SOME LEGAL ISSUES OF BIOMETRIC DATA PROTECTION IN THAILAND [*]

Panurut Chuenpukdee
Master of Laws in Business Laws (English Program)
Faculty of Law, Thammasat University
Email address: panurut.chuenpukdee@gmail.com

Received 2 October 20
Revised 30 November 20
Accepted 9 December 20

Abstract

Biometrics is a technology that can measure and analyze the physiological and behavioral characteristics of a person. Unlike a password, Biometrics data is hard to fake or steal. Since a person was born, he or she would have his or her specific fingerprints, iris, or facial which are unlike others. Biometrics is so convenient that it can identify persons from his or her own physiological or behavioral characteristics. However, Biometrics data is specific for each person. Hence, it could not be changed. Would it be dangerous if someone could hack, fake, or use our biometrics data, or is it dangerous if someone uses our Biometrics data in transactions? Is there any law in Thailand that could protect our Biometrics data in practice? Thailand has many laws that mention the rule for the protection of biometric data. Especially, The Personal Data Protection Act B.E.2562 ("PDPA") which is the first data protection act of Thailand. It provides a significant rule for the collection, use, and disclosure of personal data including biometric data. However, the PDPA is the first personal data protection act in Thailand which is very new. It provides only general and broad rules for processing all types of personal data including the biometric data which is mentioned in the Act as only a type of "personal data". There

[*] This article is summarised and rearranged from the thesis "Some Legal Issues of Biometric Data Protection in Thailand", Faculty of Law, Thammasat University, 2019.

are limitations to existing laws in Thailand to protect biometric data. It has many risks in the collection, use, and disclose of Biometric data. The provisions in The Personal Data Protection Act B.E.2562 remain unresolved in practice. Hence, This article will study the important practical issues that could happen with the PDPA which are the issues of “public interest”, “substantial public interest”, “explicit consent”, “civil liability” and “compensation”. The study of the General Data Protection Regulation of the EU (GDPR) (as a general rule followed by the PDPA), the UK Data Protection Act 2018, along with the UK’s Information Commissioner’s Office (to know how the member states provide the rules in accordance with the GDPR), and Illinois Biometric Information Privacy Act (as the first Biometric data protection act of USA) would be the best examples for Thailand to amend the act and to have a guideline for processing biometric data in order to enable it to govern the issues practically.

Keywords: Biometric Data, Personal Data, Data Protection

1. Introduction

Recognition Technologies play an important role in peoples' lives. Students or employees may be required to identify themselves at schools or workplaces by scanning students' or employees' cards. Currently, many schools and companies are using technologies that can recognize and identify persons. Instead of scanning students' or employees' cards, the technologies nowadays can identify persons by scanning their fingerprints, facials, or irises in order to identify them.[1] In today's world, many airports around the world use recognition technology to detect fingerprints or iris to identify passengers.[2] These technologies are also part of our daily lives such as a smartphone. Many smartphone brands provide the technology of fingerprints and facial recognition to unlock the phone. The technologies also have been used for banking businesses. That is, Mobile banking services have become one of the most important applications on the Internet being provided by most of the banks all over the world. The end-user can manage the accounts or make some payments without being forced to go to the physical bank office. All the technologies mention earlier are called "Biometrics". which is the word derived from Greek.[3] "Bio" means "life", "Metrics" means "to measure". There are two principal types[4] of biometrics which are; (1) physiological, such as, fingerprints, iris, and facial recognition, and (2) behavioral characteristics, such as, gait, voice, and signature

[1] Joss Fong, 'What facial recognition steals from us' (*VOX*, 10 December 2019) <https://www.vox.com/recode/2019/12/10/21003466/facial-recognition-anonymity-explained-video> accessed 10 January 2020.

[2] Webfact, 'VIDEO: Fingerprint and facial recognition now scanning passengers at Don Mueang Airport' (*ThaiVisa Forum*, 27 May 2019) <https://forum.thaivisa.com/topic/1103036-video-fingerprint-and-facial-recognition-now-scanning-passengers-at-don-mueang-airport/> accessed 6 November 2019.

[3] JAMMI ASHOK, VAKA SHIVASHANKAR, P.V.G.S.MUDIRAJ, 'AN OVERVIEW OF BIOMETRICS' (2010) 2(7) International Journal on Computer Science and Engineering' 2402-8.

