Volume 1 Issue 2, 2019: pp. 61-68. Copyright © 2019 Lampung Journal of International Law. Department of International Law, Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia.
p-ISSN: 1978-5186 E-ISSN: 2723-2603
http://jurnal.fh.unila.ac.id/index.php/lajil

LEGAL PROTECTION OF PRIVACY DATA THROUGH ENCRYPTION TECHNOLOGY

Thania Christy Corne
PT. Indo Energy Solutions
Thaniachristy97@gmail.com

Abstract

Technological developments in the era of globalization bring humans into the digital age. All things will directly contact with an electronic system. And so with the data, some of the data among this world is privacy. That's why encryption is needed to be applied. Initially, encryption was used as a privacy data protector, but in its development encryption gave birth to problems in the legal field. Where criminals use encryption as a shield for their crimes. Therefore, legal issues arise, whether for reasons of government or state security can have access to one's privacy data. How does international or national law regulate the issue of using decryption of encryption technology? The method used in this paper is a juridical-normative comparative legal research method. The result shows that international law does not regulate the use of encryption in protecting privacy data in the digital world comprehensively because some of the countries claim that the use of encryption is a part of human right, on the other hands some country has another vision on national security.

Keywords: *Protection, Privacy Data, Encryption, International, National.*

How to Cite: Thania Christy Corne, "LEGAL PROTECTION OF PRIVACY DATA THROUGH ENCRYPTION TECHNOLOGY," *Lampung Journal of International Law (LaJIL)* 1, no. 2 (2019): 61-68.

DOI: https://doi.org/10.25041/lajil.v1i2.2027

A. Introduction

The use of the internet in various fields of life not only makes things easier but also gives birth to some problems, including in the legal field. One of the legal issues related to information technology is data privacy, where internet technology allows access to someone's privacy data freely. This happens because the traffic of sending data and information is increasingly global, and the concept of open system authentication (OSA)[1] of a network makes it easy for someone to enter into another network. Often when someone wants to do a transaction or registration in an organization or mailing list on the internet, the user must send his personal data first and this data is recorded/stored in an electronic system. At this time, the data leakage occurs and is used by various parties such as companies or individuals. It often happens that internet users then receive various advertising messages (later referred to as junk mail) in their inboxes, which is most likely originated from the leakage of personal data that has been given it.[2]

On the other hand, non-governmental organizations today urged the government to be able to follow up on the public's right to get access to information on the administration of the government system to the people listed in the Freedom of Information Bill. This is because a good government can be marked by a transparent government system and is able to increase public participation and increase public accountability to the government elite. Meanwhile, in fact, there are also human rights that function to protect personal interests, namely the interests of privacy, correspondence and dignity of people (honour and reputation). Even ideally, the public interest is aimed at protecting the interests of the individual because the public is the sum total of all individuals. The balance of these two interests is a dilemma in law enforcement, where

[1] Open System Authentication (OSA) is the process by which computers can gain access to wireless networks that use the Wired Equivalent Privacy protocol (a data security method that uses keys for authentication to access points).
[2] Asri Sitompul, *Hukum Internet, Pengenalan Mengenai Masalah Hukum di Cyberspace* (Bandung: Citra Aditya Bakti, 2001), 25.

guarantees of individual interests are also harmonized with the interests of the community or other individuals. Although on the one hand, there are provisions regarding freedom of information; on the other hand, there are also provisions regarding data protection and protection of personal confidentiality of information confidentiality. One interesting case example of inequality in law enforcement on national security and privacy protection is the case between the Federal Bureau of Investigation (FBI) and Apple Company (Apple Inc.). Where in 2016, precisely after the San Bernardino shootings, Apple and the FBI launched a public battle over the availability of encryption, which basically cannot be solved in one of the consumers' devices. It is happening because Apple has increasingly increased the use of encryption that is classified as strong and secure in its products, so when the FBI tried to open a security code on the iPhone 5C used by one of the shooters in the attack in San Bernardino, California, which killed 14 people in December 2015 In the past, there were many difficulties in solving the security code, so this became an obstacle for the FBI in solving the shooting case. Right on February 16, 2016, in response to a request from the United States Department of Justice, federal judges ordered Apple to create a custom version (backdoor) of its iOS operating system that would allow investigators in this case to obtain mobile security features. Apple's Chief Executive Officer, Tim Cook, responded in an open letter, in which he stated that the government's demands were an "invasion of privacy" with "dire" consequences.

