THE DIGITAL AGE AND THE CREATION OF INNOVATIONS IN THE PRIVACY LAW OF THAILAND

Korakod Tongkachok, Thaksin University
Thongphon Promsaka Na Sakolnakorn, Silpakorn University

ABSTRACT

This research article aimed to study legal innovations in the personal data section of Thailand. Personal data was found to be related to a person's right to privacy, which was a fundamental right of a person. Because it was information that informed or identified the subject of the data subject, personal data was required by law to provide protection. Measures or criteria must be established for who will use the personal data. For example, government agencies, private entrepreneurs, or any other person who was the data controller or processor of personal data, which must comply with the law. Therefore, as the public sector, the entrepreneurship, and the people who entered the digital age, personal data had to be protected. Innovating to support the law of the data controller must obtain the consent of the data subject prior to the collection, use, or processing of that personal data. When protecting personal data was a priority, EU countries, the United States, or ASEAN countries had specific personal data protection laws. Thailand had a concept of personal data protection as stipulated in the Constitution of the Kingdom of Thailand and currently promulgated the Personal Data Protection Act B.E. 2562 (2019).

Keywords*:* Personal Data, Personal Rights, Protection, Personal Data Innovation Thailand

INTRODUCTION

At present, the rate of user growth through networks and the Internet around the world, including Thailand, is increasing and is growing rapidly. This can be seen from the number of Internet users in Thailand increasing each year with millions. These create new societies and communities in cyberspace with a good society that brings about the exchange of information, learning, education, conducting business activities, and more. In the world of society surrounded by technological advancements, it brings convenience, thought development from a vast knowledge base on the world of Internet, fast and far-reaching communications. In the advancement of society (Trakman, Walters & Zeller, 2020), hidden evil societies have evolved to encroach on individual and corporate rights in a number of ways especially the invasion of Internet privacy, which is becoming increasingly violent and damaging to great value scale. Therefore, in every country including Thailand, there must be a law to protect basic rights. Laws in information technology are essential in society.

The right to privacy is a fundamental right that applies to all human beings and is a right that the law has been recognized, such as Article 32 of the Constitution of the Kingdom of Thailand B.E. 2560, Fourth Amendment to the United States Constitution (Determann & Gupta, 2018; Carpenter, 2020), European Convention on Human Rights (EUCHR) (Rozakis, 2020; Banisar & Davies, 1999), etc. Personal Data/Personal Information is related to an individual's right to privacy (Maginnis, 2000). This makes it possible to identify or potentially identify the natural person who is the subject of the data (Aserkar, Seetharaman, Chu, Jadhav & Inamdar, 2017). In addition, the laws of some countries prescribe personally identifiable audio and video as personal information. Personal information is information that can be used to link the person who owns the information. Nowadays, there are problems with personal information such as the

risk of identity theft for crimes, the use of personal information to process information for exploitation. Problems that arise in Thailand are often cases of the use of consumer's personal information in marketing or offering of various products or products. For example, when a consumer applies for a commercial bank credit card, the bank usually requires the consumer to sign a consent document to disclose personal information such as a mobile phone number with the bank's affiliates. This creates the problem of offering health insurance, life insurance, or other financial products to consumers over the phone. This will also cause serious trouble for consumers who own the data, but also cause distress to the data subject. This is because the data subject may not know who their personal information has been passed on, for what purpose, or how long it has been kept. In these problems, we cannot deny that personal information sometimes is no longer personal or private, and sometimes personal information may be used in illegal ways and cause damage to the owner of personal information. Therefore, in order to protect the interests of individuals regarding their personal information not to be used by others without their consent, countries including Thailand come up with the concept of legislation relating to personal data protection/data privacy in order to establish guidelines on the protection of personal data and the wrongful use of the personal information of others. Therefore, the purpose of the study is to study foreign privacy laws and principles fundamentals for innovation in personal data protection of Thailand.

RESEARCH METHOD

This was a study of the basic principles of personal data protection, the development of the Thai and foreign personal data protection laws, and the current rules of the Thai personal data protection law to understand the meaning of Personal information that the law provided and the Personal Data Protection Regulations of the Thai Law, which was the personal data protection Act B.E. 2562. In addition, this study used an in-depth interview method by interviewing with private and public personal information officers, concerned citizens as owners of personal information. In addition, there was also a discussion of personal information related groups to analyze the creation of innovation to support Thailand's personal information.