[4] Shimon K Modi, *Biometrics in Identity Management: Concepts to Applications* (Artech House, Norwood 2011) 3.

recognition. Apart from biometrics that we have already known, for example, there are many other types of biometrics such as, retina scanning, DNA matching, vein recognition, etc.

2. Privacy concern of biometric data

Currently, we see the collection and use of Biometrics in many private and public organizations. For example, all the district offices in Bangkok have been using the technology of Biometrics on fingerprints collection in order to identify citizens.[5] Besides, due to the lack of technology, government sections may empower private sections to collect Biometrics data. For example, the Ministry of foreign affairs is going to collect the irises' data of citizens. Like other government sectors, the ministry does not collect Biometric data by itself due to the lack of technology. Hence, It empowers a private company to collect Biometrics data of citizens. What could be a guarantee that the government or private company would process our Biometric data properly? Does Thailand have a law that protects the collection, use, and disclosure of biometric data by the government or private section practically?

3. Five practical issues of the Personal Data Protection Act B.E. 2562 ("PDPA")

This article has found that Thailand does not have specific laws that protect the processing of Biometric Data in enough detail to be practically applicable. However, the protection of Biometric data is mentioned in many laws that are the Constitution of the Kingdom of Thailand B.E. 2560, Thailand Civil and Commercial Code, Thailand Penal Code, Computer-Related Crime Act (No.2) B.E 2560, Official Information ACT, Electronic Transaction Acts B.E. 2544. Also, the Personal Data Protection Act B.E.2562

[5] ThaiPR.net, 'Kor Tor Mor Num Rong Tum Bat Pracham Tua Doi Chai Rabob Computer Pim Lai Niw-mue [Bangkok Launched a Plan to use Fingerproint ID Card System]' (*RYT9*, 27 January 2004) (กทม.นำร่องทำบัตรประจำตัวประชาชนโดยใช้ระบบคอมพิวเตอร์พิมพ์ลายนิ้วมือ (*RYT9*, 27 January 2004)) <https://www.ryt9.com/s/prg/128254> accessed 4 April 2020.

which is the first personal data protection act of Thailand may have five practical problems that could occur in the processing and protection of Biometric data in practice.

(1) Issue of public interest: The PDPA provides the significant rule for the collection, use, and disclosure of personal data that must be consented by the data subject, except for the use for the “public interest”. However, it could be said that all state missions are considered to be done for the public interest. There is no need for the state to seek our consent to collect, use, or disclose our Biometric data. As a result, the citizens could not sue the government or private sector for their acts. Since the PDPA does not provide the definition, guidelines, or scope for the processing of Biometric data relating to the public interest. The scope of public interest needs to be addressed in order to process Biometric data in practice.

(2) Issue of substantial public interest: Since the PDPA provides the condition to collect Biometric data beyond general personal data by prescribes the word “substantial public interest” for Biometric data apart from the “public interest” for general personal data. However, the PDPA does not define the word “substantial public interest” for the processing of Biometric data. Then the definition and scope of substantial public interest need to be considered in order to process Biometric data practically in order to know the difference between the “public interest” and “substantial public interest”.

(3) Issue of explicit consent: In Thailand, the PDPA follows the rule of processing Biometric data of the GDPR by having the PDPA section 26 which states that “…collection of Personal Data pertaining to…Biometric data…is prohibited, without the explicit consent from the data subject…” However, the PDPA does not define the terms “explicit consent”. Hence, there would be a problem in the processing of the Biometric data in practice in order to know the difference between “consent” and “explicit consent”.

(4) Issue of civil liability: the problem is that the PDPA section 77 provides the words “causes damages to the data subject”. The word “causes damages” shall have the same rule as the tort law that there

needs to have actual damages to the data subject. Practically, there would be an argument against an injured person under section 77. The controller who violates the PDPA may argue to dismiss the case that he only violates the PDPA by processing Biometric data without the data subject's consent for instance, but there are no damages to the data subject yet. This provision seems to contradict the purpose of the PDPA which has the purpose to protect the personal data by controlling the controller and the processor not to violate the PDPA.

