MODEL REGULATION FOR DATA PRIVACY IN THE APPLICATION OF BIOMETRIC SMART CARD

Sinta Dewi[1]

[1] **Department of ICT Law, Law Faculty, Padjajaran University**
Email : sinta@unpad.ac.id

Submitted : 24-02-2017 | **Accepted**: 08-03-2017

ABSTRACT

Notwithstanding the foregoing, the use of this technology has raised many concerns with regard to the need of privacy data protection. It is due to the fact that biometrics technology as a powerful identifier brings along personal information that can be traced from different sources to be linked together, and also the ability of third parties to access this data in identifiable form and link to other informations and used this information for secondary uses without the consent of data subject.

Data privacy is considered as fundamental human rights and has been regulated in a number of international instruments as well as regional instruments and has been incorporated into more than 100 national laws. Countries have now recognized data privacy either as explicit constitutional rights, or in the form of comprehensive data privacy law.

This article discusses the extent to which the use of biometric smart card as a tool to examine the identification has been increasingly utilized due to its advantages, such as ability to achieve a high level of accuracy, the system cannot be easily duplicated as well as high level of security, since it involves biological characteristics like fingerprints, iris and DNA. It further explores data privacy model regulation which is intended to regulate and protect data privacy.

This article concludes that data privacy is a legal right regulated and controlled by both international and national instruments, and the use of biometric smart card often viewed as a conlict between the need of security and how far the system protects data privacy. The model of regulation approach, known as hybrid model, is aimed to ensure privacy data protection. Such hybrid model of regulations should combine 4 (four) approaches namely; government regulations, social norms, corporate privacy rules and technical regulations.

Keywords: *data privacy regulation**,** model, biometrics, privacy policy*

I. INTRODUCTION

As innovations in information technology have enabled previously unimagined forms of collecting, storing, sharing and analyzing data, data privacy has evolved to encapsulate a right to protection of personal data[1]. The concept of data privacy derived from the establishment of rules governing collection and handling of personal data, and implies that individuals have the right to decide whether to engage with society by sharing or exchanging their personal information,

[1] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honor and reputation (art. 17).

DOI: *http://dx.doi.org/10.21776/ub.blj.2017.004.01.06*

and to determine on what terms they are prepared to do so. Data privacy laws generally incorporate safeguards protecting the security of personal data and allowing for its use by others only in prescribed circumstances. In recent years , many services industries utilize smart card in providing better services for public by both government and business. Therefore all transactions will be managed quickly with high accuracy, better security and the data can be easily stored, for example for financial services, government services, educations. This technology offers a lot of significant benefits for providers and users of services, while offering a challenge for anyone who wants to develop this innovation further. High mobility is obtained from small physical size with small dimensions of chip. Security of data is supported by the microprocessor in a chip that can perform encryption process stored data[2]. However the using of modern technology such as biometric smart card have posed new threat to the way information particularly personal data will be collected, processes and disseminate and this technology enable new form of monitoring and recording personal data that eventually will be in conflict with data privacy[3].

Data privacy protection become a globally paradigm since it has been universally accepted as one of fundamental tenet for democratic society[4] and protecting privacy means protecting individual's right to control how personal data is collected, processes and distributes to third parties and in establishing biometric smart card privacy must be considered as a basic design goals and the use of biometric smart card will strengthen the ability of the system to protect data privacy user[5]. Data privacy paradigm always influenced by the rapidly technology changing since the beginning that enable new form of recording, monitoring and surveillance[6]. Technology should not be perceived as threat to privacy but also could provide a tool to protect privacy. This paper will propose the model of regulation for data privacy protection that represent 4 (four) approaches that could empower the user to control their personal information which is base on international global privacy standards, state and business practices.

[2] Smart Card Alliance Report, *Smart Card and Biometrics*, (2011), 3.

[3] Daniel J. Solove and Marc Rotenberg, *Information Privacy Law,* (Aspen Publisher, 2003), 47.

[4] Abu Bakar Munir, *Data Protection Law In Asia, (*Sweet & Maxwell, 2014), 1.

[5] Smart Card Alliance Report, *Privacy and Security Identification System : The Role of Smart Cards as A Privacy Enabling Technology,* (2003), 4.

[6] Daniel J. Solove and Marc Rotenberg, (2003), above n.4, 50.

