ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

LEGAL PROBLEMS ON REPORTING OF PERSONAL DATA BREACH ACCORDING TO THE PERSONAL DATA PROTECTION ACT B.E. 2562 (2019)

กนกพร เหลือสาคร

KANOKPORN LUEASAKHON

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต

กลุ่มวิชากฎหมายธุรกิจ

คณะนิติศาสตร์

มหาวิทยาลัยศรีปทุม

พ.ศ. 2566

LEGAL PROBLEMS ON REPORTING OF PERSONAL DATA BREACH ACCORDING TO THE PERSONAL DATA PROTECTION ACT B.E. 2562 (2019)

KANOKPORN LUEASAKHON

A THEMATIC PAPER SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF LAWS

BUSINESS LAW

SCHOOL OF LAW

SRIPATUM UNIVERSITY

2023

สารนิพนธ์เรื่อง	ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
คำสำคัญ	การแจ้งเหตุละเมิด / ข้อมูลส่วนบุคคล
นักศึกษา	กนกพร เหลือสาคร
อาจารย์ที่ปรึกษาสารนิพนธ์	ดร.รุ่งแสง กฤตยพงษ์
หลักสูตร	นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายธุรกิจ
คณะ	นิติศาสตร์ มหาวิทยาลัยศรีปทุม
พ.ศ.	2566

บทคัดย่อ

สารนิพนธ์ฉบับนี้ ได้ศึกษาแนวคิด และทฤษฎีเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง โดยศึกษากฎหมายของประเทศไทย ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา

จากการศึกษาพบว่า มีปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ ปัญหาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด” ซึ่งบทบัญญัติดังกล่าวยังขาดความชัดเจนอยู่มาก เนื่องจากไม่มีการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ต่อมาปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พบว่าการนับระยะเวลา 72 ชั่วโมงนั้น เป็นการบัญญัติกฎหมายที่เคร่งครัดมากเกินไป เนื่องจากหากเป็นกรณีที่เกิดการรั่วไหลของข้อมูลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่เกิดประโยชน์กับผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล สุดท้ายปัญหาบทลงโทษทาง

อาญา เนื่องจากในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล จึงจำเป็นต้องเสนอแนวทางในการเพิ่มเติมกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4) เพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพมากยิ่งขึ้น

ดังนั้น สารนิพนธ์ฉบับนี้ เสนอแนะในประเด็นที่ 1 ว่าให้กำหนดให้ชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4) และกำหนดกว่ากรณีใดบ้างที่ไม่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล ประเด็นที่ 2 เสนอให้แก้ไขจุดเริ่มต้นการนับระยะเวลา 72 ชั่วโมง ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาตรา 37 (4) โดยควรให้เริ่มนับเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นแล้วว่าเป็นกรณีที่ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล ซึ่งจะเหมาะสมกับการบังคับใช้กฎหมายมากกว่า เนื่องจากการกำหนดให้ผู้ประกอบธุรกิจต้องแจ้งเหตุละเมิดดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง จะทำให้เป็นอุปสรรคต่อการดำเนินงานเป็นอย่างมาก และประเด็นที่ 3 เสนอให้ใช้โทษปรับเป็นพินัยแทนบทลงโทษทางอาญา เนื่องจากปัจจุบันประเทศไทยได้มีการตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ขึ้นบังคับใช้ โดยมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก ด้วยเหตุกรณีนี้เป็นเพียงการฝ่าฝืน ไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมในการบังคับใช้กฎหมายมากกว่า และจะช่วยทำให้ประชาชนที่ถูกกล่าวหาว่ากระทำความผิดไม่ต้องเข้าสู่กระบวนการทางอาญา และไม่มีประวัติอาชญากรรมติดตัวอีกต่อไป การเปลี่ยนแปลงเช่นนี้จะเป็นกลไกทางกฎหมายเพื่อสร้างความเป็นธรรมและขจัดความเหลื่อมล้ำทางสังคม และส่งเสริมการบังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น

THEMATIC TITLE	LEGAL PROBLEMS ON REPORTING OF PERSONAL DATA BREACH ACCORDING TO THE PERSONAL DATA PROTECTION ACT B.E. 2562 (2019)
KEYWORDS	REPORTING OF DATA BREACH / PERSONAL DATA
STUDENT	KANOKPORN LUEASAKHON
THEMATIC ADVISOR	DR.RUNGSAENG KITTAYAPONG
LEVEL OF STUDY	MASTER OF LAWS BUSINESS LAW
FACULTY	SCHOOL OF LAW SRIPATUM UNIVERSITY
YEAR	2023

ABSTRACT

This thesis aims to study the Personal Data Protection Act B.E. 2562 (2019) of Thailand and the related laws of other nations, including the European Union, the Republic of Singapore, Japan, and Canada, were studied in order to better understand the concepts and theories regarding personal data breach notifications under such laws.

According to the study, there are some legal problems relating to personal data breach notifications in the provision of Section 37(4) of the Personal Data Protection Act B.E. 2562 (2019) which states that "Notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Persons. If the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Persons, the Data Controller shall also notify the Personal Data breach and the remedial measures to the data subject without delay. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Committee". The instances in which a personal data breach must be reported to the Office of the Personal Data Protection Committee are not explicitly defined. In addition, the 72-hour window for notifying the Office of the Personal Data Protection Committee of a personal data breach is too short because, in the event of a data leak that is not serious or unlikely to affect the data subject, reporting such breach will not be beneficial to both the data controller and the data subject. The final issue found is the issue of criminal penalties because in

the event that the personal data controller violates or does not comply with the Personal Data Protection Act B.E. 2562 (2019), for instance, violations involving sensitive personal data in a manner that is likely to cause harm, loss of reputation, disparagement, hatred, or embarrassment. Given that the purpose of the Act is to protect the rights of data subjects, the criminal penalties outlined in it are inappropriate in the context of Thailand. Therefore, in order to increase the effectiveness of law enforcement, it is necessary to provide guidelines for amending provisions relating to personal data breach notification in accordance with Section 37(4) of the Personal Data Protection Act, B.E. 2562 (2019).

Therefore, the researcher suggests that 1) There should be a provision stating which circumstances, as per Section 37(4) of the Personal Data Protection Act B.E. 2562 (2019), a personal data breach notification must be made and which circumstances a personal data breach is not required to be reported to the Office of the Personal Data Protection Committee and the data subject; 2) The start of the 72-hour window in Section 37(4) of the Personal Data Protection Act B.E. 2562 (2019) should be amended. This time frame shall start as soon as the personal data controller decides that notifying the Office of the Personal Data Protection Committee and the data subject of this scenario is required. Since requiring business owners to report such breach to the Office of the Personal Data Protection Committee within 72 hours would significantly hamper their operations, doing so would be more appropriate for law enforcement; and 3) Since Thailand has passed the Regulatory Fines Act B.E. 2565 (2022), which specifies and focuses on punishments in the form of fines rather than imprisonment, the regulatory fines should be used instead of criminal penalties. This is due to the fact that it is only a violation or breach, not a serious crime, and therefore a fine is a more appropriate punishment, keeping the accused out of court and avoiding a criminal record. Such changes and amendments will serve as a legal tool to establish justice, eradicate social inequity, and encourage more effective law enforcement.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สำเร็จลงได้โดยได้รับความกรุณาและความอนุเคราะห์จากผู้ทรงคุณวุฒิหลายท่าน ได้แก่ ท่านผู้ช่วยศาสตราจารย์ ดร.จิดาภา พรยิ่ง ซึ่งรับเป็นประธานกรรมการในการสอบสารนิพนธ์ ท่านอาจารย์ ดร.ศิวพร เสาวคนธ์ กรรมการสอบสารนิพนธ์ และท่านอาจารย์ ดร.รุ่งแสง กฤตยพงษ์ ที่กรุณาเป็นอย่างยิ่งในการรับเป็นอาจารย์ที่ปรึกษาและกรรมการสอบสารนิพนธ์ โดยทุกท่านได้สละเวลาอันมีค่ายิ่งในการให้คำแนะนำ คำปรึกษา ตรวจแก้ไข ตลอดจนให้ข้อคิดเห็นต่าง ๆ จนทำให้สารนิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี ผู้วิจัยรู้สึกสำนึกในความกรุณาและขอกราบขอบพระคุณท่านอาจารย์ทุกท่านเป็นอย่างสูง