There is a discussion among technology experts, but most of the technology experts, law professors, technology companies and human rights organizations support Apple's policy in this matter.[3] The broad view among those who oppose FBI requests is if Apple is forced to modify its software to unlock the cellphone password, it will set a precedent that allows the US government-and potentially other governments - as well as rival technology companies Apple to weaken or block their encryption by providing a backdoor for intelligence and other security services.

In the digital era as it is today, the use of encryption is part of protecting data privacy. This is because encryption technology can protect communications and data from spying. Unfortunately, many governments are very critical of encryption and have made policies and legal actions to prevent or limit the ability of individuals to use encryption. Countries such as Pakistan, India and Cuba prohibit encryption. Government officials, including those in France, the United Kingdom and the United States, have criticized encryption over fears that it will cause the "going dark" intelligence team.[4] This is a fact that the use of a strong encryption system can pose challenges to access information intended for law enforcement.

Based on the impact and laws governing the use of encryption technology, the author is interested in discussing: How does international law regulate the use of cryptographic technology in protecting data privacy? How does Indonesian law regulate the issue of using cryptographic technology as a tool to protect data privacy? This type of research used is juridical-normative-comparative, which is legal research literature examines a problem based on legal norms contained in international regulations and legislation and comparing between two groups or more than a certain variable to produce a conclusion. The method in data collection used to process the data in this study is the library study technique method, namely by studying the provisions of the legislation, international guidelines, books, documentation, journals, and accessing data on the internet related to issues within the scope of international law and the scope of national law. Data analysis was carried out by outlining and giving the meaning of each data obtained into sentences that are detailed, orderly, effective, logical and not overlapping to facilitate the author in interpreting and analyzing the data which then concludes response to the problems contained in this paper.

B. Discussion

1. International Provisions that Regulate Encryption Technology in Protecting Data Privacy

There is no specific regulation governing the use of encryption technology in international law. Still, two international organizations, the Organization for Economic Cooperation and Development (OECD) and Amnesty International have issued guidance on the use of encryption to protect privacy data which is then expected to be a reference in the formation of International regulations regarding the use of encryption, including:

[3] A list of amicus briefs in support of Apple for the 22 March 2016, http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march22/80635402/, accessed on 11 November 2018 at 20.22 WIB.

[4] Going dark is a term for blind, which in this case means the concern that part of online communication cannot be accessed by law enforcement or intelligence services.

a. The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data

The OECD formulated the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data for the first time in 1980 to address problems arising from increased use of personal data and global economic risks resulting from restrictions on the flow of information across national borders. This 1980 guide contains a set of privacy principles that were first agreed upon internationally. However, as patterns change in the use of personal data, as well as new approaches to privacy protection, the 1980 guidelines need to be updated. In 2013, the OECD released the 2013 guidelines for The Protection of Privacy and Transborder Flows of Personal Data as a result of the revision of the guidelines for The Protection of Privacy and Transborder Flows of Personal Data 1980. During the past three decades (1980-present), personal data has an increasingly important role in both the economic, social and daily life sectors. Information and communication technology innovations have influenced business flow, government administration, and individual activities. The volume of personal data collected, used, and stored is very broad and continues to increase. At the same time, this condition increases the risk to individual privacy. Personal data is increasingly used in almost every human activity. This increased risk indicates the need for more effective protection to protect privacy.

Based on the formulations written in these guidelines, the author can conclude that although these guidelines do not mention and regulate the provisions regarding encryption technology, explicitly in Chapter, I of the fifth section of the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data has arrangements regarding encryption technology must be made immediately considering the functional use of this technology is very effective in protecting personal data. These guidelines provide obligations for member states to make national regulations with specific principles concerning the protection of privacy and individual freedom relating to privacy data in networks recorded in cookies so as not to be misused, this becomes a universal and applicable legal formulation for member countries.[5]