II. LEGAL MATERIALS AND METHODS

The legal materials of this paper are primary and secondary legal materials. Using the statute and conceptual approaches, this paper is divided into several parts. The introduction elaborates technological development using biometric data and how this issue faced with privacy issue as guaranteed as constitutional rights. It further discuss about how such biometric use might infringe privacy protection and finaly existing model of regulation is examined. New approach in model of regulation is proposed at the end of the paper

III. RESULT AND DISCUSSION

1. Overview of Biometric Smart card

Both government and business have been utilizing smart card to provide more secure and reliable forms of electronic identification[7] such as ID cards, passport and health card. Combining smart card technology with biometrics, which is based on unique physiological features of individuals such as fingerprint, face and iris recognition and behavior characteristic such as the use of software to monitor the manner of particular invidual, will create a positive binding of smart card and difficult to clone[8] additionally biometric data will directly related to individual . Under data privacy regulation, biometric data perceived as sensitive personal data and deserving for special protection and should be subject to more strict control comparing to general personal data. The data privacy issue on smart card biometric technologies is concerning with how far the personal data is used for identification by the data user, and the data user has the responsibility to protect the personal data in order to built the trust as the main pillar for the continuation of the relationship.[9] According to smart card alliance report, there are number of factors that could be in conflict with data privacy [10]:

1) the amount and type of personal informations that used by the ID system and in the case of biometric data was being use then it need more higher protection and how far the data subject will be able to control access of their personal data;
2) the extent of technology can secure the ID system for example the possibility of privacy by design approach;

[7] Smart Card Alliance Report, (2011), above n 3, 5.

[8] Ibid

[9] Smart Card Alliance, *Smart Cards and Biometrics in Privacy-Sensitive Secure Personal identification Systems, Report,* (2002), 7-8.

[10] Ibid, 6-7.

3) the policy to protect data privacy that restricting both access and use of personal data and controlled by choice system.

Identification Biometrics Smart card

Data privacy issue concern increased with regard to identification system that will be identiable person from their biometric data such as finger print, voice, Irish as accurate evidence of one's identity since it will potrays a very unique biological characteristics that distinguish one person from another[11] and the threat to data privacy arises not from the positive identification but from the ability of third parties to access the data and link personal data with another data base secondary uses without data subject consent. According to the ASCL (Association of School and College Leader) report that estimates about 30% of biometric data using for secondary uses[12]. In handling the biometric data subject and organization must take several steps:

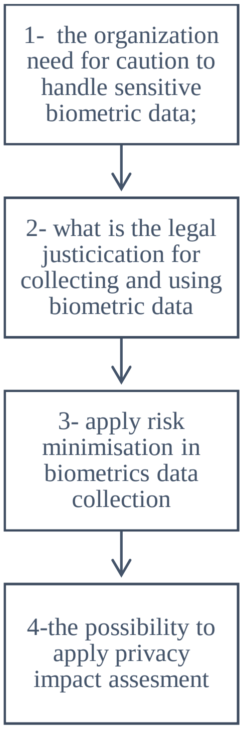
1- the organization need for caution to handle sensitive biometric data;
2- what is the legal justicication for collecting and using biometric data
3- apply risk minimisation in biometrics data collection
4-the possibility to apply privacy impact assesment

Figure 1. Steps in handling biometric personal data

2. Data Privacy Theory

The concept of data privacy protection emerged in the nineteenth century by the publication of two legal scholars Samuel Warren and Louis Brandeis's, who at the first time express there are *the right to privacy* as a result of technological development that caused a great harm to people’s comfort. Then afterwards, the right of privacy always referred to the *right to be let alone*[13] , implies that individuals have the right to

[11] Ann Cavoukian, *Privacy and Biometrics, Report, Information and Privacy Commissioners*,(Ontario 1999), 2-3.

[12] Biometrics data: Schools will need parent's approval, [http://www.bbc.com/news/education-18073988]

[13] Daniel. J. Solove and Marc Rotenberg, (2003), above n 4, 3.

decide whether to engage with society by sharing or exchanging their personal informations and to determine on what terms they are prepared to do so. Data privacy laws generally incorporates safeguards the use of personal data, and are subject to regulatory framework. Individuals or data subject have the right under personal data law to claim if the processing of their personal data against basic principles which is common under global privacy standards[14]. Alan Westin for the first time defines privacy as the right of the individuals to decide under what circumstances and to what extent their personal data will be exposed to others, and his theory is named as data privacy[15].