ผู้วิจัยขอขอบพระคุณบิดามารดาผู้ให้กำเนิดที่ส่งเสริมในการศึกษา และให้กำลังใจในการทำสารนิพนธ์ตั้งแต่ต้นจนกระทั่งประสบความสำเร็จ และขอขอบพระคุณครูบาอาจารย์ทุกท่านในระดับปริญญาโทที่ได้ประสิทธิประสาทวิชาแก่ผู้วิจัย ซึ่งเป็นประโยชน์อย่างยิ่งในการจัดทำสารนิพนธ์

ความดีของสารนิพนธ์ฉบับนี้หากจะพึงมีผู้วิจัยขออุทิศคุณความดีแด่บิดา มารดาผู้ให้กำเนิด ให้การเลี้ยงดู อบรมสั่งสอน ตลอดจนให้การศึกษา และพระคุณของคณาจารย์ผู้ประสิทธิ์ประสาทวิชาความรู้ทุกท่าน ซึ่งได้กรุณาถ่ายทอดความรู้จนนำมาใช้ในการศึกษาและทำให้สารนิพนธ์ฉบับนี้สำเร็จสมความปรารถนา

กนกพร เหลือสาคร
มหาวิทยาลัยศรีปทุม
2566

สารบัญ

บทที่ **หน้า**

บทที่ **หน้า**

สารบัญตาราง

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ถือว่ามีผลกระทบต่อภาคธุรกิจและภาคอุตสาหกรรมหลายๆ ภาคส่วนด้วยกัน ไม่ว่าจะเป็นหน่วยงานภาครัฐหรือหน่วยงานภาคเอกชน และเป็นเวลากว่า 20 ปีที่รัฐบาลไทยได้พยายามผลักดันกฎหมายการคุ้มครองข้อมูลส่วนบุคคลจนประสบความสำเร็จและประกาศในราชกิจจานุเบกษาเมื่อ 28 พฤษภาคม 2562 และมีผลบังคับใช้ตามกฎหมายในวันที่ 1 มิถุนายน 2565 โดยได้รับอิทธิพลสำคัญจาก General Data Protection Regulation หรือ (GDPR) หน่วยงานภาครัฐและเอกชนจึงควรเตรียมความพร้อมเพื่อรองรับการจัดการข้อมูลส่วนบุคคลในความครอบครองของตนเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว ซึ่งปัจจุบันถือว่าเป็นมาตรฐานใหม่ของการคุ้มครองข้อมูลส่วนบุคคลของโลก

เนื่องจากประเทศไทยยังขาดความพร้อมในการปฏิบัติตามกฎหมายอย่างเต็มรูปแบบ อีกทั้ง บทบัญญัติบางมาตราในพระราชบัญญัตินี้ ยังขาดความชัดเจนและเป็นอุปสรรคต่อผู้ประกอบธุรกิจของประเทศไทยในหลายประการ อาทิ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล หรือ Data Breach Notification ซึ่งถือเป็นหน้าที่ตามกฎหมายที่สำคัญของ ผู้ควบคุมข้อมูลส่วนบุคคลในทุก ๆ ประเทศ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้วางหลักในเรื่องการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลไว้ในทิศทางเดียวกันกับกฎหมายของสหภาพยุโรป General data Protection Regulation หรือ (GDPR)

กล่าวคือ หากเกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น ผู้ประการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนับแต่ทราบถึงเหตุการณ์ดังกล่าวโดยไม่ชักช้าและภายใน 72 ชั่วโมงนับแต่ทราบเหตุดังกล่าว ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดกรณีการแจ้ง (สำหรับกรณีที่ต้องแจ้ง) ถึงเหตุการละเมิดข้อมูลส่วนบุคคลไว้เป็น 2 กรณีคือ หากเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลผู้ควบคุมข้อมูล ต้องแจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ และ หากเป็นเหตุการละเมิดข้อมูล

ส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งถึงเหตุการณ์ดังกล่าวไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลพร้อมทั้งแนวทางการเยียวยาภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

ทั้งนี้ กฎหมายไม่ได้จำกัดเฉพาะสิทธิในความเป็นส่วนตัวของข้อมูลส่วนบุคคลเท่านั้น แต่เป็นการชั่งน้ำหนักต่อสิทธิและเสรีภาพอื่น ๆ ของเจ้าของข้อมูลส่วนบุคคลด้วย แม้ในยุคของเทคโนโลยีสารสนเทศและการสื่อสาร จะมีการมาตรการด้านความมั่นคงปลอดภัยที่ดีเหตุการละเมิดข้อมูลส่วนบุคคลไม่ว่าจะจากการโจมตีหรือข้อผิดพลาดทางเทคนิคก็มีโอกาสเกิดขึ้นได้เสมอ การรายงานหรือแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอย่างรวดเร็วภายใต้เงื่อนไขและกรอบระยะเวลาที่กฎหมายกำหนด เพื่อที่สำนักงานจะได้ดำเนินการตอบสนองต่อเหตุการณ์ดังกล่าวอย่างทันท่วงที จึงเป็นเรื่องสำคัญยิ่งที่จะสามารถช่วยป้องกันและลดโอกาสเกิดความเสียหายแก่ผู้บริโภคที่อาจจะเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคลได้[1]

ทั้งนี้ โทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แบ่งออกเป็น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความ อับอาย และการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย เพื่อแสวงหาประโยชน์ที่ไม่ชอบด้วยกฎหมาย ยกเว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐ ในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ[2] ซึ่งมีโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ[3]

1) ปัญหาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)[4] “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อ สิทธิ

---

[1] กรุงเทพธุรกิจ. (2564). ***การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/blogs/columnist/127256 [2566, 30 มิถุนายน]

[2] วารุณี เอื้อไตรรัตน์. (2564). ***พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) หากไม่ปฏิบัติตามจะมีผลอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://www.cyfence.com/article/what-are-the-consequences-of-not-being-compliant-with-pdpa/ [2566,7 กรกฎาคม]

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

และเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด" พบว่าปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจนอยู่มาก เนื่องจากไม่มีการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลส่วนบุคคล รวมถึงไม่มีการกำหนดข้อยกเว้นว่าหากเป็นการเข้าถึง เก็บ ใช้ เปิดเผย คัดลอก หรือแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตภายในองค์กร ไม่ให้ถือว่าเป็นการรั่วไหลที่ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลด้วย

2) ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พบว่า การนับระยะเวลา 72 ชั่วโมง ควรให้เริ่มนับเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นแล้วว่าเป็นกรณีที่ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และ/หรือ เจ้าของข้อมูลส่วนบุคคลหรือไม่ หากกรณีที่การรั่วไหลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่เกิดประโยชน์ทั้งกับเจ้าของข้อมูลส่วนบุคคล

3) ปัญหาบทลงโทษทางอาญา เนื่องจากในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวไม่ใช่การก่ออาชญากรรมที่ต้องมีโทษทางอาญา การกำหนดโทษทางอาญาไว้ในพระราชบัญญัติฯ นี้ โดยเฉพาะโทษจำคุกนั้น จึงมีความรุนแรงเกินความจำเป็น อีกทั้ง อาจถูกใช้เป็นช่องทางหรือเครื่องมือของผู้แสวงหาผลประโยชน์ได้ จึงควรยกเลิกโทษอาญา เนื่องจากปัจจุบันประเทศไทยได้มีการตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ซึ่งมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก เนื่องจากกรณีนี้เป็นเพียงการฝ่าฝืน ไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมกว่าในการบังคับใช้กฎหมายมากกว่า