(5) Issue of compensation: If there are many times of the violation of the PDPA but actual damages still not occur. For example, a grocery store uses facial recognition by storing faces of customers many times without their consent. The customers as the data subject may not have a chance to claim for compensation since they could not know the exact or amount of damages occurring to them. It is very hard for them to show evidence of their damages to the court. As a result, it would be a problem for them to claim compensation in practice which is contradicted to PDPA that has the purpose to fully protect the personal data.

4. The solutions for the five practical issues in foreign countries

The study of the General Data Protection Regulation (GDPR) of the EU (as a general rule followed by the PDPA), the UK Data Protection Act 2018 (DPA 2018) along with the UK's Information Commissioner's Office (ICO) (as the member state following the rule of the GDPR), and Illinois Biometric Information Privacy Act (BIPA) (as the first Biometric data protection act of USA) would be the best examples for Thailand to amend Thai law and to have a guideline for processing biometric data in order to enable it to govern the issues practically.

(1) Issue of public interest: Since the GDPR mentions the terms of processing the personal data in article 5(1) (a) which is the principle of lawfulness, fairness, and transparency. Also, the controller needs to meet one of the six conditions in the GDPR article 6(1) which is known as "lawful ground”. “Public interest” is one the lawful grounds prescribed in the GDPR article 6 (1)(e) “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;…” The problem is, the GDPR does not define the term of "public interest".

As the study of the UK Data Protection 2018 ("DPA 2018"), normally, the terms prescribed in the DPA 2018 part 2 provide the same meaning as the GDPR. In some cases, the DPA 2018 modifies, clarifies, and supplements the GDPR since the GDPR does not provide some terms. For example, in the context of public interest, the DPA 2018 supplements the rules of processing public interest by prescribing the DPA 2018 section 7 which provides that

"… (1) For the purposes of the GDPR, the following (and only the following) are" “public authorities” and “public bodies” "under the law of the United Kingdom— (a) a public authority as defined by the Freedom of Information Act 2000",… "(2) An authority or body that falls within subsection (1) is only" a “public authority” or “public body” for the purposes of the GDPR when "performing a task carried out in the public interest or in the exercise of official authority vested in it…"

Moreover, in the context of public interest, the DPA 2018 section 8 also provides a non-exhaustive list of examples of “Lawfulness of processing public interest” which refer to the GDPR article 6(1)(e) which states that

“In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest …"

As the DPA 2018 sections 7 and 8 provide only examples list of processing of public interest tasks. The Information Commissioner’s Office (ICO) which is the guideline for using the GDPR and the DPA 2018 in the UK then needs to comes to describes. The ICO provides the measurement[6] that even if the processing will fall outside the list provided in the DPA 2018 section 8, but it is still considered to be a public interest task by considering on the nature of the function not the nature of the organization., e.g.:

(a) "The administration of justice processes personal data for the public interest task should be able to rely on the GDPR article 6(1)(e)"

(b) "A private electric company does not fall within the definition of public authorities in the DPA 2018. However, the company is considered to be public authorities as it carries the function of providing public interest. It should be able to rely on the GDPR article 6(1)(e)"

Moreover, the organization must specify the relevant task and be able to demonstrate that there are no other reasonable and less intrusive means to achieve that purpose.

(2) Issue of substantial public interest: According to the processing of the special category data of the DPA 2018 and the ICO, the Biometric data as one of the special category data which needs more protection because it is sensitive data. To process Biometric data, the controller needs to concern 5 Steps:[7]

Step 1: Consider the lawful basis according to the GDPR Article 6 "processing of personal data shall be lawful"[8]

Step 2: Consider the separate 10 conditions provided for processing according to the GDPR article 9. "processing of special categories of personal data"[9]

[6] Information Commissioner's Office, 'Public task' (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/> accessed 22 May 2020.

[7] Information Commissioner's Office, 'Special category data' (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> accessed 5 May 2020.

[8] General Data Protection Regulation (GDPR) art 6.

[9] ibid, art 9.

Step 3: Consider the requirement for the controller to meet additional conditions set out in the DPA 2018 schedule 1 part 2. Since the GDPR article 9(g) states the rule to process special category data relating to the substantial public interest. However, it does not define the substantial public interest. Then the DPA 2018 Schedule 1 part 2[10] provides the 23 substantial public interest conditions.

