



Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia

Sinta Dewi Rosadi¹

¹Faculty of Law, University of Padjadjaran, Bandung, Indonesia
E-mail : sinta@unpad.ac.id

Submitted: 2018-03-05 | **Accepted:** 2018-03-28

Abstract: *Within the last five years it is noted that the people of Indonesia has become more aware of their privacy on personal data since their personal data is being collected, distributed and disseminated without their prior consent both by the government and businesses and their co-ventures . These businesses tend to commit violations by using and disseminating customers' data without the consent of their respective customers. This article focuses on Indonesian legal framework on the Privacy on personal data.*

It is argued that although there is existing laws in the privacy on personal data, however, those legal framework still developed in very sectoral nature. It is submitted that the most suitable regulatory concept for Indonesia is a combination regulatory concept, or hybrid concept., which protect Indonesian's and foreigner parties' interests privacy on personal data.

To investigate existing laws in personal data protection, this research examines both national as well as international and regional legal framework in personal data protection. Comparison between Indonesia and the practice of other ASEAN states is also conducted to determine the most suitable approaches in addressing the protection of personal data.

Keywords: *privacy, personal data protection, digital, legal framework, Indonesia*

I. INTRODUCTION

Indonesia's digital economy potential is huge and rapidly increasing and it is predicted that digital economy would contribute to the national economy nearly of 100 billion US dollars annually by 2025 and Indonesia is expected to become the largest digital economy power in ASEAN with the projected value of e-commerce transaction reaching 130 million US Dollars. One of the strong reasons for such a high value of digital transaction is due to the fact that Indonesian people is highly digital oriented i . Data from

the Indonesian Internet Service Providers Association (APJII) mention that Indonesian internet users are in the range of 52%, most of them access the internet on mobile for 4 hours per day. Furthermore, there are currently 370 million active SIM cards in Indonesia, much larger than the Indonesian population that has nearly reached 270 million . However, digital economy growth and utilization must be paired with privacy on personal data protection as one of the factors that will increase the trust in digital economy ecosystem. Privacy on personal

data protection involve the regulating and managing the processes of personal data that enabled the collecting, storing, sharing and analysing personal data as one form of privacy on personal data protection

According to G20, 2017 Ministerial Declaration trust and security are fundamental to the functioning of the digital economy, without them, acceptance of digital economy will be limited and one of the initiatives is to encourage the development of national privacy on personal data strategy cover areas such regulatory framework, corporate culture and corporate privacy on personal data management system.

Privacy on personal data issue in Indonesia has recently emerged and becoming an increasing concern due to the way the government and private companies collect and process privacy on personal data. The problems which emerged in Indonesia comprise among others: (1) the emergence of complaints raised by either individual or group or organization against violations of personal information regarding disruption of the privacy on personal data of individuals through both print and electronic media; (2) the emergence of complaints from the public because their identity and privacy on personal data are not properly kept, for example in banking industry, or more specifically in credit card industry, where customer's privacy on personal data can be accessed, disseminated and shared between bank and their agencies without the knowledge of the customer. Similarly with other privacy on personal data, causing a great concern in Indonesia relates to e-identity card program where the government compile privacy on personal data.

According to the Sophos Report, Indonesia currently is in the top 10 spammers

in the world with an estimated of 10,6 % junk mail originated from Indonesia, while according to the data released by the Association of Indonesian Internet Provider, the number of complaints relating to the advertisements entering into e-mail without user's permission has reached 8389. It indicates that privacy on personal data violations in Indonesia are increasing. These problems occur due to the absence of rules that specifically protect the privacy on personal data of personal information either for regular or print media as well as electronic media. Indonesian data protection rules are not compiled in a single law, instead, the Government has enacted sectoral laws regarding privacy on personal data with minimum legal protection. Compared to other ASEAN Countries, Indonesia is not equipped with specific legislation on the Privacy on personal data yet. Therefore the Indonesian government should immediately set up privacy on personal data protection regulation and determine which concept of regulation are the most appropriate to protect Indonesian's and foreigner parties' interests privacy on personal data.

II. LEGAL MATERIALS AND METHODS

In examining legal framework in the protection of personal data, this research use juridical normative method, which examine the consistency between Indonesian constitution and the law on the protection of personal data. Comparison with other ASEAN states is also conducted to determine which approach is suitable for Indonesia. Various legal materials ranging from primary, secondary as well as tertiary legal materials are used.