ดังนั้น ผู้วิจัยจึงมีความประสงค์ที่จะศึกษาหลักกฎหมาย กฎเกณฑ์ แนวคิด ทฤษฎี ของประเทศไทย และของต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และ

ประเทศแคนาดา ว่าปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีความเหมาะสมมากน้อยเพียงใดต่อการบังคับใช้ และสมควรแก้ไข หรือปรับปรุงกฎหมายในส่วนของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลหรือไม่ ตลอดจนการเสนอแนวทางแก้ไขกฎหมาย เพื่อให้เหมาะสมกับบริบทของประเทศไทยได้

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาประวัติความเป็นมา แนวคิด ทฤษฎี ของปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทยและต่างประเทศ

2. เพื่อศึกษามาตรการทางกฎหมายและหลักเกณฑ์ของปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทยและต่างประเทศ

3. เพื่อศึกษาและวิเคราะห์ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย

4. เพื่อเสนอแนวทางแก้ไขปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย

1.3 สมมติฐานของการศึกษา

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล มาตรา 37(4) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในปัจจุบันยังขาดความชัดเจนและเป็นอุปสรรคต่อผู้ประกอบธุรกิจของประเทศไทยและประชาชนทั่วไปในหลายประการ อาทิ ในกรณีที่การรั่วไหลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงาน เนื่องจากไม่เกิดประโยชน์ทั้งกับเจ้าของข้อมูลส่วนบุคคลและผู้ประกอบธุรกิจ นอกจากนี้ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจต้องให้ความสำคัญกับการรวบรวมข้อเท็จจริงจัดการแก้ปัญหาเบื้องต้นและระงับเหตุเป็นอันดับแรก การกำหนดให้ผู้ประกอบธุรกิจต้องแจ้งเหตุละเมิดดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สคส.) ทราบภายใน 72 ชั่วโมง จะทำให้เป็นอุปสรรคต่อการดำเนินการข้างต้น ด้วยเหตุนี้ จึงจำเป็นต้องเสนอแนวทางในการเพิ่มเติมกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพมากยิ่งขึ้น

1.4 ขอบเขตของการศึกษา

การศึกษานี้มุ่งศึกษาถึงปัญหากฎหมายในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงศึกษาหลักเกณฑ์และมาตรการทางกฎหมายเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลทั้งกฎหมายภายในประเทศและต่างประเทศ อาทิ กฎหมายของสหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา เป็นต้น เพื่อนำมาวิเคราะห์เปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย เพื่อให้ทราบถึงประวัติความเป็นมา ความหมาย แนวคิด และทฤษฎีเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ทั้งทางทฤษฎีและทางปฏิบัติ ในการวิเคราะห์ปัญหาดังกล่าว เพื่อนำมาแก้ไขปัญหาและพัฒนากฎหมายของประเทศไทยต่อไป

1.5 วิธีดำเนินการศึกษา

สารนิพนธ์ฉบับนี้ได้ดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) โดยศึกษาจากตำรา บทความทางวิชาการ วิทยานิพนธ์ งานวิจัย ตัวบทกฎหมาย การศึกษาข้อมูลจากกฎหมายของต่างประเทศ ตลอดจนคำพิพากษาของศาลในต่างประเทศ รวมทั้งการค้นคว้าจากอินเทอร์เน็ต เพื่อนำมาวิเคราะห์ถึงสภาพปัญหา พร้อมเสนอแนวทางการแก้ไขหลักเกณฑ์ต่าง ๆ ตามกฎหมายที่ยังมีปัญหาอยู่

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบประวัติความเป็นมา แนวคิด ทฤษฎี ของปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทยและต่างประเทศ

2. ทำให้ทราบมาตรการทางกฎหมายและหลักเกณฑ์ของปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทยและต่างประเทศ

3. ทำให้ทราบปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย

4. ทำให้ทราบถึงแนวทางการแก้ไขปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย

บทที่ 2

ประวัติความเป็นมา ความหมาย และแนวคิดเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคล ถือเป็นกฎหมายใหม่ที่สำคัญสำหรับประเทศไทยเป็นอย่างมาก แต่เนื่องด้วยปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อน หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม จึงกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้นมา โดยมีประวัติความเป็นมา ความหมาย และแนวคิด ที่เกี่ยวข้อง ดังต่อไปนี้

2.1 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีฐานะเป็นกฎหมายกลางกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิติ ซึ่งได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ[1]

2.1.1 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในอดีต

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐานประเภทหนึ่งที่นานาประเทศให้ความสำคัญ ซึ่งคำว่า “สิทธิมนุษยชน” หมายถึง สิทธิขั้นพื้นฐาน เป็นมาตรฐานขั้นพื้นฐานที่พึงมี เป็นสิ่งจำเป็นในการดำรงชีวิตอย่างมีศักดิ์ศรีและมีคุณค่า หากมีการล่วงละเมิดต่อสิทธิดังกล่าวย่อมได้รับการรับรองและคุ้มครองโดยกฎหมาย สิทธิมนุษยชนในสมัยโบราณถูกกำหนดขึ้นเพื่อจำกัดสิทธิการใช้อำนาจรัฐแทรกแซงสิทธิของบุคคลอันเป็นที่มา

---

[1] นพดล นิ่มหนู. (2565). หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. ***วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม***, 41(3). หน้า 51.

ของความเชื่อเรื่องปัจเจกชนนิยม (Individualism) โดยให้คำอธิบายว่า กฎหมายธรรมชาติที่รับรองสิทธิมนุษยชนเป็นกฎหมายศักดิ์สิทธิที่พระเจ้าประทานให้มนุษย์ และ เป็นกฎหมายที่มีอำนาจสูงสุด รัฐจะตรากฎหมายที่ขัดแย้งกฎหมายธรรมชาติไม่ได้ แม้ว่าต่อมาสังคมให้ความสำคัญกับหลักเหตุผลมากกว่าความเชื่อเรื่องสิ่งศักดิ์สิทธิและพระเจ้า กฎหมายธรรมชาติยังได้รับการยอมรับในฐานะกฎของเหตุผลในทางโลกที่มีขึ้นเพื่อปกป้องสิทธิและผลประโยชน์ของบุคคล[2]

Thomas Hobbs กล่าวในหนังสือ Leviathan ไว้ว่า “ในสภาวะที่ยังไม่มีสังคมมนุษย์มีชีวิตอยู่ในธรรมชาติด้วยความหวาดกลัว เห็นแก่ตัวและชอบใช้ความรุนแรง เป็นสภาวะของอนาธิปไตย ด้วยความจำเป็นเพื่อหลีกหนีจากสภาวะอันเลวร้าย มนุษย์จึงรวมตัวกันขึ้นเป็นสังคม และทำความตกลงมอบสิทธิตามธรรมชาติของตนบางส่วนให้กับรัฐควบคุมดูแล เพื่อไม่ให้เกิดสภาวะที่เป็นอนาธิปไตยได้อีก” เช่นเดียวกับ John Locke (1690 cited in Davidson, 1982) กล่าวไว้ในหนังสือ The Second Treaties of Government ไว้ว่า “มนุษย์ ในสภาวะธรรมชาตินั้นเป็นสภาวะแห่งสันติสุข ต่างช่วยเหลือเกื้อกูลกัน มีความเสมอภาคและเป็นอิสระ มีสิทธิที่สำคัญ 3 ประการ คือ สิทธิในชีวิต อิสรภาพ และทรัพย์สิน ภายใต้การควบคุมของกฎแห่งธรรมชาติ การล่วงละเมิดสิทธิที่มนุษย์มีอยู่ตามธรรมชาติจะถูกลงโทษโดยการแก้แค้น ทดแทน จากผู้เสียหายหรือญาติมิตรของผู้เสียหาย” ซึ่ง Locke เรียกว่า “ความยุติธรรมส่วนตัว” (Private Justice) เมื่อมนุษย์มาอยู่รวมกันเป็นสังคมและยินยอมอยู่ใต้อำนาจรัฐซึ่งรับมอบหมายให้ปกป้องคุ้มครองสิทธิในชีวิต เสรีภาพ และทรัพย์สิน มนุษย์จำต้องสละสิทธิตามธรรมชาติบางส่วน ของตนเพื่อให้สังคมเกิดความสงบสุขและคงสิทธิธรรมชาติอื่นไว้ได้ หากรัฐใช้อำนาจละเมิดสิทธิของประชาชนเกินกว่าสิทธิที่ได้รับมอบหมายแล้ว ประชาชนก็มีสิทธิโดยชอบธรรมที่จะล้มล้างรัฐบาล และจัดตั้งรัฐบาลขึ้นใหม่ได้[3]

โดยการคุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นอยู่ส่วนตัวนั้น ย่อมหมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นถือได้ว่าเป็นความส่วนตัว

---

[2] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[3] พงษ์เทพ สันติกุล. (2562). สิทธิมนุษยชน สิทธิพลเมือง และสิทธิทางสังคม. ***วารสารการเมือง การบริหาร และกฎหมาย***, 11(1). หน้า 37-60.

เกี่ยวกับข้อมูล โดยสิทธิความเป็นส่วนตัวมีการรับรองไว้อย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนข้อ 12[4] ก็ได้บัญญัติให้ความคุ้มครองรับรองสิทธิความเป็นอยู่ส่วนตัวไว้เช่นกัน

ในสังคมยุคปัจจุบัน บรรดาความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นเรื่องที่ประเทศส่วนใหญ่ให้ความสำคัญเป็นอย่างมาก ทั้งนี้ เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว การรับรู้ข้อมูลข่าวสารต่างๆ เป็นเรื่องที่สะดวกสบายมากขึ้น เมื่ออินเทอร์เน็ตได้เข้ามาเป็นสื่อที่มีบทบาทสำคัญในการติดต่อ สื่อสารระหว่างกันและเป็นสื่อที่ได้รับความนิยมอย่างแพร่หลาย ทำให้แทบทุกกิจกรรมที่เกิดขึ้น ล้วนแต่มีความเกี่ยวข้องกับอินเทอร์เน็ตทั้งสิ้น ส่งผลให้ธุรกิจและธุรกรรมต่างๆ บนอินเทอร์เน็ต เกิดขึ้นมากมาย ในแต่ละวันข้อมูลนับล้านถูกส่งผ่านเครือข่าย เพื่ออำนวยความสะดวกให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ อย่างไรก็ตาม ในทางกลับกันเมื่อข้อมูลต่างๆ สามารถเข้าถึงได้ง่าย จึงอาจมีการนำข้อมูลเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่น โดยอาจทำให้เกิดความเสียหายหรือสูญหายของข้อมูล หรืออาจถูกนำข้อมูลไปใช้ในทางที่ผิด ไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตาม[5]

2.1.2 ประวัติความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

สำหรับประเทศไทยซึ่งเป็นสมาชิกขององค์กรสหประชาชาติ ได้ให้การรับรองและคุ้มครองในเรื่องข้อมูลส่วนบุคคลไว้เช่นเดียวกัน โดยบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยทั้งในฉบับก่อน คือ ฉบับปี พ.ศ. 2550 ในมาตรา 35 วรรคสาม[6] และตามรัฐธรรมนูญฉบับ

---

[4] มาตรา 12 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น

[5] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[6] มาตรา 35 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ

ปัจจุบัน คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 หมวด 3 สิทธิเสรีภาพของปวงชนชาวไทย มาตรา 32[7]

ซึ่งก่อนที่จะมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562ภาครัฐได้มีความพยายามที่จะจัดให้มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเป็นระยะเวลานานกว่า 10 ปี โดยเล็งเห็นถึงความก้าวหน้าทางเทคโนโลยี การคุ้มครองความเป็นส่วนตัว และแนวโน้มการละเมิดสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวที่เพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปเปิดเผยโดยมิชอบหรือเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลเพื่อแสวงหาประโยชน์ต่าง ๆ จึงมีการศึกษาและร่างกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น

ต่อมาประเทศไทยได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น โดยมีเหตุผลที่ประกาศใช้พระราชบัญญัติดังกล่าว คือ เนื่องจากประเทศไทยมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ซึ่งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม ประเทศไทยจึงได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูล ส่วนบุคคลที่เป็นหลักการทั่วไป[8]

---

[7] มาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศชื่อเสียงและครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่งหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

[8] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

2.2 ความหมายของข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้นิยามความหมายของข้อมูลส่วนบุคคล ไว้ว่า “ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่จะไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรมโดยเฉพาะ[9]”

คำนิยามข้างต้น แสดงให้เห็นได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับกับข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลธรรมดาคนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม และไม่ใช้บังคับกับข้อมูลที่สามารถระบุไปยังตัวนิติบุคคลได้

นอกจากนี้แล้วคำนิยามของคำว่า “ข้อมูลส่วนบุคคล”[10] ยังกำหนดกรณีที่เป็นข้อมูลของบุคคลธรรมดาแต่ไม่ถือว่าเป็นข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ด้วย กล่าวคือ ข้อมูลของผู้ที่ถึงแก่ความตายแล้ว จะไม่ถือว่าเป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ ดังนั้น การประมวลผลข้อมูลส่วนบุคคลของผู้ที่ถึงแก่ความตายจึงสามารถกระทำได้โดยไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จากนิยามข้างต้นสามารถสรุปได้ว่า “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือข้อมูลที่มีลักษณะหรือองค์ประกอบ ดังนี้

1) เป็นข้อมูลของบุคคลธรรมดา (Natural Person)

2) เจ้าของข้อมูลส่วนบุคคลยังไม่ถึงแก่ความตาย

3) ข้อมูลนั้นสามารถระบุตัวบุคคลได้ไม่ว่าทางตรง หรือทางอ้อม

ดังนั้น ข้อมูลใดที่ไม่มีลักษณะ 3 ประการดังที่ระบุข้างต้น ข้อมูลนั้นไม่จัดเป็น “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การประมวลผลข้อมูลดังกล่าวจึงไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โดยมีข้อสังเกตในการพิจารณาข้อมูลส่วนบุคคล[11] ดังนี้

---

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 วรรคหนึ่ง.

[10] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6 วรรคหนึ่ง.

[11] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

1) การจะพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลหรือไม่นั้น ต้องพิจารณาถึงสภาพของข้อมูลส่วนบุคคลและบริบทของการประมวลผลข้อมูลส่วนบุคคลด้วย กล่าวคือ ข้อมูลบางอย่างหากถูกเก็บรวบรวมไว้แยกจากข้อมูลอื่น ๆ ก็จะไม่สามารถระบุตัวบุคคลได้ แต่หากรวมกับข้อมูลอื่น ๆ จะทำให้สามารถระบุตัวบุคคลได้ไม่ว่าจะทางตรงหรือทางอ้อม เช่น อายุ เพศ ศาสนา อาชีพ หากองค์กรใดแยกเก็บข้อมูลส่วนบุคคลเหล่านี้เป็นชุดข้อมูลเดี่ยว ๆ ข้อมูลเหล่านี้ก็จะไม่สามารถระบุตัวบุคคลได้

2) ข้อมูลที่เกี่ยวกับนิติบุคคลบางกรณีอาจเป็น "ข้อมูลส่วนบุคคล" ได้ เช่น หนังสือรับรองบริษัทที่มีรายชื่อกรรมการบริษัทหรือรายชื่อผู้ถือหุ้นบริษัท

3) ประเภทของข้อมูลส่วนบุคคลที่จะถูกจัดเก็บหรือประมวลผลนั้น เป็นไปตามความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