The data privacy theory then adopted into several multilateral legal instruments that establishing international recognized data privacy principles that have laid the foundation of most modern national data privacy laws[16] such as OECD's 1980 Privacy Guidelines that has been use as model to regulated data privacy in many jurisdiction , the Guidelines has defined personal data as as "any information relating to an identified or identifiable individual"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or toone or more factors that are specific to his or her physical, physiological, mental, economic, cultural or social identity[17]. The Guidelines are not legally binding but have long been recognized as a basic of norms that should govern data privacy and guide OECD members and private organizations in crafting their policies. The Guidelines define personal data as data relating to an identified or identifiable person however what exactly type of personal data is according to many interpretation but the main point is that data that connected to individuals that will be protected either by data itself or combined with other information. The listed below as examples include as data privacy such as a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of informations may still qualify as personal informations :

[14] David I. Brainbridge, *Introduction to Information Technology Law, (*Pearson Education Limited, 2008), 497.

[15] Alan F. Westin, *Privacy and Freedom,* (Atheneum, 1999), 32, see also, Abu Bakar Munir, Siti Hajar Mohd Yasin, Md Ershadul Karim, *Privacy,* (Sweet & Maxwell, 2014), 4-5.

[16] Privacy International report, *A Beginner Guide to Data Protection*, Report, (2013), 5.

[17] EU Data Protection Directive, 1995

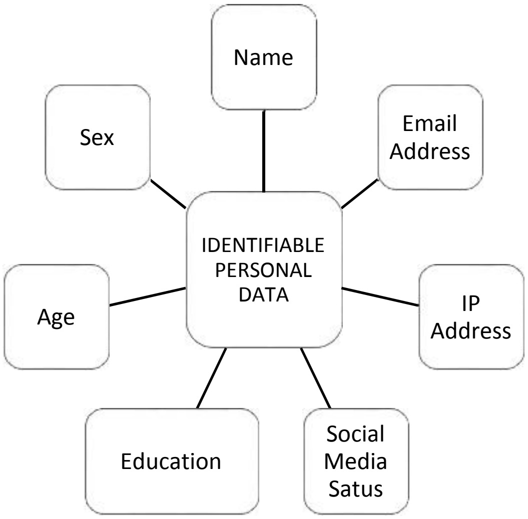

Figure 2.Identifiable personal data

Some jurisdictions mostly influenced by European Union approach, differentiate between ‘sensitive’ and ‘non-sensitive’ data based on the likelihood of harm an individual is likely to suffer if unauthorised processing were to occur. Sensitive data is typically afforded greater protection by the law. The processing of personal data is prohibited unless ‘explicit’ consent is obtained priory.

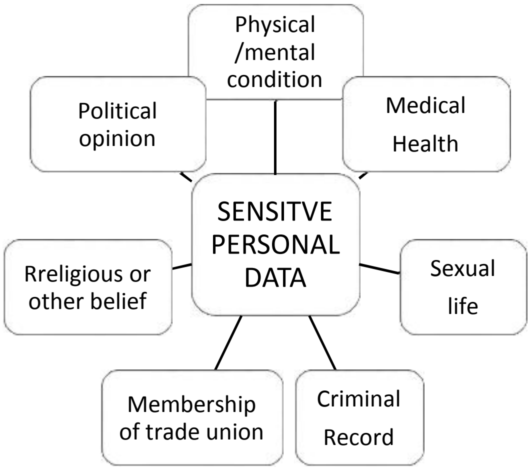

Figure 3.Sensitive Personal Data

Data privacy is protect how data privacy should be processing that including but not limited to:

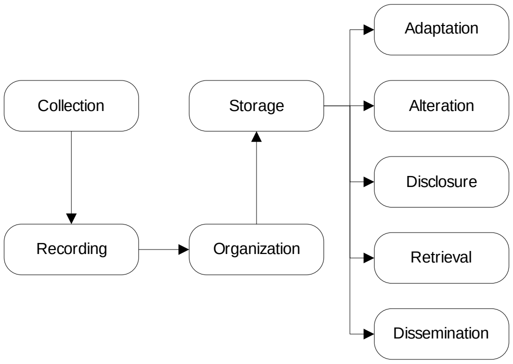

Figure 4.Personal Data Process

The Guidelines stipulate that the following principles should be adhered to when collecting and processing personal information and data:

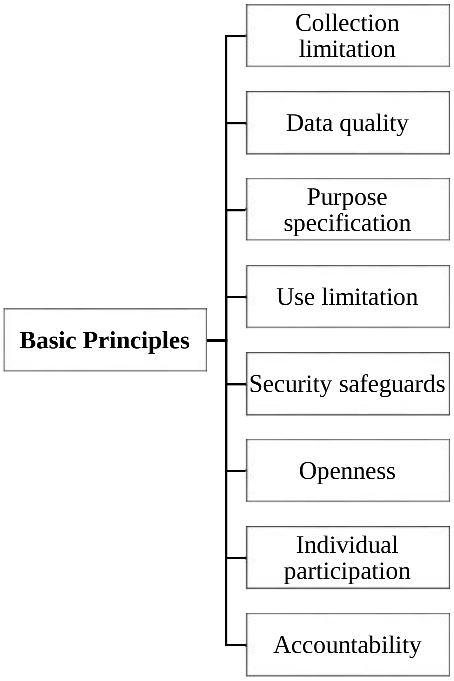

Figure 5. Basic data privacy principles in collecting and processing personal information and data

- Collection limitation: there should be limits to the collection of personal data, and data, which should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual
- Data quality: personal data should be relevant to the purposes for which they are used, and should be accurate, complete and kept up-to-date
- Purpose specification: the purposes for which personal data are collected should be specified and any subsequent use must be limited to that specification
- Use limitation: data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the individual or b) by the authority of law
- Security safeguards: data should be protected by reasonable security safeguards to protect against lost, destruction, use, modification or disclosure
- Openness: there should be a general policy about openness with respect to personal data
- Individual participation: an individual should have the right to find out information about their data and to have incorrect data erased or rectified
- Accountability: a data controller is accountable for complying with these measures.

Many multinational companies abide by these data protection principles as a way of ensuring minimum compliance in jurisdictions where Data Protection laws either do not offer stringent enough protections or do not exist.[18]

3. Model of Regulation

The model of regulation is the adaption model from Lawrence Lessig Modalities [19] named as hybrid approach that stated 4 (four) factors or modalities which can be used by individuals to control activities in information technology sector and each of this modalities have functions as a constrain on the individual actions those are (1) Law that form by the government that will impose ex post as a sanction ; this approach also posed many constraint such as how to balance between protection and innovations and causing debate since many have to harmonize the regulation and not causing a legal barrier to global information flows [20]. So the

[18] Privacy International Report, *Ibid*

[19] Lawrence Lessig, *Code Version 2.0, Basic Book* ,(New York, 2006), 290.

regulations have to be added by (2) Social norms through imposing the societal sanction in the extent the how far individual ought to behave and the sanction will be enforced not through legal norm but rather though the expectation within a particular community; (3) the third constraint is corporate privacy regulation; In the digital economy era data is the oil of 21 st Century and to extract and use data will gain a huge rewards for corporation so it is important to smooth the data functionality from the government to companies i.e :Today, data infrastructure is become a profit center and since data is the main raw materials to conduct a business , companies must treating data as corporate asset. Personal data is one of the assets, so by using, keeping and maintaining personal data the company will create new products and services. Treating data as a strategic asset indicates that organizations need to build inventories of existing data just as they do for physical assets. Organizations need to establish corporate business management to prevent from unauthorized utilization and disclosure of personal data as they can affect the integrity of the company quality and reliability of daily business decisions. Depending on the business of the organization, it must protect sensitive data, such as customer information, patient information, credit card numbers and personally identifiable information (PII), as well as intellectual property.

The main goals of business are to keep the business growing, gaining profits and maintaining the business by way of attaining customer trust and satisfaction as to get customer’s loyalty. In return, loyal customer may recommend the business to others, and also it may lead to repeat purchase. Hence, it is essential to gain and keep a trust.

In ICT business there two pillars of trust, namely Security and Privacy. Therefore, corporate should establish the standards of business conduct that will embedded in corporate management conduct. This standards will be drawn in the form of corporate privacy rules in protecting customer data privacy:

1. Employees must comply with data privacy laws and regulations and data privacy contractual requirements that apply to personal identifiable information;
   a. Comply data privacy principles to limit comply collection, use, access, distribution costumer personal data;
   b. Comply with company privacy policy
   c. Provide corporate security manuals;
   d. Report immediately for all suspected and actual personal data breach

e. Bring all failure to the attention of supervisors, customers, subcontractors and vendors.