Such legal materials include the following legal instruments as well as other journal articles relevant to the topic:

- Universal Declaration of Human Rights
- 1945 Indonesian Constitution
- Indonesian Act No. 36 of 1999 on Telecommunications
- Indonesian Act No.39 of 1999 concerning Human Rights
- Indonesian Act No. 29 of 2004 on Medical Practice
- Indonesian Act No. 17 of 2007 on National Development Planning Policy
- Indonesian Act No. 11 of 2008 on Information and Electronic Transaction.

III. RESULTS AND DISCUSSIONS

Establishing the Concept of Privacy on personal data: Indonesian Legal Framework

Indonesia is often ignored in discussion of privacy on personal data¹ and in the Indonesian legal system, there is no specific regulation concerning privacy on personal. The initiative to provide protection upon privacy on personal data is derived from the Human Rights Rules under the Constitution² This is also driven by the influence of information technology development where most Indonesian people have access and learn that their privacy on personal data will be in jeopardy, and also because there are so many advertising practices that collect privacy on personal data without clear regulations. Furthermore, the significant driving factor is the strong international and regional obligation either politically, economically as well as legal cooperation, since Indonesia has a strategic position in international trade, including electronic

trade. Therefore, the legal basis to establish a law on privacy on personal data privacy on personal data in Indonesia can be drawn from several sources:

Privacy on personal data and Data Protection according to the Constitution of 1945.

Similar to several other countries, Indonesia perceives privacy on personal data as a part of human rights. The Indonesian Constitution of 1945, which is the primary source of Indonesian laws, does not explicitly mention privacy on personal data, but recommends protecting human rights. The Preamble of said Constitution states that human rights are the ideal as well as Indonesia's national goal. The national goal is to protect the citizens of Indonesia and the whole country, as well as to promote the general welfare and the intellectual life of the nation and the establishment of world order based on freedom, social justice, and world peace. Furthermore, the concept of privacy on personal data and data protection can be found in the Amendment to the Constitution of 1945, articles 28F and 28G³. Even these articles do not directly mention the privacy on personal data, but can be considered as a legal basis for regulation on the matter. Although the articles have not been applied directly in the regulation in Indonesia, but there is no doubt that the articles are concerned with human dignity as a human right.

¹ Graham Greenleaf, *Asian Data Privacy on personal data Law, Trade and Human Rights Perspectives*, (Oxford University Press, 2014), 374.

² Sinta Dewi Rosadi, above n.5, 8.

³ Indonesian legal scholars often refer to Article 28G of the 1945 Constitution as the rather vague basis for more specific privacy on personal data

legislation. Article 28G of the 1945 Constitution: *Each person shall have the right to protection of their personal selves, families, respect, dignity and possessions under their control and shall have the right to security and protection from threat of fear for doing or for not doing something which constitutes a human right.*

Privacy on personal data according to the Provisions on Human Rights

Human Rights Law in Indonesia

Indonesia adopted UDHR through its National Act No.39 of 1999 concerning Human Rights (UU 39/1999) which also reiterates the right to privacy on personal data. Article 31 and 32 of this Act state that no one shall be subjected to arbitrary interference with his home and with his correspondence.⁴ Enacting this Act is an evidence that Indonesia has a moral and legal responsibility to respect, execute, and uphold the Universal Declaration on Human Rights promulgated by the United Nations, and several other international instruments concerning human rights ratified by the Republic of Indonesia. In the case of violations of Article 31 and 32 of UU.39/1999, Indonesia provides a mediation settlement conducted by National Commission of Human Rights⁵. Concerning issues of data, Human rights law provides Article 12, which states:

"Every person is entitled to protection of personal development, to get education, to educate himself, and improving the quality of human life in order to be faithful, devoted, responsible, noble, happy, and prosperous in accordance with human rights."

⁴ Article 30 of Act 39 of 1999 says :

- (1) No one shall be subject to arbitrary interference with his home.
- (2) No one shall set foot in or enter the enclosure of a house or enter a house without the permission of the person who lives there, except for reasons provided for under prevailing legislation.