LIRATURE REVIEW

The European Union was a group of countries that had made great progress and advancements in the protection of personal data and the so-called "GDPR" (General Data Protection Regulation) (Goddard, 2017). The Personal Data Protection Law of Thailand has also adopted the EU Personal Data Protection Principle that was a comprehensive personal data protection law (Zeno-Zencovich, 2020). Both the public and private sectors were obliged to protect personal data, as the world over recognized the principle that the law applied to both the public and private sectors. In addition to the EU General Data Protection Law or GDPR, APEC Group's Cross-Border Privacy Rules or “CBPR” (Sullivan, 2019) were also protected. This GDPR was not a law, but it was a personal data protection practice or agreement that APEC uses to facilitate operators in moving or transferring data across borders to operate business. GDPR was used all over the world to protect personal data which was not limited to only APEC member states.

Personal data protection in accordance with international laws. The concept of personal data protection first took place in Germany, where the first privacy law was the Hessen State Law (Kuner, 2010), the law that was enforceable at the state level and established in 1970. Later, in 1977, Germany (Vezzoso, 2015) enforced the Federal Act on Data Protection (Lachaud, 2018; Fondren, & McCune, 2018) and later other countries enacted privacy laws such as France and the United States. In addition, ASEAN countries such as Malaysia, Singapore, and the Philippines had specific laws that protect personal information.

In 1995, the European Union issued Directive95/46/EC (Malatras, SanchezBeslayCoisel, VakalisD'Acquisto & Zorkadis, 2017) came into force in the Member States of the European Union (Decker & Ford, 2017) as a personal data protection and freedom data movement act. Later in 2016, the European Parliament adopted a new data protection law, the EU General Data Protection Regulation (GDPR), which came into effect in 2018 (Regulation, GDP (It was a material law protecting the rights of citizens of the European Union with respected to personal information and privacy, with rules on the use of extraterritorial jurisdiction (Svantesson, 2015). That was to protect the personal information of EU citizens, whether that information was collected or in any area of the world, which imposed a penalty on people who caused damage or caused leakage of personal information (Voigt & Von dem Bussche, 2017) with a fine of 20 million euros or a fine of up to 4% of the entity's global revenues, which depends on which amount was greater, and set out criteria on the subject's consent and the withdrawal of consent (Mohamed & Zulhuda, 2019).

RESULTS & DISCUSSION

Currently, many countries have placed great importance on the protection of personal data, whether it is EU countries, the United States, and ASEAN member countries such as Thailand, Indonesia, Malaysia, Philippines, Singapore, and Vietnam, etc. Many countries have enacted privacy laws to protect the rights of their citizens. As for the universal privacy principles, guidelines are set and the focuses are on defining and describing lawful principles on the collection, usage, or disclosure of personal information and to maintain security of personal information to be safe, but these may differ in content or substance in certain areas depending on the country context.

From group discussions, related people saw that in the issue of standardization, we can summarize the stance of countries in the Asia Pacific region on the protection of personal information to be consistent that there was a need to raise the level of protection standards more. It was not just to preserve the rights of a person, but to have clear standards that increased economic opportunities for the private sector of their country. In other words, both the public and private sectors recognized the need for a balance between "privacy protection" (Bhasin, 2016) and "promoting the free flow of information" (Shahwahid & Miskam, 2014), leading to the creation of economic competitive opportunities. This was because increasing consumer trust both locally and internationally was a key to increasing the competitive edge for businesses dealing with large amounts of personal data, whether IT businesses with sale points being at the free and flexible movement of information or service businesses that were concerned with meeting the needs of individual customers who needed to know and maintain information that may be particularly personal sensitive data of the customer. While different countries had different needs for protecting personal information according to socioeconomic conditions, people of different countries may have different attitudes and trust in disclosure. All countries should consider the consistency between national measures and international standards and strive to keep their protection systems up to date, both in legal and technological terms.

How can the Personal Data Protection Act B.E. 2562 come into force in May 2020 to help protect our personal information more safely? The Personal Data Protection Act B.E. 2562 will come into force. This law relates to all of us as the data subject and includes operators and entities directly responsible for collecting personal information for our purposes. These can be summarized into 8 points as follows:

1) Personal Data Protection Law for natural persons only. Personal information is information about an individual that makes it possible to directly or indirectly identify that individual (Peng, 2011), but does not specifically include information of the deceased. Therefore, it means information of first name, last

name, address, phone number, ID card number, email address, fingerprint, IP. address, Cookie, etc. of the general public and do not protect corporate information.

