridge Analytica scandal; privacy watchdog 'concerned'", *Today Online*, April 05, 2018, <https://www.todayonline.com/singapore/more-65000-singapore-facebook-users-may-have-been-affected-cambridge-analytica-data-breach>, (accessed May 26, 2018).

said until now Yahoo has not known how the system can be hacked. However, a group of hackers based in Eastern Europe are reportedly secretly selling Yahoo information, based on information compiled by InfoArmor, a cybersecurity firm that monitors the 'dark side' of the internet. Since then, there have been at least three buyers, two of whom are known as 'spammers' and the other is allegedly interested in using Yahoo's data for espionage activities, which pay \$ 300 thousand for a set of Yahoo databases, as revealed by InfoArmor. Yahoo said, data theft occurred in 2013, and 2014 have no relevance.¹⁵ The US Department of Justice said a man named Karim Baratov was found guilty in court Tuesday 28 November 2017 for hacking Yahoo email accounts and selling email passwords to a Russian agent. Not only Baratov, in its statement, but the US Department of Justice also announced three others detained men, including two Russian agents (FSB) for hacking into 500 million Yahoo accounts.¹⁶ The prosecutor's office said the two FSB agents named Dmitry Dokuchaev and Igor Sushchin directly paid the hacker group and employed Alexsey Belan, one of the most wanted FBI cybercriminals, to Yahoo's boss. When both FSB agents know that their target has a non-Yahoo email account, they also hire the services of Baratov's hacking. He is known to get paid for the action to break into 80 email accounts. Some of the accounts being targeted belong to Russian officials, CEOs of metal companies, to leading bankers. At least, out of 80 accounts targeted by Baratov are owned by Google. The US Department of Justice also said Baratov admitted he unlawfully broke into 11 thousand email accounts both at the request of both FSB agents and other consumers. Hacking is done from 2010 to March 2017, before being detained by the Canadian government. According to Baratov, he advertises his services on the Russian-language website. He also gains access to his victims' accounts with fake correspondence designed to look as if sent from the relevant email host. Baratov pleaded guilty to charges of conspiracy in violation of the Computer Fraud and Abuse Act and eight allegations of identity theft.¹⁷

From the information of various data theft cases in various countries it can be concluded that: first, data theft is a big crime that can be done anywhere and by anyone against one's data. Voluntarily a consumer provides his data to a company. The Company is obliged to retain and not be able to distribute or provide to any other party except by the consent of the

¹⁵ Muhamad Imron Rosyadi, "Misteri Hacker Pembobol 3 Miliar Akun Yahoo", *Detik*, October 04, 2017, <https://inet.detik.com/security/d-3669890/misteri-hacker-pembobol-3-miliar-akun-yahoo>, (accessed June 10, 2018).

¹⁶ From <https://www.justice.gov/opa/press-release/file/948201/download>

¹⁷ Agustin Setyo Wardani, "Begini Pengakuan Hacker Pembobol Jutaan Akun Yahoo", *Liputan6*, November 29, 2017, <https://www.liputan6.com/tekno/read/3179946/begini-pengakuan-hacker-pembobol-jutaan-akun-yahoo>, (accessed June 15, 2018).

consumer owning such personal data. Secondly, in the presence of various cases of personal data theft that have occurred in various countries, Indonesia should have anticipated that this does not happen by making clear legal protection to get out of the problem quickly. It is not done by Indonesia.