(4) The Final model of regulation is by technology in the form os software or hardware that will determine how people should interact. [21]For example the PET which is defines "*is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without theloss of the functionality of the information system.*"

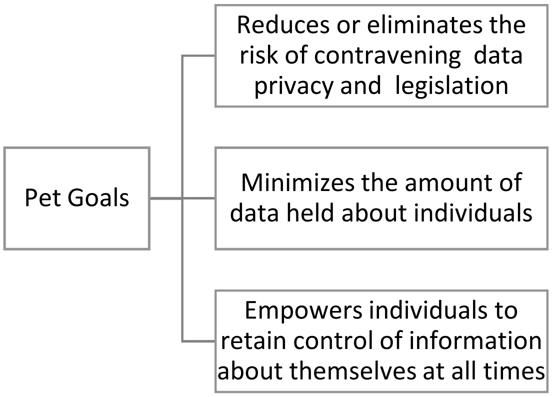
Pet Goals
Reduces or eliminates the risk of contravening data privacy and legislation
Minimizes the amount of data held about individuals
Empowers individuals to retain control of information about themselves at all times

Figure 6. PET Goal

PET for example is encryption. Encryption today is a relatively mature technology, though still in a state of advancement. Encryption supports the security and proportionality principles of data protection law. In the past two years we have seen an increasing trend for regulators to become more prescriptive in their approach to encryption,[22]. Anonymisation also use as a one of the model to protect data privacy and the main principles is that the data rendered shall be anonymous in such a way that the data subject is no longer identifiable[23].

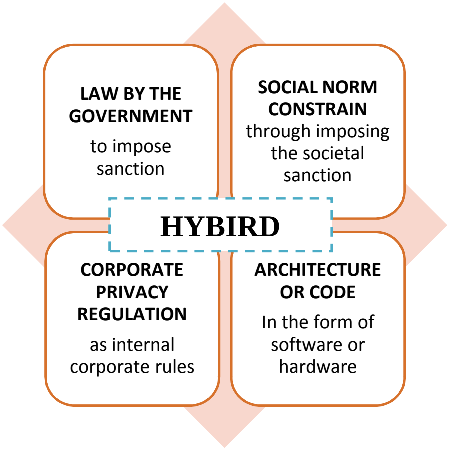
LAW BY THE GOVERNMENT
to impose sanction
SOCIAL NORM CONSTRAIN
through imposing the societal sanction
HYBIRD
CORPORATE PRIVACY REGULATION
as internal corporate rules
ARCHITECTURE OR CODE
In the form of software or hardware

Figure 7. Hybrid model of regulation

The hybrid model offered in this paper is the combination of four crucial elements, which include law by the government, social norm living within the society, corporate privacy regulation and relevant code. While each element usualy goes sectoraly without integration, often it resulted in the overlapping of regulations. Thus, it is proposed that those four elements should be integrated and read as cumulative elements in regulating the use

[21] Lawrence Lessig, *(2006), above n 20,* 290. See also Andrew Murray, *Information Technology Law, The Law and Society*, (Oxford University Pers, 2010), 62-63.

[22] Privacy Report, above n 19.

[23] ICO Report, *Privacy By Design*, https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

of biometric data without violencing the privact issue and other constitutional rights.

IV. CONCLUSION AND SUGGESTION

This article concludes that data privacy is a legal right regulated and controlled by both international and national instruments, and the use of biometric smart card often viewed as a conlict between the need of security and how far the system protects data privacy. The model of regulation approach is aimed to ensure privacy data protection. The approach is called hybrid model of regulations that combine 4 (four) approaches namely; government regulations, social norms, corporate privacy rules and technical regulations.

REFERENCES

Books

Abu Bakar Munir, *Data Protection Law in Asia*, (Sweet & Maxwell, Hongkong, 2014)

Alan F. Westin, *Privacy and Freedom,* (Atheneum, 1967)

Andrew Murray, *Information Technology Law*, *The Law and Society,* (Oxford University Pers, 2010)

Daniel J. Solove and Marc Rotenberg, *Information Privacy Law,* (Aspen Publisher, 2003)

David I. Brainbridge, *Introduction to Information Technology Law,* (Pearson Education Limited, 2008)

Ian J. Llyod, *Information Technology Law,* (Oxford University Press, Oxford, 2011)

Lawrence Lessig, *Code Version 2.0*, Basic Book , (New York, 2006)

Report

Ann Cavoukian, Privacy and Biometrics, Report, Information and Privacy Commissioners, Ontario, 1999.

Biometrics data : Schools will need parent's approval, [http://www.bbc.com/news/education-18073988]

Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honors and reputation (art. 17).

Privacy International report, *A Beginner Guide to Data Protection,* Report, pp, 2013.

Smart Card Alliance Report, *Smart Card and Biometrics,* 2011.

Smart Card Alliance Report, *Privacy and Security Identification System : The*

Role of Smart Cards as A Privacy Enabling Technology, 2003.

Smart Card Alliance Smart Card Alliance Report, Smart Card and Biometrics, 2011.

Smart Card Alliance, *Smart Cards and Biometrics in Privacy-Sensitive Secure Personal identification Systems*, Report, 2002.