World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:12, No:8, 2018

Strengthening Legal Protection of Personal Data through Technical Protection Regulation in Line with Human Rights

Tomy Prihananto, Damar Apri Sudarmadi

***Abstract*—**Indonesia recognizes the right to privacy as a human right. Indonesia provides legal protection against data management activities because the protection of personal data is a part of human rights. This paper aims to describe the arrangement of data management and data management in Indonesia. This paper is a descriptive research with qualitative approach and collecting data from literature study. Results of this paper are comprehensive arrangement of data that have been set up as a technical requirement of data protection by encryption methods. Arrangements on encryption and protection of personal data are mutually reinforcing arrangements in the protection of personal data. Indonesia has two important and immediately enacted laws that provide protection for the privacy of information that is part of human rights.

***Keywords*—**Indonesia, protection, personal data, privacy, human rights, encryption.

I. Introduction

THE development of information and communication technology has had an impact on human activities, which was originally done manually to be done electronically, resulting in various new terms of activities, such as electronic commerce (e-commerce), electronic-based education (e-education), electronic-based health (e-health), electronic-based governance (e-government), electronic-based budgeting (e-budgeting), and so on. Indirectly, these developments also have an impact on their data management activities. Of course, the available data turned into electronic data and the data management also becomes different ways because the nature of the data into electronic. In line with this, Indonesia has provided legal protection to data management activities. This can be seen in the enactment of several laws and regulations that protect or keep certain data, such as Disclosure of Public Information Act (Undang-Undang Keterbukaan Informasi Publik), Population Administration Act (Undang-Undang Administrasi Kependudukan), Health Act (Undang-Undang Kesehatan), Minister of Informatics and Communication Decree on Protection of Personal Data (Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi), Minister of Informatics and Communication Decree on Registration of Telecommunication Service Customer (Peraturan Menteri Komunikasi dan Informatika tentang Registrasi Pelanggan Jasa Telekomunikasi), etc. Thus, arrangements on personal data and data management are still scattered in various laws and regulations in accordance with the substance of each regulation, not yet integrated into one comprehensively [1]. In addition, the regulation is still limited to the provision of norms to safeguard/keep secrets from unauthorized parties, but has not provided clearer and more technical provisions concerning the protection mechanisms that should be provided/conducted by those who have an obligation to do so.

Tomy Prihananto is with Badan Siber dan Sandi Negara, Indonesia (corresponding author, e-mail: tomy.prihananto@bssn.go.id).

Damar Apri Sudarmadi is with Badan Siber dan Sandi Negara, Indonesia (e-mail: damar.apri@bssn.go.id).

II. Current Situation

Indonesia has arranged various matters concerning the management of data spread in various existing laws and regulations, such as Disclosure of Public Information Act, Population Administration Act, Health Act, Minister of Informatics and Communication Decree on Protection of Personal Data, Minister of Informatics and Communication Decree on Registration of Telecommunication Service Customer, and so on. This indicates that data management is an important thing to do in relation to each regulatory substance that governs it, in order to provide protection and create a sense of security for the owner of the actual data.

The provisions on data management in Disclosure of Public Information Act that public information has several categories, namely information that must be provided and announced periodically, information must be announced promptly, information must be available at any time, and information that is excluded. The regulation provides protection to certain information through access restrictions. Excluded information may include information that may impede law enforcement, information that may interfere with the protection of intellectual property rights and business competition, information that may harm the defense and security of the country, information that may reveal natural wealth, information which could harm the resilience of the national economy, information that may harm foreign relations, information which may reveal the contents of authentic deeds or wills, information that may reveal private secrets, and letters or memorandum between/intra public bodies [2]. The arrangement is made to various objects covering various aspects that are related with the interests of the state/ government, business interests, and personal interests. In other words, this arrangement is very broad and has covered all the information that exists in everyday life that needs protection. With its vast reach, the Disclosure of Public Information Act becomes the fundamental legal (generalis) that provides legal

protection for all laws on data protection in Indonesia.

The Population Administration Act regulates about population data that needs to be protected. Population data as stipulated in the regulation has an understanding is individual data and/or aggregate data that is structured as a result of the activities of Population Registration and Civil Registration.

"Demographic data are individual data and/or aggregate data that are structured as a result of the activities of Population Registration and Civil Registration" [3].