Article 31 of Act 39 of 1999 : says : No one shall be subject to arbitrary interference with his correspondence, including electronic

Based on the above mentioned articles, it is evident that Indonesia seeks to protect human rights even though privacy on personal data not stated specifically but the article 21 regarding the right to personal integrity has perceived as to protect privacy⁶

Article 21 of the Human Rights Act states:

"Every person has the right to personal integrity, both spiritual and physical. And therefore there can be no object of research without consent from him. "

Article 29 states: *"(1) every person has the right to protection of self-personal, family, honour, dignity, and his property. (2) Every person has the right to recognition as a person before the law wherever he is."*

Privacy on personal data according to Law on Telecommunications

Basically, this Law describes the government's protection of civil rights on telecommunications issues. However, protection related to privacy on personal data and human rights can also be found in articles 38-42 of Law No. 36 of 1999 on Telecommunications. In this Law, privacy on personal data specifically stipulated in Article 38:

"Every person is prohibited from doing acts that may cause physical and electromagnetic interference on telecommunications services"

communications, except upon the order of a court or other legitimate authority according to prevailing legislation

⁵ The role of National Commission of Human Rights as mediator on human rights issue can be seen in Article 76, Article 90 to 99 of UU 39/1999.

⁶ Sinta Dewi, 'Balancing Privacy Rights and Legal Enforcement : Indonesian Practice's, (2012) 5 *International Journal of Liability and Scientific Enquiry*, 232.

Article 40:

"Every person is prohibited from conducting wiretaps on information transmitted over telecommunications network in any form."

Article 42:

(1) The telecommunications service provider is obliged to keep confidential the information that is sent and or received by its telecommunications services customers through telecommunications networks and or telecommunications services provided.

(2) For the purposes of the criminal justice process, the telecommunications service provider may record information sent and or received and may provide the necessary information upon:

a. written request from the Attorney General or the Chief of Police of the Republic of Indonesia for certain criminal acts;

b. investigator's request for certain criminal acts in accordance with applicable laws.

(3) The provisions on the procedures regarding requests for, and granting of the recorded information referred to in paragraph (2), shall be regulated by a Government Regulation.

Privacy on personal data in the Law of Health

Privacy on personal data also stipulated in Law No. 36 of 2009 on Health, which stated in Article 57 that:

"Everyone is entitled to its personal health conditions confidentiality that

has been presented to health care providers."

Article 47 (2) of Law No. 29 of 2004 on Medical Practice also states that:

"Medical records referred to in paragraph (1) shall be stored and kept confidential by the physician or dentist and the management of health-care facilities."

Within the Indonesian legal system, the protection provided by the government to the citizens is aimed to protect the privacy on personal data of their medical history from any disclosure made by health care providers. Individual's medical history is a part of human dignity and cannot be disclosed without the patient's consent. In other words, health care providers are prohibited from disclosing any information about the patient to other third party.

Privacy on personal data in Electronic Transactions Law

The growth of the internet and advances in technology has led to the passage of Electronic Information and Transactions Law No. 11 of 2008 (the "ITE Law"). The ITE Law prohibits the use of information acquired through electronic media containing privacy on personal data related to an individual without the consent of such person. The ITE Law further provides that anyone deliberately and without having valid rights shall be prohibited from changing, adding, reducing, transmitting, destroying, eliminating, transferring or hiding electronic information and/or electronic documents owned by any other person or owned by the public.

Concept of Regulation for Indonesia

In regulating privacy on personal data, the countries have their own regulatory concept. From practical point of view, it is found that there are very large differences in concept regulations especially between United States and the European Union. Although these two regions have, historically common perception in terms of political economy and culture, but with regard to the privacy on personal data settings there are fundamental differences in terms of the government role in regulating information. The roots of the differences between two jurisdictions is due to the differing legal approaches.⁷

In the USA, although the legal culture is quite familiar with privacy on personal data, its regulatory concept is based on sectoral regulations, by which the government only regulates the areas that are considered necessary to be protected by law. Other areas are entrusted to the industry (self-regulation).

On the other hand, the European Union (EU) regulates privacy on personal data more comprehensively in a single legislation covering all sectors namely public and private sectors. The basic of privacy on personal data arrangements in the EU, has clearly put privacy on personal data as a fundamental right protected by the human rights regime; hence, provide more clear direction.