ทั้งนี้ ข้อมูลส่วนบุคคลบางประเภท เป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีการกำหนดข้อมูลส่วนบุคคลไว้อีกประเภทหนึ่ง เรียกว่า "ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)" โดยที่ มาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดว่า ข้อมูลอันเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ รวมถึงข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการกำหนด ถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว[12]

2.3 แนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

แนวความคิดของความเป็นส่วนตัวได้มีการพัฒนามาตลอดตั้งแต่สมัยโบราณ แต่จะมากน้อยขึ้นอยู่กับบริบทของสังคมและวัฒนธรรมในช่วงเวลานั้นๆ พัฒนาการครั้งสำคัญที่เห็นว่ามีความชัดเจนในการพัฒนาแนวความคิดการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวมากที่สุดคือ เมื่อมีการเผยแพร่บทความเรื่อง "The Right to Privacy" โดย ซามูเอล ดี. วอร์เรนที่ 2 (Samuel D. Warren) และ Louis D. Brandeis บทความดังกล่าวเป็นผลสะท้อนของการพัฒนาเทคโนโลยีในช่วงปี ค.ศ.1890 การเกิดขึ้นของโทรเลข โทรศัพท์ แท่นพิมพ์หนังสือที่สามารถพิมพ์หนังสือได้รวดเร็ว และการคิดค้นเครื่องมือเครื่องใช้ใหม่ๆ และการพัฒนาระบบธุรกิจซึ่ง Warren และ Brandeis กล่าวว่า ความก้าวหน้าดังกล่าวนี้ทำให้มีความจำเป็นต้องให้ความคุ้มครองแก่บุคคล เพราะพัฒนาการของ

[12] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 26 วรรคหนึ่ง.

เทคโนโลยีดังกล่าวทำให้เกิดการคุกคามสิทธิประโยชน์ของบุคคลอย่างน่ากลัวในบทความ The Right to Privacy ดังกล่าว Warren และ Brandeis อธิบายถึง “สิทธิในความเป็นส่วนตัว (Privacy)” ว่าหมายถึง “สิทธิที่จะอยู่ตามลำพัง (the right to be let alone)” เป็นการมองสิทธิในความเป็นอยู่ส่วนตัวเป็นสองแง่มุม คือ ความเป็นส่วนตัวในแง่นามธรรม ได้แก่การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ ความรู้สึกนึกคิด ตลอดจนความเชื่อถือศรัทธาในลัทธิศาสนา ส่วนความเป็นส่วนตัวในทางรูปธรรม คือ สิทธิที่จะอยู่โดยลำพังปราศจากการรบกวนและการแทรกแซงจากสังคม การอยู่อย่างสันโดษโดยไม่ติดต่อสัมพันธ์กับสังคม[13]

โดยแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นครั้งแรกในประเทศเยอรมนี โดยกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลฉบับแรก คือ กฎหมายของรัฐ Hessen ซึ่งเป็นกฎหมายที่มีผลบังคับใช้ในระดับรัฐบัญญัติขึ้นในปี ค.ศ. 1970 และต่อมาในปี ค.ศ. 1977 ประเทศเยอรมนีได้บังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับสหพันธรัฐ (Federal Act on Data Protection)(Library of Congress, 2018) และต่อมาประเทศอื่นๆ ก็ได้มีการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ประเทศฝรั่งเศส[14] ประเทศสหรัฐอเมริกา[15] นอกจากนี้ประเทศในกลุ่มประชาคมอาเซียน (ASEAN) เช่น ประเทศมาเลเซีย[16] สาธารณรัฐสิงคโปร์ [17] ประเทศฟิลิปปินส์[18] ต่างก็มีกฎหมายซึ่งให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ

ในปี ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ คือ Directive95/46/EC ขึ้นมาบังคับใช้ในกลุ่มประเทศสมาชิกของสหภาพยุโรป โดยเป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูลต่อมาในปี ค.ศ. 2016 รัฐสภาแห่งยุโรปได้ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ คือ EU General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้แล้วเมื่อปี ค.ศ. 2018 โดยเป็นกฎหมายที่มีสาระสำคัญเกี่ยวกับการคุ้มครองสิทธิของประชาชนในกลุ่มประเทศสมาชิกสหภาพยุโรปเกี่ยวกับข้อมูลส่วนบุคคลและความเป็นส่วนตัว

---

[13] สุขวสา ถมังรักษ์สัตว์. (2562). การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์. ***วารสารเกษมบัณฑิต,*** 20(1). หน้า 131-145.

[14] Act No. 78-17 of 6 January 1978 on information Technology, Data Files and Civil Liberties

[15] การคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาไม่ได้อยู่ในรูปแบบของกฎหมายซึ่งให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แต่จะเป็นการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายในเรื่องอื่น เช่น ในกฎหมายระดับสาธารณรัฐ การคุ้มครองข้อมูลส่วนบุคคลจะเป็นไปตามบทบัญญัติของ Federal Trade Commission Act หรือการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของสถาบันการเงิน คือ Gramm Leach Bliley Act เป็นต้น

[16] Personal Data Protection Act 2010 (PDPA)

[17] Personal Data Protection Act 2012 (No. 26 of 2012)

[18] Data Privacy Act of 2012 (Republic Act No. 10173)

โดยมีหลักเกณฑ์เกี่ยวกับการใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) คือ ให้ความคุ้มครองต่อข้อมูลส่วนบุคคลของประชาชนในกลุ่มประเทศสหภาพยุโรปไม่ว่าข้อมูลนั้นจะถูกรวบรวมหรือประมวลผลในพื้นที่ใดในโลก กำหนดบทลงโทษแก่ผู้ที่ก่อให้เกิดความเสียหายหรือทำให้ข้อมูลส่วนบุคคลรั่วไหล โดยต้องโทษปรับ 20 ล้านยูโร หรือปรับไม่เกินร้อยละ 4 ของรายได้ทั่วโลกของกิจการนั้น ขึ้นอยู่กับว่าจำนวนใดมากกว่า รวมทั้งกำหนดหลักเกณฑ์เกี่ยวกับการให้ความยินยอมของเจ้าของข้อมูลและการยกเลิกการให้ความยินยอม (European Commission, 2018)[19]

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-operation and Development หรือ OECD) ซึ่งเป็นองค์การระหว่างประเทศได้จัดทำ Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ซึ่งกำหนดหลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้ (OECD, 2013)

1) หลักการจัดเก็บรวบรวมข้อมูลส่วนบุคคลโดยจำกัด (Collection Limitation Principle) หมายถึง การจัดเก็บข้อมูลส่วนบุคคลต้องเป็นไปโดยจำกัด และต้องใช้วิธีการโดยชอบด้วยกฎหมายและเป็นธรรม โดยเจตนาของข้อมูลส่วนบุคคลต้องรับรู้และยินยอมให้มีการจัดเก็บข้อมูลส่วนบุคคลนั้น

2) หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพ (Data Quality Principle) หมายถึง ข้อมูลส่วนบุคคลที่ถูกจัดเก็บรวบรวมต้องเกี่ยวข้องกับวัตถุประสงค์ของการจัดเก็บข้อมูลนั้น และข้อมูลส่วนบุคคลนั้นต้องถูกต้อง สมบูรณ์ และปรับปรุงให้เป็นปัจจุบันเสมอ

3) หลักการระบุวัตถุประสงค์ (Purpose Specification Principle) หมายถึง การจัดเก็บรวบรวมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์แห่งการจัดเก็บนั้นก่อน หรือในเวลาที่ทำการจัดเก็บข้อมูล และการใช้ข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปตามวัตถุประสงค์ดังกล่าวเท่านั้น หากวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคลเปลี่ยนแปลง วัตถุประสงค์ที่เปลี่ยนแปลงไปนั้นจะต้องไม่ขัดหรือแย้งกับวัตถุประสงค์เดิม

4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle) หมายถึง ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผย เข้าถึง หรือใช้สำหรับวัตถุประสงค์เพื่อการอื่นนอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้ตามที่บทบัญญัติของกฎหมายได้กำหนดไว้

5) หลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguards Principle) หมายถึง ข้อมูลส่วนบุคคลจะต้องถูกปกป้องรักษาโดยใช้วิธีการรักษาความปลอดภัยที่

---

[19] ตวงพร ปิยวิทย์. (2564). กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศ***ไทย. วารสารวิชาการ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏนครราชสีมา***, 1(1). หน้า 83-83.