In other words, the data that is administered and protected by the rules is personal data. Similarly, in the Health Act which provides for the protection or recognition of the confidentiality of a person's informed consent provided for in Article 57. The exception that the secrets of personal health conditions may be sought based on a law order, court order, consent of the person concerned, and the person's interests [4]. Thus the Health Law also provides normative arrangements on the management and delivery of personal data protection.

In relation to the administration of electronic systems, the protection of personal data has also been regulated by the Minister of Informatics and Communication through Decree which regulates the registration of telecommunication service customers and the protection of personal data. Registration of telecommunication service customer arrangement stipulates that every telecommunication service customer is required to register using customer number, id number, and passport for foreigner [5]. This determines that the registration is performed using the personal data of the telecommunication services customer so that the subscriber can enjoy the services provided by the telecommunication operator. In addition, the regulation also regulates the storage of customer data, reporting, and supervision and control. Protections and obligations to conceal the personal data of telecommunication service customers are also provided for in the regulations which are conducted based on the certification provisions in the field of information security [5].

For the protection of personal data in electronic systems has been regulated by Minister of Informatics and Communication Number 20 in 2016 by providing protection during the process:

a. Registration and collection.
b. Processing and analyzing.
c. Storage.
d. Appearance, announcement, dispatch, dissemination and/or access opening.
e. Destruction. [6]

Article 4 that decrees states the existence of an obligation to use a certified electronic system in conducting the five protection processes.

Of the several laws and regulations mentioned above, it is known that the use of personal data of a person is given by that person as the owner of personal data to another party as a user of personal data in accordance with the interests of the owner of the personal data. Of course, the laws and regulations are in accordance with the substance of the services provided to the owner of personal data and more normative nature. It means it has the absence of more detailed technical provisions and regulations described in providing protection to personal data. Although it has been given legal protection as regulated by various laws and regulations, but with no provision on technical protection of personal data, this effected with various crimes related to personal data.

Until now there has been some fake e-KTP (electronic Kartu Tanda Penduduk is an identity card in Indonesia) as a representation of the data of a person's residence. This is seen from the case of ownership of e-KTP by foreign citizens in Indonesia so that with the ownership of e-KTP, the foreign citizen can be as if acting as an Indonesian citizen and doing activities like Indonesian citizens, which should be an illegal action by foreign citizens who do not have a permit [7]. In addition, there are also cases revealed by the Minister of Maritime Affairs and Fisheries that many fishermen of foreign nationals have e-KTP [8]. This has an adverse impact on Indonesia as Indonesia's natural wealth is explored by foreign nationals who act as Indonesian citizens without permit.

III. Discussion

The provisions concerning personal data are governed by international law in the Universal Declaration of Human Rights 1948, International Covenant on Civil and Political Rights 1966, European Convention for the Protection of Human Rights and Fundamental Freedoms 1950, the American Convention on Human Rights 1979, and the Cairo Declaration of Islamic Human Rights 1990 [1]. In such provision it is stated that compulsory shall provide protection against everyone from unlawful and arbitrary interference and intervention to personal, family, home, communications. Therefore, the regulation on privacy in human rights is also regulated in the Indonesian Constitution, namely Article 28 G of the 1945 Constitution "Every person shall have the rights to protection for personal protection, family, honor, dignity, and property under his control, and shall be entitled to a sense of security and protection from the threat of fear of doing or not doing something constituting human rights" and Article 29 of the Law on Human Rights "Everyone has the right to personal, family, honor, dignity and property rights". Therefore, this protection is then explained into privacy rights protection that is categorized into the privacy of information, body privacy, communications privacy, and territorial privacy [1].

In general, Indonesia has given the recognition of the right to privacy as a human rights. However, such arrangements have not been comprehensive. The concept of appropriate personal data protection arrangements is through a comprehensive arrangement [1]. Of course, a comprehensive arrangement is made of any information included in personal data/privacy that has been regulated by each sector regulations also need to be followed by a technical mechanism for data protection. Technical mechanisms of protection can be performed using encryption.

The process of concealing a message by hiding its substance is called encryption [9]. Cryptography is the art and science used to keep messages safe [9]. This mechanism is used in every activity, such as telecommunication or in every communication and information technology based on

electronic system devices, including using for electronic voting system. In order to minimize those problems (about transparency of vote counting), it is often advocated to apply a combination of various e-voting systems that allow for the electronic counting of votes with a paper receipt of the vote (e.g. Punchscan) as well as systems which employ advanced cryptographic techniques [10]. There are three uses of encryption: full-disk encryption or device is a process whereby all information stored on a computer or smartphone is encrypted while on the device; end-to-end encryption ensures that communications sent from the sender to the recipient cannot be decrypted or read by unauthorized parties or service providers; and transport encryption or transport layer encryption (often known including HTTPS using TLS or SSL) is a means of communication on the websites and browsers that are accessed encrypted [11].