b. Amnesty International Policy on Encryption

This non-governmental organization (NGO) issued a research report titled "Encryption: A Matter of Human Right" with index number: POL40 / 3682/2016 on March 22, 2016, which outlines the human rights issues related to the use of technology encryption in digital communications and services. This research report not only discusses facts that have occurred globally with regard to cases involving national security and privacy protection for personal data due to the use of encryption technology but also includes international policies on the use of encryption technology which are still classified as recommendations for can be used as a reference for countries in formulating national and international policies later. International policy recommendations on encryption technology issued by Amnesty International represent Amnesty International's position with respect to human rights and the standards that apply to the use of encryption devices and services in digital technology by right-holders, and the potential restrictions on their use by countries. These policy recommendations will be reviewed and revised as needed on an ongoing basis.

In these guidelines, it is explained that in the digital age, the use and access to encryption is an important part of the right to protect privacy and freedom of expression, information and opinions, and also have an impact on the rights of freedom of association, association and other human rights. Encryption is a very important tool for human rights defenders, activists and journalists, who all depend on it with increasing frequency to protect their safety and those of others. Amnesty International believes that countries must facilitate the use of encryption and must not violate, or allow interference by others, in ways that cannot be justified.

Both of these guidelines are considered insufficient to be used as an international regulation that can be universally applied. For this reason, each country has its own rules governing the use of encryption technology. The diversity of laws and regulations used in various countries proves that encryption technology is very important to regulate. Still, currently, there is no single regulation regarding the use of encryption products and services that can be applied universally and apply in all countries. Through the matrix above the writer tries to show that the regulation of the use of encryption across countries has a very significant difference. Each country has its own opinion based on their needs to decide whether the use of encryption is an attempt to protect privacy or is a form of control for national security. The debate that exists

[5] Albert J. Marcella Jr. dan Carol Stucki, *Privacy Handbook: guidelines, exposures, policy implementation, and international issue* (New Jersey: John Wiley & Sons, Inc, 2003), 74.

in the international cyber world today is the issue of privacy which is a part of human rights can be legally protected through the use of encryption technology. The author himself believes that the use of encryption technology is a form of protection for privacy data so that in the name of human rights, the government should not have access to encrypted communication data.

2. Encryption Technology Regulations in Protecting Data Privacy according to National Law

National legislation does not contain provisions regarding the use of encryption technology, but in the implementation of law enforcement efforts tapping is legalized. Tapping is a form of action of encrypting encrypted data. National law authorises wiretapping on the grounds as an aid in the collection of digital evidence.

Law Number 11 the Year 2008 concerning Information and Electronic Transactions jo. Law Number 19 Year 2016 concerning Amendments to Law Number 11 the Year 2008 concerning Information and Electronic Transactions explicitly mentions prohibited acts regarding electronic information and transactions. Some examples of prohibited acts in the Information and Electronic Transactions Law are access to electronic systems belonging to others by breaking, exceeding, or breaking into security systems to obtain information, as well as tapping on information on other people's computers unless done by a special party with special permission (such as for law enforcement efforts). The contents of this regulation are good enough, but there is no regulation regarding encryption technology that often plays a vital role in data protection. Encryption technology is needed to ensure the security of data owned by individuals and institutions to maintain confidentiality. In this Information and Electronic Transactions Law, tapping activities are legalized under the pretext of law enforcement efforts, which of course can only be done by a special body that already holds a special permit to do so. Thus it can be said that if wiretapping is legalized, all forms of encryption technology, which is necessary in the proof as evidence, the government may require companies or individuals to decrypt or even create a "backdoor" to be able to access encrypted data.

The action to be able to retrieve data or information stored in electronic storage media can be used as new evidence.[6]In Indonesia, the authority for investigators and investigators to conduct wiretapping is regulated in statutory provisions. But in the implementation of wiretapping in the field, this issue has become the most discussed and debated issue today. Especially for reasons because tapping involves protecting one's privacy and all kinds of forms related to the implementation of one's duties.

Tapping referred to as decryption, has not been normatively regulated in a separate law. While in practice continues to cause controversy about the procedures for tapping/decryption. The arrangements are still scattered in various laws. So that there is no general guideline for the Police, Attorney General's Office, National Narcotics Agency, the Corruption Eradication Commission, in conducting wiretapping, each tapping technique is in accordance with the orders of each institution in the law. Whereas on the other hand, some people consider that the action of wiretapping/decryption carried out by each law enforcement officer is contrary to human rights, especially regarding the protection of privacy.