In addition, in regulating privacy on personal data the EU tries to balance the two interests, namely the protection of privacy on personal data as a fundamental right which is governed by the regime of human rights both domestically and internationally, and to ensure the smoothness of traffic information

and trade among member countries. This comprehensive approach in privacy on personal data basic arrangement is to create harmony in regulating privacy on personal data, due to the fact that each EU member has its own laws but applying different standard arrangements that cause difficulties in transferring information among member countries and ultimately leads to hamper trade. However the EU approach has continually over the sixty-five years influenced national legislation on every continent⁸

Until now there are some similarities in the regulations regarding the privacy on personal data at the multilateral, regional and national level of certain countries. From this point of view it can be observed that:

1. There is a strong inclination regarding the efforts to standardize regulation on the privacy on personal data;
2. There are similarities meanings of the key terms used, such as: data; privacy on personal data; sensitive personal data; personal information; data processor; data processing; data controller; commissioner, etc.;
3. There are similarities in general principles regarding the privacy on personal data issues;
4. Regulations concerning privacy on personal data are not limited only to apply to public sector, but also applied to private sector, either through "legislative approach", "self-regulatory", and "co-regulatory";
5. To facilitate the international trade, the adequate protection relating to privacy on personal data particularly

⁷ Paul M. Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law', (2017) 106 *Georgetown Law Journal*, 2.

⁸ Marc Rotenberg, Julia Horwitz, Jeramie Scott (ed), *Privacy on personal data in the Modern Age*, (The New Press, 2015), 72.

the "trans-border flow of data", is a prerequisite that must be considered.

Considering the above mentioned, in addressing the direction and ongoing international trend, Indonesia should take the following steps:

1. The existence of a Law on Privacy on personal data is a necessity that cannot be postponed any longer, because it is very urgent for a variety of national interest and as to facilitate international relations of Indonesia, especially in expediting trade, industry, transnational investment;
2. There have been many complaints which led to demands for damages particularly upon marketing activities in accessing, compiling, distributing and trading - in customers' privacy on personal data;
3. Implementation of E-Government Program especially Electronic Identity Program (E-KTP) in which the government collects privacy on personal data of the people without adequate protection that leads to a high potential of violations.
4. The existence of this Law will also be able to foster Good Governance and to achieve the Clean Government.

It is recognized that each regulatory concept has certainly its own advantages and disadvantages. In term of comprehensive regulatory concept, its advantages are among others:

1. Legal certainty, because privacy on personal data is decisively regarded as a basic right that should be protected by the state;

2. Strictly regulate the government and private sector activities;
3. It is suitable for countries having a Civil Law legal system that puts the legislation as one of the main sources of law;
4. This regulatory concept is suitable for countries that do not have yet privacy on personal data protection Act because it contains the principles and key mechanisms that must be done to protect the privacy on personal data of information.

By observing the international and regional developments which have shaped the globalization of information that has put Indonesia as part of a world information society⁹, this requires the establishment of regulations that will protect the privacy on personal data of electronic information. Moreover, the need for government to support the development of information technology through regulations is to make the use of information technology safely, as well as reduce the potential losses that have been incurred in Indonesia, as a result of invasion of privacy on personal data. In addition, the urgency of privacy on personal data regulation on personal information in Indonesia has been mandated in the Long Term Development Plan 2005-2025, in anticipation of the implications of the convergence of telecommunications, information technology, and broadcasting¹⁰.

Therefore, Indonesia must establish a good and well-coordinated system of information technology law as to achieve a certainty and the legal order. Legal order is the ultimate goal of a good legal system by: (1) recognizing and balancing between

⁹ Laws No. 11 of 2008 on Information and Electronic Transaction.

¹⁰ Law No. 17 of 2007 on National Development Planning Policy

private rights and public rights, (2) determining the restriction of such rights, and (3) regulating such rights¹¹. .

This opinion is in line with the opinion of Lawrence M. Friedman, whereas building the legal system must fulfil three elements namely structure, substance and legal culture¹². Structure means, the extent to which the Indonesian court can resolve the case of privacy on personal data invasion. This is not an easy task since it involves human resource capability, i.e. the ability of judges to understand the development of technology and be responsive towards new developments. Yet, the responsive law requires participation of all parties concerned, including judges¹³ who can implement legislation into cases for which the injured party may claim for damages.

Taking into account the above mentioned development, Indonesia should develop a specific legislation on privacy on personal data. In formulating a good concept of regulation, the initial process starts with the good goal setting. As stated by Mochtar Kusumaatmadja, law is not only the rules and principles that govern human life in society, but also covers institutions and processes to realize that law in the reality¹⁴. Meanwhile, Roscoe Pond in the Theory of Interest argues that the law should meet the interests as a demand to reach by humans both as individuals and as a group or association and

the law should regulate as to how these interests can be achieved¹⁵.