2) Personal data subject must consent first. Collection of personal data for collection, usage, or disclosure must be collected directly from the data subject and with the direct consent of the data subject in writing or online in a specified format. Therefore, before obtaining consent, the owner of the data must read the information carefully and collect information that they have consented to collect, usage, disclose information with what departments (Olivares, 2019).
3) Provide clear and complete details. The data collector must clearly communicate the purpose of the data collection, usage of the data, disclosure of the data, and the period to the subject matter clearly. Importantly, the information subject information to obtain the consent of the data subject must be clearly separated from the other text, easy to read for the data subject to understand, and understand before consent to data collection (Cieh, 2013).
4) The absolute right person is the owner of the information. The personal information provided is that the data subject can de-collect, use, correct, and delete information from the system which the collector cannot deny (Purtova, 2018). Therefore, the data collector must arrange for the cancellation as convenient as accepting. This protection includes personal information submitted for a job application. Applicants can request the company to send back or destroy personal information such as copies of ID cards, house registration copies, photographs, and educational documents after application to prevent these is sensitive personal information from being leaked.
5) The collector must keep the information safe and confidential. The collector of personal information must have a duty to maintain data security without altering it by anyone who does not the owner of the data or access it illegally, and ensure that it is not lost (Hui, 2015). In this regard, the operator or organization that collects the data must have the system, method, working group, and the responsible team, etc., to keep the information as secure as possible. If information is leaked or stolen, the data collector must notify the data subject within 72 hours of the incident.
6) Covers people who collect - use - disclose information both in and outside the country. The Personal Data Act applies to the collection, usage, or disclosure of personal information by domestic organizations or operators whether data collection, usage, or disclosure takes place in the country or outside the country (Rich, 2014). If the people who collect - use - disclose information outside the country, they will be controlled when having availability of goods or services and the monitoring of the behavior of the data subject in Thailand.
7) Personal Data Protection Officers can use outsource. The Personal Data Protection Officers, who are responsible for providing practical advice, verifying correct operations, coordinating when in trouble, and maintaining confidentiality, can be employees of the organizations or service contractors according to the contract.
8) Violators are punished with imprisonment and fined up to 5 million baht. If people are violated, there are criminal, civil, and administrative penalties. For criminal penalties, violators are imprisoned for a term of not more than 6 months to 1 year or a fine of not more than 500,000 to 1,000,000 baht or both. As for the punishment, an administrative fine is not more than 500,000 to 5,000,000 baht.

Some innovations involving personal information are to help organizations comply with the Personal Data Act, in both structured and unstructured forms completely. The main guidelines are divided into 3 areas: Identity and Access Management, Information Protection, Threat Protection.

Every entrepreneur is affected by modifying or transforming their ways of working to use digital technology. The more an operator has to use digital data, the more it poses a management issue with regards to the information they use, especially managing the risks of using multiple and personal information. Operators must be able to identify and manage information on a risk basis appropriately. Therefore, this guideline is the most basic process for the handling of personal information in other areas.

Personal information that was easily captured in the digital world made it possible for many users to be concerned about the security of their own data (Gomatam, Karr, Reiter, & Sanil, 2005) that it will be externalized or another used. To enhance the protection of such information, the Personal Data Protection Act of 2019. The data collector department must clarify the information and purpose for which it is collected, and only obtain permission or consent from the data subject to access and use the owner's data. The data collector must maintain the security and stability of the information so that it cannot be altered, modified or

accessed by unrelated persons. The data subject can revoke the data collector's access rights and can request deletion or destruction of the data at any time.

The government has appointed an agency that oversees Law compliance in accordance with the Personal Data Protection Act of 2019 as follows: 1. The Office of the Personal Data Protection Committee (PDPC) has a duty to prepare a master plan, set measures for the collection, use, and disclosure of information and educate the public, private and the general public. 2. A panel of experts will consider complaints, investigate, and mediate disputes and to be consistent with the Personal Data Protection Act B.E. 2562.

Guideline on Duties and Responsibilities of Controllers and Processors

This section describes the duties and responsibilities of the data controller and the data processor, comprising five sub-sections:

1) Guidelines on general rights and duties of data controllers and processors.
2) Guidelines for establishing Data Processing Agreement between the data controller and the data processor.
3) Guidelines for handling data subject requests
4) Guidelines on handling government requests from or government officials.
5) Civil, criminal, and governing liability under the Personal Data Protection Law, the operator must state that you are the data controller or is a data processor, considering that you determine the possibility of the personal information. This is said that is it possible to define the purpose, method and handling of personal information?

Guideline on Lawful Basis for Processing Personal Data

Data processing can only take place when there is a basis for justification for such data processing, whether it is collection, use, dissemination, and storage. In each data processing, the data controller must specify a processing base, notify the owner of the processing base, act on that data according to the different limitations of each base, and keep a record of which bases are used to process each data set. Article 24 of the Personal Data Protection Act states that consent is the basis for data processing, where consent is a very important base because it allows the data subject to “choose” to manage their own data completely.