2. The actuality of Privacy Data Protection in International Law and National Law in Indonesia

The history of the development of the protection of privacy laws in Indonesia cannot be separated from the development of international legal instrument itself. National law in Indonesia is influenced by international law and based on international law by not neglecting local values such as Pancasila and the 1945 Constitution of the Republic of Indonesia. The following will be conveyed on the international developments and actions that have been done by Indonesia to implement the international rules.

a. Evolution of the Protection of Privacy Rights in International Law Instruments

The protection of privacy is a fundamental right protected by the laws and by international conventions. The protection of privacy rights recognized by international law start after the World War II, precisely following the establishment of the United Nations (UN) which replaced the Society of Nations. Alan F Westin was a professor of Public Law and Government Emeritus, divides the development of privacy following phases:¹⁸

- 1) After World War II (1945-1960) or called The First Privacy Baseline. In the age of information technology has not developed and people trust the government and business sector to collect personal information they do not object when their information is accessed and stored. The information collected is information standards and usually for the benefit of population censuses.
- 2) From 1961-1979, it was called The First Era of Contemporary Privacy Development. This period begins with data search technology (data surveillance) used by government and industry sector. Around 1960, began to find third-generation computer technology used by the government to start storing data primarily by the bank. The personal information of the population is being accessed and stored by the government. At this time, the public began to worry about privacy.
- 3) From 1980-1989 called The Second Era of Privacy. At this time, began to find VDT technology (video display terminals) and PC (personal computer), making it an easier way of collecting data at a cheaper cost.

¹⁸ This division is only in the period after World War II and specifically for developed countries such as Europe and the United States.

Internationally, countries are beginning to develop a Guideline that protects personal data, especially in EU countries.

- 4) From 1990-2003 called The Third Era of Privacy. At this time privacy becomes a very important issue, especially in the European Union, the United States, parts of Asia and Central America. This period is called the advancement of telecommunication technology informatics and media so that information can be accessed and collected by anyone with a lot. This period is also called the period of the globalization of privacy issues as countries outside the EU and US states begin to realize privacy and begin to make arrangements to protect privacy such as in Canada, Australia, New Zealand, some Asian countries such as Japan, Hong Kong, India, South Korea, and Taiwan.¹⁹

After the establishment of the United Nations in 1945, the rights to privacy are governed in several international instruments:

- 1) Universal Declaration of Human Rights (UDHR), 1948, is stipulated in Article 12 that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honors and reputation. Everyone has the right to the protection of the law against such interference or attacks" UDHR is the most important international instrument because it has been successfully agreed almost the whole country as a reaction to World War II and Germany's actions against the Jews.²⁰
- 2) International Covenant on Civil and Political Rights (ICCPR), 1966, stipulated in Article 17 paragraph (1), no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Next paragraph (2) everyone has the right to the protection of the law against such interference or attacks.
- 3) European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 1950, provided for in Article 8 paragraph (1), everyone has the right to respect for his private and family life, his home, and correspondence. Further paragraph (2), there shall be no interference by public authority.
- 4) The American Convention on Human Rights (1979), provided for in Article 11 paragraph (1), "Everyone has the right to have his honor respected and his dignity recognized. No one may be the subject of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on His Honor

¹⁹ Alan F. Westin, "Social and Political Dimension of Privacy", *Journal of Social Issues*, 59, (2003), pp. 1-10.

²⁰ Marc Freeman and Gibran Van Ert, *International Human Rights Law*, Canada: Irwin Law Inc., (2004), p. 70.

reputation. "Furthermore, paragraph (2), states that "Everyone has the right to protection of the law such as interference or attacks."

- 5) Cairo Declaration of Islamic Human Rights, 1990, outlined in article 18b, "Everyone shall have the right to privacy in his conduct of his family, about his property and his relationships. It is not permitted to spy on him, to him under surveillance or to besmirch his good name. The State shall protect him from the arbitrary interface. "Next Article 18c, states" A private residence is inviolable in all cases. It will not be written without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted."

Based on a report submitted by the Elsam Non-Governmental Organization in 2015, in August 2014, more than 100 countries in the world have enacted protection laws. The best provision is that owned by Canada and the European Union was known as "The 1995 Data Protection Directive". The Directive is a provision created by the Council of the European Union which gives orders to each member of the European Union to adjust the national provisions of each country by EU standards.²¹

b. Indonesia Action to provide Legal Protection

In Indonesia, the importance of protecting the right to privacy is increasingly sticking along with the increasing number of cell phones and internet users.²² Therefore, since the amendment to the 1945 Constitution, this seems to bring fresh air to the protection of the right to privacy and then added to the ratification of conventions relating to the protection of the right to privacy. Arrangements on the protection of personal data in Indonesia can at least be seen from various regulations such as the Constitution, the Law, and the Government Regulation. The following are rules in Indonesia that can be used as legal protection of privacy data protection.