เหมาะสม โดยต้องป้องกันต่อความเสี่ยงที่ข้อมูลส่วนบุคคลจะสูญหาย ถูกเข้าถึงโดยมิชอบ ถูกทำลาย ถูกใช้ ถูกแก้ไขเปลี่ยนแปลง หรือถูกเปิดเผย

6) หลักความโปร่งใส (Openness Principle) หมายถึง การมีนโยบายเกี่ยวกับความโปร่งใสของ การพัฒนา การปฏิบัติงาน และนโยบายเกี่ยวกับข้อมูลส่วนบุคคลโดยวิธีการนั้น ต้องแสดงให้เห็นถึงการมีอยู่และลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์หลักของการใช้ รวมถึงชื่อและสถานที่ตั้งของผู้ควบคุมข้อมูลส่วนบุคคล

7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle) หมายถึง เจ้าของข้อมูลส่วนบุคคลต้องมีสิทธิดังต่อไปนี้[20]

(1) สิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่ามีข้อมูลส่วนบุคคลของตนเองหรือไม่

(2) สิทธิที่จะติดต่อสื่อสารกับผู้ควบคุมข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสม ปราศจากค่าใช้จ่ายหรือเสียค่าจ่ายโดยน้อยที่สุด โดยวิธีการที่เหมาะสม และโดยรูปแบบที่เจ้าของข้อมูลสามารถเข้าใจได้โดยง่าย

(3) สิทธิที่จะได้รับการชี้แจงในกรณีที่ผู้ควบคุมข้อมูลปฏิเสธไม่ปฏิบัติตามสิทธิทั้ง 2 สิทธิข้างต้น และ มีสิทธิที่จะโต้แย้งการปฏิเสธนั้นได้

(4) สิทธิที่จะโต้แย้งการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลของตน และหากการโต้แย้งสำเร็จ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำลาย แก้ไขให้ถูกต้อง ทำข้อมูลให้สมบูรณ์ หรือแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตน

8) หลักความรับผิดชอบ (Accountability Principle) หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบต่อการปฏิบัติตามมาตรการต่างๆ เพื่อให้เป็นไปตามหลักการพื้นฐานคุ้มครองข้อมูลส่วนบุคคลข้างต้น

อีกทั้ง แนวความคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นแนวความคิดที่มีพัฒนาการมาจากการคุ้มครองสิทธิในความเป็นส่วนตัว (Privacy Right) มีพัฒนาการมาเป็นระยะเวลายาวนานแล้วโดยในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องความเป็นส่วนตัวยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง ในเขตแดนเสมือนเป็นที่พักที่บุคคลไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาส่วนตัว เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องจากคนอื่น แนวความคิดในการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจนและได้รับการยอมรับมากที่สุดเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” หรือ “สิทธิในความเป็นส่วนตัว” ของ Samuel D. Warren และ Louis D. Brandies ที่สะท้อนปัญหา

[20] ตวงพร ปิยวิทย์. อ้างแล้วเชิงอรรถที่ 19. หน้า 83-83.

การคุกคามความเป็นส่วนตัวของปัจเจกบุคคลจากการนำเสนอข่าวของสื่อมวลชน ผู้วิจัยอธิบายว่าสิทธิในความเป็นส่วนตัวหมายถึง สิทธิที่จะอยู่โดยลำพัง (Right to be let alone) นอกจากนี้ยังกล่าวด้วยว่าสิทธิในความเป็นส่วนตัวของบุคคลย่อมหมดไปเมื่อบุคคลนั้นเปิดเผยข้อมูลของตนเองสู่สาธารณะหรือด้วยความยินยอมของเจ้าของข้อมูลเองบทความดังกล่าวมีอิทธิพลต่อกฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวในบริบทของกฎหมายละเมิดของสหรัฐอเมริกาเป็นอย่างมาก รวมทั้งแสดงให้เห็นถึงการขัดกันระหว่างสิทธิในความเป็นส่วนตัวของปัจเจกบุคคลกับเสรีภาพในการแสดงความเห็นของสื่อมวลชนอีกด้วย ส่วนแนวความคิดในการตรากฎหมายเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลเริ่มจากภาคพื้นยุโรปเป็นที่แรก กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกเกิดขึ้นที่รัฐเฮ็สส์ (Hesse) ประเทศสหพันธ์สาธารณรัฐเยอรมนี ในปี 1970 ตามมาด้วยประเทศสวีเดนในปี 1973 ประเทศสหรัฐอเมริกาในปี 1974 และประเทศฝรั่งเศสในปี 1978[21]

2.4 ประเภทของข้อมูลส่วนบุคคล

การให้ความคุ้มครองข้อมูลส่วนบุคคลสามารถแบ่งความคุ้มครองแก่ข้อมูลออกเป็น 2 ประเภทแตกต่างกัน[22] คือ ข้อมูลทั่วไป[23] (Non-Sensitive Data) และข้อมูลประเภทที่มีความอ่อนไหว[24] (Sensitive Data) โดยข้อมูลแต่ละประเภทมีลักษณะดังต่อไปนี้

2.4.1 ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data)

ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data) คือ ข้อมูลเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลซึ่ง สามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ ซึ่งข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งมิได้มีความละเอียดอ่อนจนอาจนำมาสู่ปัญหาต่างๆ ได้จึงทำให้ ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวม เปิดเผย หรือใช้ได้ ทั้งนี้ ภายใต้หลักเกณฑ์ที่กฎหมายกำหนดไว้

ข้อมูลส่วนบุคคลทั่วไป[25] ได้แก่

---

[21] บรรเจิด ภาคาพันธุ์. (2563). ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 13(1). หน้า 120-135.

[22] วันพิชิต ชินตระกูลชัย. (2564). ***ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหวคืออะไร มีกี่ประเภท มีอะไรบ้าง*** ?. (ออนไลน์). เข้าถึงได้จาก: https://openpdpa.org/personal-data-type/. [2566, 30 มิถุนายน]

[23] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 6.

[24] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 26.

[25] บทความสาระ. (2564). ***PDPA คืออะไร? – สรุป PDPA เกี่ยวกับธุรกิจที่คุณควรรู้! ฉบับเข้าใจง่าย ?.*** (ออนไลน์). เข้าถึงได้จาก: https://easypdpa.com/article/easypdpa-summary-what-is-pdpa [2566,9 กรกฎาคม]

1) ชื่อ-นามสกุล

2) เบอร์โทรศัพท์ อีเมลส่วนตัว ที่อยู่ปัจจุบัน

3) เลขบัตรประชาชน เลขหนังสือเดินทาง เลขใบอนุญาตขับขี่

4) ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ข้อมูลทางการแพทย์

5) ทะเบียนรถยนต์ โฉนดที่ดิน ทะเบียนบ้าน

6) วันเดือนปีเกิด สัญชาติ น้ำหนักส่วนสูง

2.4.2 ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive data)

ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive data) คือ ข้อมูลของบุคคลซึ่งถือเป็นเรื่องเฉพาะตัวของตัวบุคคล เป็นข้อมูลซึ่งมีความละเอียดอ่อนสูง กล่าวคือ ข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ตามมา เช่น กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไปเป็นข้อมูลที่ก่อให้เกิดความขัดแย้งได้ ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล เป็นต้น โดยข้อมูลประเภทดังกล่าวเจ้าของข้อมูลประสงค์ที่จะเก็บข้อมูลประเภทนี้ไว้เป็นความลับหรือไม่ประสงค์ให้มีการเปิดเผยข้อมูล[26] เช่น