The controller must identify which of these conditions appears to most closely reflect his purpose. The controller needs to demonstrate that specific processing is "necessary for reasons of substantial public interest", on a case-by-case basis. A generic public interest is not enough since the public interest covers a wide range of society. Also, the controller needs to make specific arguments about the concrete wider benefits of the processing.

Step 4: The controller must determine his or her conditions for processing Biometric data as special category data. There are also needs to have an 'appropriate policy document' in place in order to meet a UK Schedule 1 condition for processing in the DPA 2018.

Step 5: Lastly, for any type of processing that is likely to be high risk, the controller needs to complete a data protection impact assessment (DPIA).

(3) Issue of explicit consent: The ICO acknowledges that the GDPR does not provide a clear distinction between consent and explicit consent. However, the ICO provides that the "Explicit consent is not defined in the GDPR, but must meet the usual GDPR standard for consent." In particular, "it must be freely given, specific, affirmative (opt-in) and unambiguous, and able to be withdrawn at any time. In practice, the three extra requirements for consent to be 'explicit' are likely to be"[11]

[10] Data Protection Act 2018 (DPA) Schedule 1 part 2.

[11] Information Commissioner's Office, 'What are the condition for processing?' (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-

1. "explicit consent must be confirmed in a clear statement (whether oral or written), rather than by any other type of affirmative action;"
2. "it must specify the nature of the special category data; and"
3. "it should be separate from any other consents you are seeking"

(4) Issue of civil liability: The Civil Liability for violation of the Illinois Biometric Information Privacy Act ("BIPA") was introduced as "Right of action" The BIPA provides the rules of the right of action in the BIPA section 20 which prescribes that *"Right of action. Any person aggrieved by a violation of this Act shall have a right of action"*

From the BIPA, it set out that a person can be sued if he fails to inform opt-in consent for collecting biometric data. Moreover, data subjects mealy have to prove only that their biometric privacy is injured but they do not need to prove other injuries like identity fraud or physical harm. There also be the study case of The Illinois Supreme Court mentioned to this rule, that is, *Rosenbach v. Six Flags.*[12] The defendant violated the BIPA by failing to seek the consent of the plaintiff. The defendant filed a motion that the plaintiff was not an "aggrieved party" under sec. 20 of the BIPA because the plaintiff had not alleged an "actual injury." However, the court ruled that only the violation of the law itself is sufficient to support a private right of action under BIPA. There is no need to be actual damages of the plaintiff.

In sum, as the PDPA section 77 provides the words "causes damages to the data subject" which could be interpreted to be an injured person according to the rule of tort law which requires actual damages of an injured person. However, as the example of the rule of "aggrieved party" provided in the BIPA, the aggrieved party can sue the defendant for violating of the BIPA without concerning actual damages.

(5) Issue of compensation: The BIPA Section 20 provides that a person shall have "the right to recover each violation:"

protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> accessed 22 May 2020.

[12] *Rosenbach v. Six Flags Entertainment Corp.,* 2019 IL 123186.

(1) “against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;"

(2) "against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;..."

There is an example case supporting this rule, that is, Brian Norberg v Shutterfly, in this case, there were many times of breaching the BIPA. Consequently, the court ruled under the BIPA section 20 that the plaintiffs had the rights to

1 "Awarding statutory damages of $5,000 for each intentional and reckless violation according to the BIPA section 20(2)."

2 "Awarding statutory damages of $1,000 for each negligent violation according to the BIPA 20(1)"

According to the study, The BIPA provides the minimum standard liquidate damages of $1,000 for negligently, and of $5,000 for each intentionally or recklessly violates the BIPA.

5. Conclusion and suggestions

From the study of the five concerning issues and solutions, this article would suggest guidance for the processing of biometric data in Thailand in practice as follows:

(1) The issue of public interest: Thailand should provide the guidelines and standard rules for the measurement of processing personal data pertaining to the public interest, by following the rules of the DPA 2018 and the ICO, that is;

1. “Determine whether an organization performs the public interest task by considering the nature of the function not the nature of the organization.”