1) National Regulations on the Protection of Privacy Rights

²¹ The Institute for Policy Research and Advocacy (Elsam), *Privasi 101 Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi*, (2015), p.37

²² Based on data from the Central Bureau of Statistics, within a period of five years (2010 to 2015) there was an increase in the number of cellular telephone customers (62.3 percent or from 211,200,297 to 338,948,340 customers. This information can be accessed at <https://www.bps.go.id/statictable/2015/09/22%2000:00:00/1844/jumlah-pelanggan-telepon-menurut-jenis-penyelenggaraan-jaringan-2010-2015.html>. Based on data from the Indonesian Internet Service Provider Association (Asosiasi Penyelenggara Jasa Internet Indonesia), it was reported that in 2014 Indonesian internet users reached 88.1 million, and in 2016 it rose to 132.7 million, meaning that there was an increase of 66.3 percent where the largest concentration was in Java. Information can be accessed at <https://apjii.or.id/downfile/file/surveipenetrasiinternet2016.pdf> accessed on 2nd august 2018.

- a) Article 28 paragraph (1) The 1945 Constitution of the Republic of Indonesia fourth amendment, namely:
"Everyone is entitled to personal protection, honorary family, dignity, and property under his control, and is entitled to a sense of security and protection from the threat of fear to do or not to do something that is a human right."
- b) Law no. 12 on 2005 of Ratification of ICCPR.
- c) Law no. 39 on 1999 of Human Rights, Article 29 paragraph (1) states that everyone is entitled to personal, family, honor, dignity, and property protection. Further paragraph (2) that everyone has the right to recognition before the law as a private human wherever he is.
- d) Law no. 36 of 1999 on Telecommunication, Article 40 is stated, every person is prohibited from intercepting information transmitted through telecommunication network of any kind. Furthermore, in Article 42, telecommunication service providers shall keep confidential information transmitted and received by telecommunication service subscribers through telecommunication networks. In paragraph two it is possible to provide customer information where necessary for judicial proceedings.
- e) Law no. 11 of 2008 on Information and Electronic Transactions, Article 26 of the Law on ITE, states:
 - I. The use of any information through electronic media concerning the personal data of a person shall be made with the consent of the person concerned.
 - II. Any Person whose rights are violated as referred to in paragraph (1) may file a lawsuit for damages incurred under this Act.
 - III. Act No. 19 of 2016 on Amendment to Law Number 11 on 2008 of Information and Electronic Transactions.
 - IV. Government Regulation of the Republic of Indonesia Number 82 on 2012 of Electronic System and Transaction Management.
- f) Regulation of the Minister of Communications and Informatics No. 20 of 2016 on Personal Data Protection (PDP) is set on November 7, 2016.
- g) Personal key rule data outlined in the Ministerial Regulation No 20 of 2016 on Personal Data Protection (PDP) established 7 November 2016, enacted and effective from 1 December 2016. The Regulation states that Personal Data is a different personal data which stored, directed, and kept true and of anonymity.

In this rule, an electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal rules on the protection of personal data which must pay attention to aspects of the application of technology, human resources, methods, and costs. The owner of the personal data, is entitled to the confidentiality of his data; have the right to file a complaint in the resolution of a personal data

dispute; entitled to access to obtain historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system.