By means of the Law

A good concept of regulation should cover: principles, rules, processes, and institutions. If it is associated with the concept of privacy on personal data regulation, then such regulation should include:

- 1) The principle to be the basis in establishing a regulation should consider both national and international developments. The principles of information privacy on personal data regulation should be based on the 1945 Constitution wherein Article 28 (G) has clearly recognized that the right to privacy on personal data must be protected¹⁶. In addition, the basic privacy on personal data protection has been stipulated in Law No. 11 of 2005 on the Ratification of the ICCPR, which clearly recognizes privacy on personal data as one of the fundamental rights, and declares that the state must protect privacy on personal data. As for electronic transactions, privacy on personal data has been regulated in Law No.11 of 2008 on Information and Electronic Transactions. Thus, from the legal point of view, privacy on personal data protection in Indonesia has had a legal source.

¹¹ Roscoe Pond, *My Philosophy of Law*, (Julius Rosenthal Foundation Northwestern University, 1941), 249.

¹² Lawrence M. Friedman, *American Law: An Introduction*, (Norton, W. W. & Company, Inc, 1997), 19

¹³ Philippe Nonet and Philip Selzenick, *Law & Society in Transition*, (Transaction Publishers, 2001), 97

¹⁴ Mochtar Kusumaatmadja, *Legal Concept in the Development (Konsep-Konsep Hukum dalam Pembangunan)*, (Alumni, 2006), 12

¹⁵ Roscoe Pond Theory of Interest : *Interest is a demand or desire or expectation which human beings, either individually or in groups or association or relations, seek to satisfy*. See Roscoe Pond above n. 17, 16

¹⁶ *Each person shall have the right to protection of their personal selves, families, respect, dignity and possessions under their control and shall have the right to security and protection from threat of fear for doing or for not doing something which constitutes a human right*.

2) In addition to the basic principles, the concept of regulation must also consider the so called principles of fair use of information (fair information principles) which calls for standards of practices required to ensure that entities that collect and use personal data provide adequate protection¹⁷. These standards that have been internationally recognized and as such adopted by many countries such as: the principles of the OECD Guidelines in 1980, the EU General Directive 1995, and the APEC Framework 2004, these include the following principles:

- a) Principle of limitation in the collection of information. The information obtained, processed and disseminated should be limited only to lawful and fair purposes and should be upon the knowledge and consent of the information owner.
 - b) Principle concerning the quality of information. Personal information must be obtained in accordance with the intent and purpose of its collection. Quality of information must be maintained in terms of its accuracy, completeness and updates.
 - c) Principle of the objective. Personal information may only be opened in accordance with its intended use.
 - d) Principle of retention. The retention of information for a particular purpose should not be longer than the necessary period of time.
 - e) Principle of maximum security on personal information. Personal information shall be protected by adequate security system in order to avoid the risk of losing or unlawful act such as access, destruction, use, modification or disclosure of such information by other parties.
 - f) Principle of transparency. The management of information must take necessary steps so that the information owners can learn about the kinds of personal information held by the data manager.
 - g) Principle of individual participation of information subject. Information's owners shall have the right to access their personal information maintained by the data manager, including the right to make corrections to their personal information.
 - h) The principle of accountability. Information manager is fully responsible to implement the above mentioned principles.
- 3) Furthermore, there must be clear definitions of the substantial terms to be mentioned in the regulation, such as:
- a) Use of the term "data" or "information". As discussed already in the previous chapter, countries use different terms. The European Union uses the term "data", the U.S. uses the term "information", meanwhile Indonesia in article 26 of the ITE Act

¹⁷ James Waldo, Herbert S. Lin, Lynette I. Millet (ed) *Engaging Privacy and Information Technology In*

A Digital Age, (the National Academy of Science Press 2007), 48.

used the term “privacy on personal data”¹⁸.

- b) In the discussion concerning privacy on personal data, the use of the term privacy on personal data and information are often used interchangeably. Actually, these two terminologies are not the same since information refers to data that has been processed so it can be understood by a wider audience, while data refers to the starting data or raw data materials as a source of information¹⁹. Practically, countries do not distinguish the meaning of privacy on personal data and personal information; hence, both terms are used interchangeably and have been accepted as one of the types of privacy on personal data rights that must be protected²⁰.

With regard to e-commerce, “information” is more precise term than “data”, because in the cyber world privacy on personal data can be accessed, manipulated and disseminated so that it may become new information for others.

- c) Scope of regulation must be clear. The object to be protected should be clearly defined, whether the information that may be accessed manually or electronically, since in Indonesia there is no specific law governing the protection of personal information done through manual transaction. As for privacy on personal data in electronic

transactions, it is arranged already in the ITE Law, although the arrangement is still too common. Therefore it is very important that the scope of arrangement covers both manual information as well as electronic information. It is also of the utmost importance to manage due to violations of financial information especially credit card information in Indonesia which has prompted dissemination practices of financial information on the Indonesian credit card holder without the knowledge of the information owner.