There are Encryption Act in some states, such as Israel and United States of America. Encryption is regulated by the Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974, as amended (the Encryption Order) [12]. In United States of America, encryption regulation is regulated in The Security and Freedom Through Encryption (SAFE) Act. This Act regulate how to sell and use of encryption, and also exports of encryption devices [13].

In relation thereto, further mechanisms may be employed to provide strengthening to personal data protection regulations through building of regulations in the technical area of protection through the following considerations:

a. Crucial level of regulation in the field of encryption.
b. Selection of discussion priorities between The Draft of Encryption and The Draft of Personal Data Protection considering scope of regulation and legal void.

Referring to the domestic rules that already have various normative regulations in the field of personal data protection scattered in various laws and regulations, Indonesia also needs to build a regulation on the technical protection of personal data through The Draft of Encryption Act. This is in view of the fact that regulations governing the technical protection (encryption) can provide reinforcement and strengthening in providing real personal data protection. It is hoped that with the enactment of technical regulation of protection it can be prevented the occurrence of leakage or falsification of data in the future, so that with the existence of The Draft of Encryption Act hence the privacy become protected as this is a demand from Human Rights. Of course the regulations made are adjusted to the existing conditions in Indonesia today.

Currently regulation in the field of encryption and protection of personal data and information has been listed in the National Legislation Program 2015-2019 [14]. Both draft regulations were initiated by the government to be discussed with Parliament. The progress that occurred that the drafting of the Draft of Encryption Act and the Draft of Protection Data and Personal Information has been drawn up its bill and academic script [15] so that in the near future can be done discussion between Dewan Perwakilan Rakyat (DPR is a house of representative in Indonesia) and government.

Encryption as a method of data protection is closely related to privacy which is a basic human right. This is demonstrated by the compatibility of encryption used as data protection with specific elements of privacy, such as the rights against disclosure of concealed information, or right to limit access to the self, or control of information pertaining to oneself. The difference is in the scope, purpose, and objects governed by privacy and data protection.

Data protection explicitly protects everything under privacy protection, such as the need for fair treatment, consent, legitimacy, and non-discrimination [16]. The protection of the right to privacy also involves communications by a person or group, either verbally or through electronic communications. This is then set forth in the Draft of Encryption Act by setting the use of encryption by the public. The regulated provisions are

> "Everyone has the rights to use encryption for information security in the interest of protecting his/her privacy and/or personal data. Such information includes information that is his or her own and/or information that resides in him as obtained legally" [16].

Further consideration, a priority selection mechanism should be made in the discussion of the Draft of Encryption Act with the Draft of Personal Data Protection Act through consideration of the scope of arrangements and legal void. Certainly with regard to the current conditions that the Draft of Encryption Act and the Draft of Personal Data Protection Act has been included in the National Legislation Program 2015-2019 then the discussion of the two draft law can be done simultaneously considering the second purpose of the bill provides strengthening in providing personal data protection so that the human rights of privacy information can more secure. However, sometimes considering the density of legislation activities, there is a need for alternative discussion priorities.

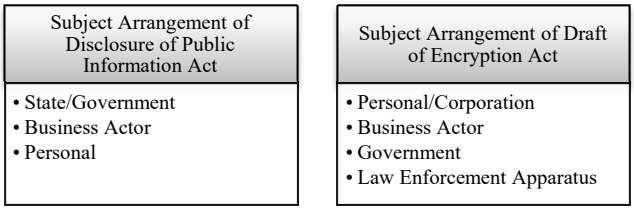

Fig. 1 Comparison between subject of Disclosure of Public Information Act and the Draft of Encryption Act

Subject of arrangement Disclosure of Public Information Act is state/government, business actors, and personal. It is considered to the purpose of Public Information Disclosure Act is related to that such subject interests. And the subject of arrangement of the Draft of Encryption Act is personals, business actors, government, and law enforcement apparatus [16]. Referring subject of arrangement, there is a similarity between subject of Public Information Disclosure Act and the Draft of Encryption Act, that is related with state/government, business actors, and personal