The government through the Ministry of Communications and Informatics must be able to ensure Facebook adheres to the provisions in Indonesia because although ownership of Facebook is in the United States, the company is conducting operations in Indonesia and used by Indonesian citizens. It is at this level that the interests of the Government of Indonesia are closely related as this concern the safety of personal data of its citizens. The provisions that should get attention from the Facebook side in particular namely the Regulation of the Minister of Communications and Information No. 20 of 2016 on Protection of Personal Data in Electronic Systems.

The Ministry of Communications and Informatics requested Facebook to guarantee the protection of personal data, to provide the results of the application audit plans and features developed by the partners and to close the application or quiz feature of personality tests related to Cambridge Analytica Case. It was conveyed through the First Warning Letter (SP I) by the Ministry of Communications and Informatics on April 5, 2018. Furthermore, due to no response from the Facebook, on Tuesday, April 10, 2018, again sent the Second Written Letter (SP II) for misuse of Data Personal Users by Third Parties. In SP II signed by the Director General of Informatics Applications Samuel Abrijani Pangerapan. This letter contains a warning back to Facebook Indonesia to provide confirmation and explanation about the abuse of personal data users by third-party applications that use the Facebook platform.

As a result, the Government has received an official answer from Facebook. Steps those have been done include Facebook has conducted an audit of the leakage of personal data from users, although the results of the audit have not been submitted in complete and detailed to The Ministry of Communication and Information Technology. Facebook has provided detailed information on third-party access to user pass log in data in the Cambridge Analytica application. And, Facebook has updated policy and feature changes so that third parties do not use the user's data. But the Ministry of Communications and Informatics assessed the explanation of the Facebook is still inadequate and has not included data requested by the Government of Indonesia so that the steps and stages of compliance with legislation and regulations are done in protecting the rights of the community.

Are the steps taking by the Government sufficient and by the applicable provisions, and can Indonesia make policy breakthroughs to protect the interests of its citizens. The steps taken by the Government of Indonesia are not enough to make the perpetrators of personal data breach deterrent. The heaviest sanction that can be given is in the form of closing access in

Indonesian territory. The basic thing that needs to be considered and more effective is to build public awareness. The Ministry of Information and the Government of Indonesia must be able to provide and enrich people's knowledge of the importance of privacy data. It can be done in two major stages, namely short-term and long-term actions. Short-term actions can be carried out through socialization into the community. As for long-term action, namely by providing basic education starting from the elementary school level, junior high school, and high school. Citizen privacy data is a reflection of the country itself. Therefore, protection of the security of private data must have a place as a basic right that needs to be protected and attached to each. Such protection should not appear when data theft has occurred. The last and important thing to do, Indonesia must have a Privacy Commissioner that has the power to conduct investigations, follow up on reports and impose sanctions when they find an organization that violates the law.

Bibliography

A. Books

- David, Robert. (2004). *A dictionary of Human Rights*. Europa, London, New York.
- Freeman, Marc and Gibran Van Ert. (2004). *International Human Rights Law*. Canada: Irwin Law Inc.
- The Institute for Policy Research and Advocacy (Elsam). (2015). *Privasi 101 Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi*.
- Norman E. Bowie, Karim Jamal. (2006). *Privacy Rights on the Internet: Self-Regulation or Government Regulation*. Business Ethics Quarterly. <https://doi.org/10.5840/beq200616340>
- Raymond, Wacks. (2013). *Privacy and Media Freedom*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199668656.001.0001>
- Westin, A.F. (1967). *Privacy and Freedom*. New York: Atheneum

B. Journal

- Westin, A.F. "Social and Political Dimension of Privacy," *Journal of Social Issues*, 59, (2003).

C. Legislations

- International Covenant on Civil and Political Rights (ICCPR)
- International Covenant on Economic, Social and Culture Rights
- Law No. 11 on 2008 of Information and Electronic Transactions
- Law No. 12 on 2005 of Ratification of the International Covenant on Civil and Political Rights.