- d) In addition, the subject to be regulated by the law must be determined. The question is whether the subject is all parties involved as in the EU, namely the government, individuals, and private, or sorted out as applied in the US. Since Indonesia does not have yet a specific regulation on the privacy on personal data of personal information, then a regulation that covers the whole, namely the government, private sector and individuals will be more preferable. The regulation can be in general, and if there are other business sectors that need to be specifically regulated, then it can be dealt separately.
- e) Legislation should also regulates exceptions in order for personal information to be disclosed for special cases, such as request for disclosures for the purpose of

¹⁸ Unless otherwise provided by the legislation, the use of any information through the electronic media regarding privacy on personal data should be made with the approval of the concerned person.

¹⁹ Abu Bakar Munir , Siti Hajar Mohd Yasin, Md. Ershadul Karim, *Data Protection Law in Asia*. (Thomson Reuters Hongkong Limited, 2014), 6-8

²⁰ Practice in the United States, European Union, Hong Kong and Singapore.

national security, national defence, public interest and judicial process.

4) Board of Supervisory

In achieving a good concept of regulation, involvement of both institution and process is a must²¹. Karl Llewellyn, one of the leading legal realism of the United States argues that the law as an institution plays a very important role in the formation process of law. In the law-making process, the institution has an obligation to be able to carry out its duties properly and must always be accountable for all of his duties to the public²². In relation to the concept of information privacy on personal data regulation in Indonesia, the institution's function is vital in carrying out the law so as to effectively oversee and resolve legal issues. The respective institution is divided into two types, namely:

Public institutions consist of:

1. The court as an adjudication institution is authorized to settle claims of the people's for privacy on personal data violations;
2. Information Commission has the duties to:
 - a) disseminate the law to the public including the industrial sectors as to make them understand their rights and obligations with respect to the privacy on personal data of information;
 - b) advise the Minister on matters related to the implementation of the law;
 - c) conduct research on, and monitoring the development of the information process and

technological advances to derive a knowledge of the adverse impacts of these developments on privacy on personal data of information;

- d) encourage associations and institutions to prepare and disseminate to its members the rules of practice (code of practice) as guidance for fulfilling the law's requirements;
- e) As mediator to resolve information privacy on personal data disputes outside the court.

Private institutions are institutions set up by the private sector to participate in regulating information privacy on personal data. These institutions take the form of business associations and other private institutions that formulate the rules of practice (code of practice) in accordance with the mandate of the law.

As for the process, is how the legislation can be implemented and adhered to by all related parties that will lead to a legal certainty. Good process can be carried out through two approaches

1. First, through a top-down approach, where this approach is one of the effective ways to take, especially when the new regulation implemented in a country. Part of Indonesian people know already the term privacy on personal data particularly among artists and educated people, however, most people is not informed of it therefore socialization by the government to the public is imperative

In a top down-down approach, government and related industrial

²¹ Mochtar Kusumaatmadja, above n. 12, vi.

²² Freeman, M.D.A (Ed), *Lloyd's Introduction to Jurisprudence*, (Sweet & Maxwell, 1994), 661

sectors must come together in socializing legislations, policies and rules of thumb (code of practices) and implementing legislation by imposing forceful sanctions to violators. In this case, the industrial sector should also be encouraged to apply the rules of thumb consistently, i.e. to obey and implement the law and will take action by imposing sanctions against any violation committed by any of its members. Through the co-regulatory concept, there will be a good cooperation between the government and private sectors.

2. Second, through the bottom up approach, namely encouraging the public to learn and understand the law through education and publication. Education can be done through counselling to the public by way of discussions, seminars and provides feedback mechanism from the community through non-profit organizations or educational institutions. In addition, publication organized by the academicians with regard to the information privacy on personal data law would greatly help the public's understanding²³.

In most countries that have regulated the privacy on personal data (except the United States, Japan and Singapore), an independent institution has been formed whose task is to oversee the implementation of the law²⁴. The establishment of an

independent institution is in order to ensure the effective implementation²⁵ of the law

In order to perform their duties effectively, this institution must be able to position itself as an independent agency even though this particular agency is appointed and financed by the government. The agency has the authority to oversee the implementation of the law; issuing guidance on the privacy on personal data principles that must be adhered by each sector; investigating individual complaints and oversee the preparation and implementation of the rules of conduct (code of conduct) made by industry sector. Furthermore, this supervisory agency also acts as a mediator for resolving disputes out of court. In the event such dispute cannot be resolved by the agency's mechanism, then it can be submitted to and filed in the court.