Tapping arrangements are also contained in other legislation, such as Government Regulation Number 19 of 2000 concerning the Joint Team for Corruption Eradication and strictly stated in Article 87, Article 88, Article 89. Other regulations, namely Government Regulation Number 52 of 2000 concerning Telecommunications, Regulation of The Minister of Communication and Informatics Number 11 of 2006 concerning Technical Tapping of Information, Regulation of The Minister of Communication and Informatics Number 1 of 2008 concerning Recording of Information for State Defense and Security, Regulation of The Head of Police In The State of The Republic of Indonesia Number 5 of 2010 concerning Tapping Procedures at the Republic of Indonesia National Police Monitoring Center and the highly confidential Operational Procedures of the Corruption Eradication Commission are inaccessible.

Regulation of The Minister of Communication And Informatics Number 20 Year 2016 concerning Protection of Personal Data in the Electronic System has stipulated that any personal data stored in the electronic system must be in the form of encrypted data. This is contained in Article 15 paragraph (2): "Personal Data stored in an Electronic System must be in the form of encrypted data." the government as contained in Article 23 paragraph (1), namely:

"For the purposes of the law enforcement process, the Electronic System Provider is required to provide Personal Data contained in the Electronic System or Personal Data generated by the Electronic System at the request of a legitimate request from law enforcement officials based on statutory provisions."

[6] Al Wisnubroto dan G. Widiartana, *Pembaharuan Hukum Acara Pidana* (Bandung: Citra Aditya Bakti, 2005), 100-101.

Arrangement of restrictions on the privacy rights of every citizen or restrictions on human rights through tapping arrangements is contained in the law: Narcotics; Psychotropic drugs; Telecommunication; Corruption Crime; Criminal Acts of Terrorism; Trafficking in Persons; Information and Electronic Transactions; State Intelligence; Corruption Eradication Commission; Advocate; Judicial Commission; and other laws, by law to become legal. By law, the wiretapping provisions stipulated in various laws do not conflict with the basic norms (constitution), especially Article 28J paragraph (2) of the 1945 Constitution.

The state itself must maintain, serve, protect, and create comfort, security for Indonesian citizens with one of the legal instruments applied in criminal law. Considering the increasing number of crimes, especially extraordinary crimes, and these crimes have a serious impact on the interests of the state and the interests of the people, regulating wiretapping in the various laws mentioned above is very urgent.

The wiretapping provisions stipulated in various laws mentioned above are not solely intended to carry out abuse of state power. Still, it is done with the intention solely to guarantee recognition and respect for the rights and freedoms of others and to fulfil demands justice by moral considerations, religious values, security and public order in a democratic society.

Various laws and regulations in Indonesia do not include regulations on the use of encryption technology, which in this case is intended as data privacy protection. The government can own private data belonging to each individual. The national security portal in Indonesia severely restricts the freedom of individuals to be able to store their private data. The following is a comparison of Indonesian laws and regulations in the use of encryption.

National Regulation	**General right to encryption**	**Mandatory minimum or maximum encryption strength**	**Licensing/registration requirements**	**Import/export controls**	**Obligations on providers to assist authorities**	**Obligations on individuals to assist authorities**
1945 Constitution	Explicitly in Article 28F	-	-	Explicitly in Article 33 paragraph (2)	Explicitly in Article33 paragraph (2)	Explicitly in Article28 J paragraph (2)
Law Number 11 Year 2008 jo. Law Number 19 Year 2019 concerning Amendments to Law Number 11 Year 2008 concerning Information and Electronic Transactions	-	-	-	[tapping] Explicitly in Article 31 paragraph (1) dan (2)	-	-
Law Number 5 of 1997 concerning Psychotropics	-	-	-	[tapping] Explicitly in Article 55 letter c (by the police)	-	-
Law number 35 of 2009 concerning Narcotics	-	-	-	[tapping] Explicitly in Article1 number (19) and Article 75 letter i (by the national narcotics agency investigator)	-	-