CONCLUSION

From innovation to support personal information because it is a new law that Thailand has to implement in order to comply with the law. Both the public and private sectors have to adapt to create innovation for agencies and beneficiaries, both citizens, businesses, and the public sector. The public sector will be assured that personal information is kept in a safe and appropriate manner, will be used or disseminated within the scope of the stated early objectives that minimize the damage and harm caused by personal data breach, have the right to expressly acknowledge the purpose of collecting, using or distributing personal information, to allow or not to allow or withdraw consent to the collection, use or dissemination of personal information request access, obtain a copy or request disclosure of personal data acquisition, request deletion, destruction, or request for suspension of the use of personal information, and can file a complaint and request for compensation, if personal information is found to be used outside of the stated purpose. Business sectors increase confidence in international standards for the collection, use, or dissemination of personal information, increase the capacity and opportunity of conducting business in which personal information is shared with foreign countries, have appropriate mechanisms for the protection of personal data of the organization, the data subject consents to the collection, use or dissemination of personal information for its purposes, promote corporate governance, and the processing of personal information is transparent, verifiable, and responsible

for social. In the government sector, it will be equal to international law and regulations in the protection of personal data, have regulatory measures, including effective personal data protection governance tools, good governance, personal information protection operations are transparent and verifiable, building a strong society because government and business operations on the protection of personal information can be properly examined.

REFERENCES

Aserkar, R., Seetharaman, A., Chu, J.A.M., Jadhav, V., & Inamdar, S. (2017). Impact of Personal Data Protection (PDP) regulations on operations workflow. *Human Systems Management, 36*(1), 41-56.

Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. The John Marshall, *Journal of Information Technology & Privacy Law, 18*(1).

Bhasin, M.L. (2016). Privacy protection legislative scenario in select countries. *International Journal of Social Science and Business, 1*(2), 1-18.

Cieh, E.L.Y. (2013). *Personal data protection act 2010: An overview analysis*. In Beyond Data Protection, 31-64. Berlin, Heidelberg: Springer.

Carpenter, C. (2020). Privacy and proportionality: Examining mass electronic surveillance under article 8 and the fourth amendment. *International and Comparative Law Review, 20*(1), 27-57.

Decker, S., & Ford, J. (2017). Chapter 13 - *Management of 3D image data*. Editor(s): David Errickson, Tim Thompson, Human Remains: Another Dimension. Academic Press, 185-191.

Determann, L., & Gupta, C. (2019). Indian personal data protection act, 2018: Draft bill and its history, compared to EU GDPR and California Privacy Law. *UC Berkeley Public Law Research Paper*, 1-27.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703-705.

Gomatam, S., Karr, A.F., Reiter, J.P., & Sanil, A.P. (2005). Data dissemination and disclosure limitation in a world without microdata: A risk-utility framework for remote access analysis servers. *Statistical Science, 20*(2), 163-177.

Fondren, E., & McCune, M.M. (2018). Archiving and preserving social media at the library of congress: institutional and cultural challenges to build a Twitter archive. *Preservation, Digital Technology & Culture, 47*(2), 33-44.

Hui, S. (2015). Modern identity protection: A multifaceted response to a surreptitious threat. *Singapore Law Review, 33*, 157-191.

Kuner, C. (2010). *Regulation of transborder data flows under data protection and privacy law: Past, present, and future*. TILT Law & Technology Working Paper No. 016. Tilburg Law School.

Lachaud, E. (2018). The general data protection regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review, 34*(2), 244-256.

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., … & Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review, 33*(4), 458-469.

Rozakis, C. (2020, May). The European convention on human rights as a tool of european integration. *European Convention on Human Rights Law Review, 1*(1), 22-24.

Maginnis, M. (2000). Maintaining the privacy of personal information: The DPPA and the right of privacy. *South Carolina Law Review, 51*(4), 8.

Olivares, B.D.O. (2019). The impact of GDPR on European Name & Shame tax defaulter lists. *Computer Law & Security Review, 35*(3), 241-250.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40-81.

Peng, G. (2011). Individual information rights and EU protection.

Regulation, G.D.P.R. (2018). General data protection regulation (GDPR).

Rich, C.Y.N.T.H.I.A. (2014). Privacy and security law report (No. 13). Law Report.

Svantesson, D.J.B. (2015). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law, 5*(4), 226-234.

Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer Law & Security Review, 35*(4), 380-397.

Shahwahid, F.M., & Miskam, S. (2014). Personal data protection Act 2010: Taking the first steps towards compliance. *E-proceedings of the Conference on Management and Muamalah (CoMM)* 2014, 153-163.

Trakman, L., Walters, R., & Zeller, B. (2020). Digital consent and data protection law–Europe and Asia-Pacific experience. *Information & Communications Technology Law, 29*(2), 218-249.

Voigt, P., & Von dem Bussche, A. (2017). *The eu General Data Protection Regulation (GDPR)*. A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10, 3152676.

Zeno-Zencovich, V. (2020). *Free-flow of data*. Is international trade law the appropriate answer?