International and Regional Obligations

As Indonesia has ratified and signed various international instruments, hence, Indonesia has a legal basis to make laws that apply at the national level. As an APEC member, Indonesia has adhered to the so-called APEC Privacy on personal data Framework 2004, in which its preface clearly mentions that "Potential of electronic commerce cannot be realized without the cooperation of governments and businesses as to develop and implement technology and policies that address issues including privacy on personal data"²⁶ The APEC membership is expected to stimulate the national

²³ Warren B. Chik. 'The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on personal data on the Internet', (2005), 14 1, *International Journal of Law and Information Technology*, 22-23.

²⁴ In the Directive on the Protection of Information (95/46) the authority of supervisory agency provided for in Article 28. The Agency has a very broad authority, i.e conducting surveillance,

investigation and intervention in the management of personal information.

²⁵ *Handbook on European Data Protection Law* (Publications Office of the European Union, 2014), 114.

²⁶ Sinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, (Widya Padjadjaran, 2009), 70

legislation to create a balance between protecting and promoting economic cooperation, particularly in the electronic trading among members. The European Union is a very attractive market for Indonesia as the largest market for the non-oil and gas exports, and so far European investors also have proved to be the most stable and reliable partner for Indonesia. So, it is important for Indonesia to overcome all the challenges and constraints that must be faced when doing business across the country. In other words, it is important for Indonesia to meet the EU standards regarding privacy on personal data. Not only for economic reasons, the privacy on personal data policy should also be introduced as part of the law concerning human rights. Privacy on personal data is a part of human rights and the protection of privacy on personal data is one way to honour this right. In Indonesia, concerns about the protection of privacy on personal data is growing since there is no clear legislation yet. Therefore, the issues of privacy on personal data have become an urgent agenda.

Many countries establish laws that deal with this matter, but there is no law in Indonesia regulating this matter. Improvement and development of science and technology, globalization, and the power of the media have created the need for privacy on personal data. As an Asian countries, Indonesia has found it is quite difficult to define and regulate privacy on personal data. Most countries in Asia are not familiar with privacy on personal data.

Privacy on personal data issues have not been considered as "serious" in Asia, including Indonesia. Most Asian people traditionally live in communal societies, which do not pay attention to privacy on personal data. Privacy on personal data terms as a human right derived from the West has become more and more important in the era of information and communication technology (ICT).

The 21st Summit of the Association of South East Asian Nations (ASEAN) was held in Phnom Penh in November 2012. One of the outcomes/resolutions is the adoption of the ASEAN Human Rights Declaration by the ten member states. This declaration raised many criticisms from senior United Nations officials, human rights experts and hundreds of civil society and grassroots organisations at the national, regional and international levels; nonetheless it was still adopted by ASEAN leaders as an ASEAN human rights law and standard.²⁷ For a long period of time the Asia Pacific region has been disparaged as the only geographic block not to have a regional human rights instrument. Africa has the African (Banjul) Charter on Human and Peoples' Rights, the Americas have the American Convention on Human Rights and Europe has the European Convention on Human Rights. Conventions bind upon States once they ratify it, that is, it is a legally binding treaty. A declaration, on the other hand, is not legally binding, but does carry moral weight. For example, the UDHR is not a binding treaty but over time has come to have enormous force and influence in international human rights law. Furthermore,

²⁷ Asean Declaration of Human Rights was deemed to have undermined, rather than affirmed, international human rights law and standards. The drafting process as well as the substance of the Declaration are considered as fatally flawed. See: <http://www.icj.org/icj-condemns-fatally-flawed-asean-human-rights-declaration/>, [http://theconversation.edu.u/asean-human-rights-](http://theconversation.edu.u/asean-human-rights-declaration-a-step-forward-or-a-slide-backwards-10895)

[declaration-a-step-forward-or-a-slide-backwards-10895](http://theconversation.edu.u/asean-human-rights-declaration-a-step-forward-or-a-slide-backwards-10895), <http://uncut.indexoncensorship.org/2012/11/asean-human-rights-declaration/>, <http://www.hrw.org/news/2012/11/19/civil-society-denounces-adoption-flawed-asean-human-rights-declaration>.

a declaration is also often the precursor to a binding treaty. For instance, UDHR led to the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, which are collectively known as the international bill of rights. So the new ASEAN Human Rights Declaration should perhaps be viewed as a first step on the path towards greater protection of human rights in the region, rather than an end in itself.