1) เชื้อชาติ เผ่าพันธุ์

2) ความคิดเห็นทางการเมือง

3) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

4) พฤติกรรมทางเพศ

5) ประวัติอาชญากรรม

6) ข้อมูลด้านสุขภาพ ความพิการ เช่น โรคประจำตัว การฉีดวัคซีน ใบรับรองแพทย์

7) ข้อมูลสหภาพแรงงาน

8) ข้อมูลพันธุกรรม

9) ข้อมูลชีวภาพ เช่น ลายนิ้วมือ แบบจำลองใบหน้า ข้อมูลม่านตา

สำหรับหลักเกณฑ์ในการให้ความคุ้มครองต่อข้อมูลทั้งสองประเภทดังกล่าวมีความแตกต่างกัน เนื่องจากการเก็บรวบรวม เปิดเผย หรือใช้ข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) อาจนำมาซึ่งปัญหาต่างๆ ดังที่ได้กล่าวมาแล้ว ดังนั้น ในหลายๆ ประเทศข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) จึงถูกกำหนดให้เป็นข้อมูลที่ห้ามทำการเก็บรวบรวม ใช้

---

[26] วันพิชิต ชินตระกูลชัย. (2564). ***ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหวคืออะไร มีกี่ประเภท มีอะไรบ้าง*** ?. (ออนไลน์). เข้าถึงได้จาก: https://openpdpa.org/personal-data-type/. [2566, 30 มิถุนายน]

หรือเปิดเผยข้อมูลโดยเด็ดขาด เว้นแต่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือเป็นกรณีอื่นตามที่กฎหมายกำหนดไว้ เช่น เป็นการปฏิบัติตามกฎหมาย หรือเป็นการจำเป็นเพื่อการดำเนินคดี เป็นต้น แต่ข้อมูลประเภทข้อมูลทั่วไปนั้น (Non-Sensitive Data) กฎหมายกำหนดให้สามารถทำการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลได้ หากได้รับความยินยอมจากเจ้าของข้อมูล

นอกจากนี้ยังสามารถแบ่งประเภทของข้อมูลส่วนบุคคลในประเด็นเกี่ยวกับความอ่อนไหวที่อาจส่งผลกระทบต่อผู้เป็นเจ้าของข้อมูลส่วนบุคคลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้นได้เป็น 3 ระดับ ดังนี้

1) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับต่ำ (Low-Sensitive) ข้อมูลประเภทนี้เป็นข้อมูลที่ความเกี่ยวข้องกับบุคคลเป็นข้อมูลที่มีความอ่อนไหว เนื่องจากข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น

2) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับปานกลาง (Moderate-Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่มีความอ่อนไหวมาในแง่ที่มีโอกาสที่จะก่อให้เกิดความเสียหาย เมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิดอยู่ในระดับสูง ข้อมูลประเภทนี้ครอบคลุมถึงข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมในทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้ มีความสำคัญ เช่น กันกับข้อมูลที่มีความอ่อนไหวระดับสูง และไม่ควรเก็บไว้โดยสิ้นเชิง

3) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับสูง (High-Sensitivity) ข้อมูลประเภทนี้ ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่น ๆ ในชีวิตของบุคคล ซึ่งสามารถกล่าวได้ว่าเป็นเรื่องส่วนตัวหรือลับเฉพาะข้อมูลประเภทนี้มีความอ่อนไหวสูง จึงมีความสำคัญและไม่ควรถูกเก็บรวบรวมไว้โดยสิ้นเชิง[27]

2.5 หลักการทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลเป็นสิ่งสำคัญในการพัฒนาเศรษฐกิจ การดำเนินธุรกิจล้วนอาศัยข้อมูลเป็นปัจจัยสำคัญ ดังนั้น ประเทศต่างๆ จึงให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลโดยนำหลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งหลักการขององค์การต่างๆ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development

[27] เอกณัท สุชาติพันธุ์, ประพันธ์พงษ์ ขาอ่อน. (2562). การคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร. ***การประชุมนำเสนอผลงานวิจัยบัณฑิตศึกษาระดับชาติ ครั้งที่ 14 ปีการศึกษาที่ 2562.*** หน้า 202-207.

หรือ OECD) หรือองค์การสหประชาชาติ เป็นต้น มาเป็นแนวทางในการร่างกฎหมาย เพื่อที่จะสามารถทำความเข้าใจกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศได้ดีจึงควรศึกษาหลักการทั่วไป และหลักการขององค์การต่างๆ

2.5.1 หลักการทั่วไป

1) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกฎหมายทั่วไป

ในปี ค.ศ. 1970 บัญญัติกฎหมายทั่วไปขึ้นมาฉบับหนึ่งซึ่งเป็นกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น ซึ่งนับเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก ซึ่งในเวลาต่อมาหลายประเทศก็ได้มีการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยวางหลักการทั่วไปครอบคลุมถึงการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลทั้งของภาครัฐและภาคเอกชน โดยกำหนดให้มีหน่วยงานกลางคอยกำกับดูแลให้มีการปฏิบัติตามกฎหมาย ภาคธุรกิจอุตสาหกรรมอาจกำหนดหลักเกณฑ์ในการคุ้มรองข้อมูลส่วนบุคคลขึ้นเพื่อใช้บังคับกันเองและมีหน่วยงานกลางคอยดูแลให้มีการปฏิบัติตามหลักเกณฑ์ที่กำหนด[28]

2) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกฎหมายเฉพาะ

การคุ้มครองโดยกฎหมายเฉพาะการบัญญัติกฎหมายเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคลเฉพาะกรณีเป็นวิธีการที่นิยมใช้ในบางประเทศ เช่น สหรัฐอเมริกา เป็นการหลีกเลี่ยงการวางหลักทั่วไปโดยมีกฎหมายแต่ละเรื่องไว้เป็นการเฉพาะ[29] เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต (Children's Online Privacy Act of 1998:COPPA) กฎหมายคุ้มครองข้อมูลส่วนบุคคลในการหาคู่ทางคอมพิวเตอร์ (Computer Matching and Privacy Protection Act of 1998) ข้อดีของการบัญญัติกฎหมายเฉพาะต้องมีการบัญญัติกฎหมาย คือรัฐสามารถวางกฎเกณฑ์เฉพาะเรื่องได้ ส่วนข้อเสียคือการบัญญัติกฎหมายเฉพาะต้องมีการปรับปรุง พัฒนา แก้ไข หรือบัญญัติกฎหมายใหม่เพื่อรองรับให้ทันกับเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา

3) หลักการคุ้มครองข้อมูลส่วนบุคคลโดยกลไกการกำกับดูแลตนเอง

การใช้กลไกกำกับดูแลตนเอง (Personal Data Protection) ในการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นการที่ผู้ประกอบการภาคธุรกิจประเภทเดียวกันหรือกลุ่มเดียวกันร่วมกันจัดทำประมวลจริยธรรมเพื่อเป็นระเบียบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลและร่วมกันดูแล ให้สมาชิกปฏิบัติตามกฎระเบียบปฏิบัตินั้นโดยไม่มีหน่วยงานกลางคอยกำกับดูแล[30]

---

[28] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[29] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[30] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

4) การใช้เทคโนโลยี

ในปัจจุบันมีการพัฒนาเทคโนโลยีอย่างรวดเร็วจึงมีการติดต่อสื่อสารผ่านคอมพิวเตอร์[31] เช่น การส่งอิเล็กทรอนิกส์เมล์ (E-mail) หรือ แอพริเคชั่นต่างๆ กันอย่างแพร่หลาย จึงมีผู้คิดค้นเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลในระหว่างการติดต่อสื่อสารในช่องทางดังกล่าวการคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลายรูปแบบโดยหลักเกณฑ์หรือรูปแบบดังกล่าวมีลักษณะมีหลักเกณฑ์หรือหลักปฏิบัติที่แตกต่างกันออกไป เนื่องจากการบังคับใช้กฎหมายในแต่ละประเทศหรือองค์กรนั้นรวมทั้งรูปแบบของข้อมูลที่แตกต่างกัน