Law No. 19 on 2016 of the Amendment of Law No. 11 No. 2008 of ITE
 Ministry Regulation No. 12 on 2016 of Registration of Telecommunications
 Service Customers
 Ministry Regulation No. 20 on 2016 of Personal Data Protection (PDP)
 The Constitution of the Republic of Indonesia 1945
 Universal Declaration of Human Rights

D. World Wide Web

- Antara. "Data Bocor, Elsam: Menutup Facebook Bukan Solusi", *Tempo*, April 11, 2018, <https://bisnis.tempo.co/read/1078332/data-bocor-elsam-closing-facebook-not-solution>, (accessed May 26, 2018).
- Antika, Asih. "Tahukah Kamu, Kapan Internet Pertama Kali Masuk Ke Indonesia", *Official website* of Dewan Teknologi Informasi dan Komunikasi Nasional (WANTIKNAS), October 03, 2016, <http://www.wantiknas.go.id/2016/10/03/tahukahkamu-kapan-internet-pertama-kali-masuk-ke-indonesia/>, (accessed May 17, 2018).
- Australia Plus. <http://www.australiaplus.com/indonesian/berita/fb-indonesia-di-bareskrim/9674954>, (accessed May 26, 2018).
- Ayuwuragil, Kustin. "Kronologi Pembobolan Facebook oleh Cambridge Analytica", *CNN Indonesia*, March 03, 2018, <https://www.cnnindonesia.com/teknologi/20180322194919-185-285163/kronologi-pembobol-facebook-oleh-cambridge-analytica>, (accessed June 10, 2018).
- Bohang, Fatimah Kartini. "DPR Beri Waktu Facebook 1 Bulan", *Kompas*, April 17, 2018, <https://tekno.kompas.com/read/2018/04/17/16240047/dpr-beri-waktu-facebook-1-bulan/>, (accessed June 10, 2018).
- Chin, Neo Chai and friends, "65,000 Singapore users may be hit in Cambridge Analytica scandal; privacy watchdog 'concerned'", *Today Online*, April 05, 2018, <https://www.todayonline.com/singapore/more-65000-singapore-facebook-users-may-have-been-affected-cambridge-analytica-data-breach>, (accessed May 26, 2018).
- Elsam. <http://elsam.or.id/2018/05/elsam-menghadiri-rapat-dengar-pendapat-umum-dari-panja-pengamanan-data-ponsel-komisi-i-dpr-ri/>, (accessed 10 June 2018).
- Encyclopedia of Philosophy (Fall 2012 Eds), Edward N Zalta (ed). Can be downloaded at <http://plato.stanford.edu/archives/fall2012/entries/privacy/>.
- Kominfo. https://www.kominfo.go.id/content/detail/13163/rudiantara-bakal-inskiasi-regulasi-soa-l-konten-medsos/0/sorotan_media, (accessed May 26, 2018).

- Prosser, William, as quoted in DeCew, Judith, "*Privacy*", The Stanford rd
- Rosyadi, Muhamad Imron. "Misteri Hacker Pembobol 3 Miliar Akun Yahoo", *Detik*, October 04, 2017, <https://inet.detik.com/security/d-3669890/misteri-hacker-pembobol-3-miliar-akun-yahoo>, (accessed June 10, 2018).
- Tempo. <https://tekno.tempo.co/read/1080112/dpr-bert-facebook-besok-bahas-skandal-data>.
- The New Lens. <https://international.thenewslens.com/article/93805>, (accessed May 26, 2018).
- Wardani, Agustin Setyo, "Begini Pengakuan Hacker Pembobol Jutaan Akun Yahoo", *Liputan6*, November 29, 2017, <https://www.liputan6.Com/tekno/read/3179946/begini-pengakuan-hacker-pembobol-jutaan-akun-yahoo>, (accessed June 15, 2018).
- Yusuf, Oik, "Data 1 Juta Pengguna Facebook Indonesia Dicuri", *Kompas*, April 05, 2018, <https://tekno.kompas.com/read/2018/04/05/10133697/data-1-juta-user-facebook-indonesiadicuri>, (accessed June 12, 2018).