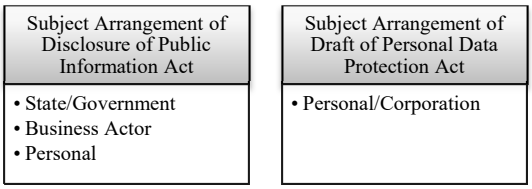

Fig. 2 Comparison between subject of Disclosure of Public Information Act and the Draft of Personal Data Protection Act

The subject of the Bill of Personal Data Protection is persons or corporations [1]. Referring to that, subjects set forth in the Public Information Disclosure Act with the Bill of Personal Data Protection have the distinction that the subject set does not cover from all subject arrangements made by Public Information Disclosure Act. Whereas when comparing subjects set forth in the Draft of Encryption Act with the Bill of Personal Data Protection, of course subjects regulated by the Draft of Encryption Act is more widespread because the subject set in the Draft of Encryption Act is same with Disclosure of Public Information Act.

The priority of discussion selection can be seen from the void of law. Arrangements on the protection of personal data have been set out in several enactment laws, namely the Health Act, the Population Administration Act, and so on. While the regulation on technical protection, using encryption has not been set at all at the level of legislation.

Considering the above matters, the discussion can be conducted simultaneously between the Draft of Encryption Act and the Bill of Personal Data Protection. However, priority of discussion can be done by determining the discussion of the Draft of Encryption Act first with the consideration that the extent of the Draft of Encryption Act wider and fill the legal void and provide more legal certainty in providing protection of personal data that has been regulated by some other laws.

IV. Conclusion

Setting up arrangement in encryption and protection of personal data is a mutually reinforcing arrangement in providing protection against personal data. Therefore, Indonesia considers the crucial two bills to be immediately enforced so as to provide protection against information privacy as specified in human rights.

In relation to this matter, discussion of the bill can be done simultaneously between the Draft of Encryption Act and the Bill of Personal Data Protection. Nevertheless, in the case of the need for alternative priority discussions, the Draft of Encryption Act can be discussed firstly considering the Draft of Encryption Act becomes crucial reminding it is doing technical protection of personal data, the wider range of arrangements because not only regulate the protection of personal data only, and can fill the void of law so as to provide more real legal certainty in providing personal data protection.

References

[1] Badan Pembinaan Hukum Nasional (BPHN), *Naskah Akademik Perlindungan Data Pribadi*, Jakarta: BPHN, p. 152, 29, 31, 153, 132.

[2] Indonesia, *Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.*

[3] Indonesia, *Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.*

[4] Indonesia, *Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan*.

[5] Indonesia, *Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2006 tentang Registrasi Pelanggan Jasa Telekomunikasi*, Article 3, 17.

[6] Indonesia, *Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*.

[7] Nelayan-Nelayan Filipina Pencuri Ikan Punya KTP Indonesia, http://regional.liputan6.com/read/2631201/nelayan-nelayan-filipina-pencuri-ikan-punya-ktp-indonesia, accessed on 23th March 2018.

[8] Susi Sebut KTP Palsu ABK Filipina Berasal dari Indonesia Timur, https://www.merdeka.com/uang/susi-sebut-ktp-palsu-abk-filipina-berasal-dari-indonesia-timur.html, accessed on 23th March 2018.

[9] Bruce Schneier, *Applied cryptography (2nd ed.): Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc.: 1995, p. 1, 2.

[10] Magdalena Musial-Karg, *The Use of Information and Communication Technologies in Electoral Procedures: Comments on Electronic Voting Security, World Academy of Science, Engineering and Technology*, International Journal of Law and Political Sciences Vol 11 No 9 2017.

[11] Amnesty International, *Encryption: A Matter of Human Rights*, https://www.amnestyusa.org/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf, p. 6-7, accessed on 26th March 2018.

[12] The Law Library of Congress, *Government Access to Encrypted Communications*, https://www.loc.gov/law/help/encrypted-communications/gov-access.pdf, p. 40, accessed on 26th March 2018.

[13] United States of America, *The Security and Freedom Through Encryption Act*.

[14] Program Legislasi Nasional 2015-2019, http://www.dpr.go.id/uu/prolegnas-long-list, accessed on 26th March 2018.

[15] Indonesia, *Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan*.

[16] Badan Pembinaan Hukum Nasional (BPHN), *Naskah Akademik Persandian*, Jakarta: BPHN, p. 31-32, 112, 107-108.