Law Number 36 of 1999 concerning Telecommunications	-	-	-	Article 42 paragraph (1)	Article 42 paragraph (2) (by the company to be given to the police)	-
Regulation of The Minister of Communication And Informatics Number 20 Year 2016 concerning Protection of Personal Data	Article 15 paragraph (2)	-	-	-	Article 23 paragraph (1)	-

Based on this table, the author believes that the regulation regarding the use of encryption technology has not been sufficient in dealing with the issue of privacy, data protection. Indonesian laws are only focused on the government's authority to be able to access and even have the right to obtain data on each individual in the electronic system with reasons for law enforcement and protection of national security. Thus, the regulation is concretely regulates the use of encryption as a protection for data privacy starts from the regulation of the rights of each individual to be able to use encryption technology, restrictions on the use of encryption, requirements for encryption product and service providers, control of encryption controls, to provider obligations, and encryption users in helping authorities enforce the law.

C. Conclusion

Encryption technology is considered very important in protecting data privacy. Regulations regarding the use of encryption technology in international law have been established in several guidelines such as the OECD Guidelines for The Protection of Privacy and Transfers of Personal Data and Amnesty International Policy on Encryption. It allows every country to decrypt individual personal data based on sovereignty, national security and public policy, but *vice versa* as stipulated in the UN Guiding Principle on Business and Human Rights. Companies have the responsibility to respect human rights independently and regardless of the ability and will of the state, but these regulations cannot be applied globally because the legalization is only soft law. International arrangements regarding encryption technology that apply to all countries in the world have not been established until now. The regulation of encryption technology is very important because the problem of using encryption technology services and services, and their description are closely related to human rights.

The national regulation regarding encryption technology is not written for its use. In several national legislation, it is stated that the wiretapping activity (which is a special continuation in the form of decryption measures on the use of encryption services and services) is legalized under the pretext of being a law enforcement effort, which of course, it can only be done by a special body that already has a special permit to do it. The normative authority of wiretapping to law enforcement officials does not conflict with human rights. The authority of wiretapping/decryption of the use of encryption technology, although not yet concretely written, has fulfilled the principle of legality and is in accordance with the basic norms in Article 28J paragraph (2) of the 1945 Constitution.

References

A list of amicus briefs in support of Apple for the March 22 2016, d http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march22/80635402/, accessed on November 11, 2018, at 20.22 WIB.

Al Wisnubroto & G. Widiartana, *Pembaharuan Hukum Acara Pidana*, Bandung: Citra Aditya Bakti, 2005.

Albert J. Marcella Jr. & Carol Stucki. *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issue*. New Jersey: John Wiley & Sons, Inc, 2003.

Corruption Eradication CommissionStandard Operational Procedures

Evan Perez and Tim Hume, *"Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone,"* CNN, February 18, 2016, https://www.cnn.com/2016/02/16/us/san-bernerdino-shooter-phone-apple.

Government Regulation Number 19 of 2000 concerning the Joint Team for Corruption Eradication

Government Regulation Number 52 Year 2000 concerning Telecommunications Operation

Hon. Michael Kirby. *30th anniversary of the OECD Privacy Guidelines.* www.oecd.org/internet/interneteconomy/49710223.pdf., accessed on June 22, 2019, at 21.40 WIB.

Law Number 11 Year 2008 concerning Information and Electronic Transactions jo. Act Number 19 of 2016 concerning Amendments to Act Number 11 of 2008 concerning Information and Electronic Transactions

Law number 35 of 2009 concerning Narcotics

Law Number 36 of 1999 concerning Telecommunications

Law Number 5 of 1997 concerning Psychotropics

Regulation of The Head of Police In The State of The Republic of Indonesia Number 5 of 2010 concerning Tapping Procedures at the Republic of Indonesia National Police Monitoring Center

Regulation of The Minister of Communication and Informatics Number 1 of 2008 concerning Recording Information for National Defense and Security

Regulation of The Minister of Communication and Informatics Number 20 Year 2016 concerning Protection of Personal Data

Regulation of The Minister of Communication and InformaticsNumber 11 of 2006 concerning Technical Tapping of Information

Sitompul, Asri. *Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace.* Bandung: Citra Aditya Bakti, 2001.

The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data Amnesty International Policy on Encryption