2. “An organization that processes the personal data or Biometric data must be able to specify the relevant task and to shows a reasonable

purpose and less intrusive means to achieve that purpose. For example, a district sector must provide the reason for citizens in the collection of fingerprints. Also, It needs to choose the best way to reduce all the risks that could occur to these fingerprints information.

(2) The issue of Substantial public interest: I would suggest the following 5 required steps to process biometric data in Thailand:

Step 1: Consider the lawful basis (by following the GDPR, Article 6)

Step 2: Consider the separate 10 conditions (by following the GDPR, Article 9) in order to have more protection for the processing of special categories of personal data.

Step 3: Consider The requirement substantial public interest conditions for the processing of special category data (by following the DPA 2018, Schedule 1 part 2) in order to identify which of these conditions appears to most closely reflect his purpose.

Step 4: The controller must determine his or her conditions and have an 'appropriate policy document' in place. (by following the DPA 2018, schedule 1) because this document will demonstrate that the processing of special category data based on the rules on steps 1 – 3 above.

Step 5: Lastly, for any type of processing that is likely to be high risk, the controller needs to complete a data protection impact assessment (DPIA).

(3) The issue of explicit consent: I would suggest that Thailand should follow the guideline provided by the ICO by having the guideline of "explicit consent" in the processing of Biometric data that need to be under these 3 conditions which are;

(1) "a clear statement,"

(2) "specify the nature of the special category data,"

(3) "separate from any other consents you are seeking."

(4) The issue of civil liability: Since the words prescribed in the PDPA section 77 "causes damages to the data subject" could be interpreted to be an injured person according to the rule of tort law which requires actual damages of an injured person. I would suggest that there should be the amendment of the PDPA by removing the word "causes damages to the data subject" so that the data subject would sue the defendant for violating of the BIPA without concerning actual damages to have the law that fully protects the Biometric data according to the purpose of the PDPA.

(5) The issue of compensation: Biometric data is considered to be a special type of data that needs to be highly protected under the PDPA, if there are many times of the violation of the PDPA, the data subject should get compensated for each violation. I suggest amending the PDPA by

1. "Adding the right to recover for each violation"
2. "Adding minimum standard liquidate damages by indicating the minimum amount of liquidated damages in each intentional and reckless violation or each negligent violation"

For example, if a shopping mall violates the law by collecting fingerprints without the consent of customers five times, the customers shall have the right to claim compensation for five violations with a minimum standard liquidate damage for example 10,000 baht for each violation.

Bibliography

Book

Modi S K, *Biometrics in Identity Management: Concepts to Applications* (Artech House, Norwood 2011)

Case

Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186

Journal

ASHOK J, SHIVASHANKAR V, MUDIRAJ PVGS, 'AN OVERVIEW OF BIOMETRICS' (2010) 2(7) International Journal on Computer Science and Engineering'

Legislations

Data Protection Act 2018 (DPA)

General Data Protection Regulation (GDPR)

Websites and Blogs

Fong J, 'What facial recognition steals from us' (*VOX*, 10 December 2019) <https://www.vox.com/recode/2019/12/10/21003466/facial-recognition-anonymity-explained-video> accessed 10 January 2020

Information Commissioner's Office, 'Public task' (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/> accessed 22 May 2020

'Special category data' (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> accessed 5 May 2020

‘What are the condition for processing?’ (*ICO.*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> accessed 22 May 2020

ThaiPR.net, ‘Kor Tor Mor Num Rong Tum Bat Pracham Tua Doi Chai Rabob Computer Pim Lai Niw-mue [Bangkok Launched a Plan to use Fingerproint ID Card System]’ (*RYT9*, 27 January 2004) (กทม.นำร่องทำบัตรประจำตัวประชาชนโดยใช้ระบบคอมพิวเตอร์พิมพ์ลายนิ้วมือ (*RYT9*, 27 January 2004)) <https://www.ryt9.com/s/prg/128254> accessed 4 April 2020

Webfact, ‘VIDEO: Fingerprint and facial recognition now scanning passengers at Don Mueang Airport’ (*ThaiVisa Forum*, 27 May 2019) <https://forum.thaivisa.com/topic/1103036-video-fingerprint-and-facial-recognition-now-scanning-passengers-at-don-mueang-airport/> accessed 6 November 2019