IV. CONCLUSIONS AND SUGGESTIONS

The most suitable regulatory concept for Indonesia is a combination regulatory concept, or hybrid concept. This regulatory concept combines several approaches in regulating privacy on personal data particularly in e-commerce the reason behind selecting this concept is due to the rapid growth of information technology, so that the personal information may easily be accessed, processed, compiled and distributed to others. Hence, the regulatory concept must combine several approaches: First, through the legislation that applies the principles and international standards that will encourage

the harmonization of the laws and to reduce the potential for conflicts between states. Second, through the market approach (market-based solution), online industries via their associations are encouraged take active part in protecting customers' privacy on personal data, through privacy on personal data policy in the form of a statement that the industry will protect consumer privacy on personal data by implementing fair information principles. Third, through technology approach, on the reasons that the invasion of privacy on personal data in e-commerce is due to the advancement of information technology, so one way of protection measures is to take advantage of technology, among others with PETS (Privacy on personal data Enhancing Technology). Fourth, through corporate privacy on personal data rules approach in the form of code of conduct that applies to multinational companies especially those who are doing online business. These practical rules should bind the multinational companies and all of their affiliates.

REFERENCES

Journal Articles

- Schwartz, M, Paul and Nikolaus, Karl, Peifer, 'Transatlantic Data Privacy Law', (2017) 106 *Georgetown Law Journal*.
Sinta Dewi, 'Balancing Privacy Rights and Legal Enforcement: Indonesian Practices', (2012) 5 *International Journal of Liability and Scientific Enquiry*.
Sinta Dewi, 'Concept Regulation for Privacy on personal data in The Applications of Biometric Smart Card', (2017) 4 2, *Brawidjaya Law Journal*.

- Warren B. Chik, 'The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on personal data on the Internet' (2005) 14 1, *International Journal of Law and Information Technology*

Books

- Abu Bakar Munir, Siti Hajar Mohd Yasin, Md. Ershadul Karim, *Data Protection Law in Asia*. (Thomson Reuters , 2014)

- Friedman, M, Lawrence, *American Law: An Introduction*, (Norton, W. W. & Company, Inc, New York, 1997).
- Greenleaf, Graham , *Asian Data Privacy on personal data Law, Trade and Human Rights Perspectives*, (Oxford University Press, 2014)
- Rotenberg, Marc Rotenberg , Horwitz, Julia , Scott, Jeramie Scott (ed), *Privacy on personal data in the Modern Age*, (The New Press, 2015)
- M.D.A, Freeman, (Ed). *Lloyd's Introduction to Jurisprudence*, (Sweet & Maxwell, 1994)
- Mochtar Kusumaatmadja, *Legal Concept in the Development (Konsep-Konsep Hukum dalam Pembanguna)*, (Alumni, 2006)
- Nonet, Philippe and Selzenick, Philippe, *Law & Society in Transition*, (Transaction Publishers, 2001)
- Pond, Roscoe, *Jurisprudence Vol IV*, (West Publisihing, 1959).
- Sinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, (Widya Padjadjaran, 2009)
- Sinta Dewi Rosadi, *Privacy on personal data from International Law, Regional and National Perspectives* , (Refika Aditama, 2015).
- Waldo, James, Lin, S, Herbert, Millet, I, Lynette I. (ed) *Engaging Privacy and Information Technology In A Digital Age*, (The National Academy of Science Press, 2007)

Legislations

- Universal Declaration of Human Rights
- 1945 Indonesian Constitution
- Indonesian Act No. 36 of 1999 on Telecommunications

- Indonesian Act No.39 of 1999 concerning Human Rights
- Indonesian Act No. 29 of 2004 on Medical Practice
- Indonesian Act No. 17 of 2007 on National Development Planing Policy
- Indonesian Act No. 11 of 2008 on Information and Electronic Transaction.

Handbook, Report, Paper

- Handbook on European Data Protection Law (2014), Publications Office of the European Union, Brussel.

Internet

- Unleashing Indonesia Digital Economy Potential,
<http://www.thejakartapost.com/academia/2017/08/07/> (aceses 17 Januari, 2017)
- Roadmap for Digitalisation: Policies for Digital Future
<http://www.g20.utoronto.ca/2017/170407-digitalization-annex1.html>,
 (aceses 12 December, 2017)