2.5.2 การคุ้มครองข้อมูลส่วนบุคคลตามหลักสากล

หลักการพื้นฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลนั้น มีหลักการสำคัญซึ่งเป็นหัวใจของเรื่องอยู่ 9 หลัก[32] ดังต่อไปนี้

1) หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดเพียงเท่าที่จำเป็นเท่านั้น และการเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย นอกจากนี้ ต้องกระทำภายใต้ความรับรู้ และความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลด้วย

2) หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน (Data Quality and Proportional Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลที่ทำการประมวลผลนั้นต้องมีความเกี่ยวข้อง เพียงพอ และได้สัดส่วนหรือเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ข้อมูลส่วนบุคคลนั้นต้องมีถูกต้องสมบูรณ์และมีการปรับปรุงให้ทันสมัยอยู่ตลอดเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลและใช้ข้อมูลส่วนบุคคลนั้น อย่างไรก็ดี หลักการนี้ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้น จัดเก็บและประมวลผลข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้งซึ่ง ข้อมูลประเภทที่มีความอ่อนไหว[33] เช่น ข้อมูลเกี่ยวกับชาติกำเนิด ความเชื่อทางศาสนา หรือความเชื่อทางปรัชญา เป็นต้น

---

[31] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[32] อธิพร สิทธิธีรรัตน์.(2558). ***ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาการค้าระหว่างประเทศ, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 18-21.

[33] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

3) หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล (Purpose Specification Principle)

หลักการดังกล่าวกำหนดให้ต้องมีการระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วน บุคคลภายหลังสามารถกระทำได้หากเป็นเพียงเพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ อย่างไรก็ตามหากมีการเปลี่ยนแปลงวัตถุประสงค์ ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์การใช้ที่เปลี่ยนแปลงไปนั้นทุกคราวด้วย นอกจากนี้ การเก็บและใช้ข้อมูลส่วนบุคคลนั้นต้องไม่เกินกว่าระยะเวลาที่จำเป็นเพื่อให้วัตถุประสงค์ที่ได้แจ้งไว้สำเร็จลุล่วง[34]

4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle)

หลักการดังกล่าวห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยทำให้สามารถเข้าถึงได้หรือนำข้อมูลส่วนบุคคลไปใช้เพื่อการอย่างอื่นนอกจากจากวัตถุประสงค์อื่นซึ่งไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้อำนาจตามบทบัญญัติของกฎหมายเพื่อความมั่นคงของประเทศ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อการปฏิบัติตามกฎหมาย หรือเพื่อประโยชน์มหาชนอื่นๆ

นอกจากนี้ ยังกำหนดให้บุคคลใดซึ่งมิใช่ผู้จัดเก็บข้อมูลส่วนบุคคลจะนำข้อมูลส่วนบุคคลนั้นไปเปิดเผยโดยเจ้าของมิได้ยินยอมมิได้ แม้ทั้งการเปิดเผยนั้นจะมิได้ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลเลยก็ตาม นอกจากนี้เมื่อเจ้าของข้อมูลส่วนบุคคลอนุญาตให้มีการเปิดเผยแล้ว เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมเพื่อยุติการเผยแพร่ข้อมูลส่วนบุคคลนั้นได้ตลอดเวลา[35]

5) หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguard Principle)

หลักการนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการป้องกันรักษาความปลอดภัยของข้อมูลเพื่อมิให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ถูกทำลาย มีการใช้หรือเปลี่ยนแปลงแก้ไข หรือมีการเปิดเผยข้อมูลโดยบุคคลซึ่งปราศจากอำนาจ

6) หลักเปิดเผยโปร่งใส (Openness Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงการจัดเก็บหรือการ

---

[34] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[35] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

รวบรวมข้อมูลส่วนบุคคล หรือการนำข้อมูลส่วนบุคคลนั้นไปใช้ ระบบการประมวลผลข้อมูลส่วนบุคคล ต้องสามารถแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล รวมทั้งชื่อและสถานที่ตั้งของนายทะเบียนผู้ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล

7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

หลักการดังกล่าวกำหนดสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคล ดังต่อไปนี้[36]

(1) ได้รับแจ้งหรือยืนยันจากนายทะเบียนว่าได้ทำการประมวลผล ใช้ หรือโอนข้อมูลส่วนบุคคลของตนหรือไม่

(2) ได้รับการติดต่อจากนายทะเบียนเกี่ยวกับข้อมูลส่วนบุคคลของตน

(2.1) ภายในเวลาอันสมควร

(2.2) อาจมีค่าใช้จ่ายได้แต่ต้องไม่เกินสมควร

(2.3) โดยวิธีที่เหมาะสม

(2.4) โดยรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจได้

(3) ได้รับเหตุผลเมื่อคำร้องตามข้อ 1) และ 2) ถูกปฏิเสธ และมีสิทธิในการอุทธรณ์การปฏิเสธนั้น

(4) คัดค้านการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับตน และหากการโต้แย้งนั้นรับฟังได้มีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล ปรับปรุงหรือแก้ไขเพิ่มเติมเพื่อให้ข้อมูลส่วนบุคคลนั้นถูกต้องและสมบูรณ์

8) หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน (Restriction on Onward Opposition)

หลักการดังกล่าวมีวัตถุประสงค์เพื่อป้องกันมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับที่อยู่ในประเทศซึ่งปราศจากกฎหมายและวิธีปฏิบัติที่สามารถเป็นหลักประกันการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีสัญญาส่งโอนข้อมูลส่วนบุคคลระหว่างกันที่ให้หลักประกันอย่างเพียงพอ[37]

9) หลักความรับผิดชอบของนายทะเบียน (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการที่ 1 ถึง 8 อย่างเคร่งครัด หากฝ่าฝืนหลักการดังกล่าวและก่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ควบคุม ข้อมูลส่วนบุคคล

---

[36] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

[37] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

ต้องรับผิดทั้งในทางแพ่งและทางอาญา และรับผิดในค่าใช้จ่ายเพื่อแก้ไขข้อมูลส่วน บุคคลให้ถูกต้อง รวมไปถึงต้องลบหรือทำลายข้อมูลส่วนบุคคลอีกด้วย[38]

2.6 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และการละเมิดข้อมูลส่วนบุคคลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควบคุมการเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามบทบัญญัติ เช่น การนำข้อมูลที่ได้เก็บรวบรวมไว้ไปใช้ผิดจากวัตถุประสงค์ที่ได้รับความยินยอมโดยการนำไปหาประโยชน์ทางการตลาด หรือ การนำไปขายเพื่อประโยชน์ทางธุรกิจ หรือเกิดการละเมิดข้อมูลส่วนบุคคล ย่อมเป็นเหตุให้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเกิดความรับผิด ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในส่วนของการละเมิดข้อมูลส่วนบุคคล เป็นความผิดที่มีโทษสูงและก่อความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้มากหากเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้อธิบายความหมายของการละเมิดข้อมูลส่วนบุคคลเอาไว้โดยเฉพาะ คำอธิบายที่มีอยู่ในกฎหมายต่างประเทศโดยผู้วิจัยยกตัวอย่างจากคำนิยามในกฎหมาย General Date Protection Regulation (GDPR) ของสหภาพยุโรป มาตรา 4 (12) “การละเมิดข้อมูลส่วนบุคคล หมายถึงการละเมิดความปลอดภัยที่นำไปสู่การทำลาย สูญเสีย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกส่ง เก็บรักษา หรือประมวลผล โดยอุบัติเหตุหรือไม่ชอบด้วยกฎหมาย” ศึกษาเทียบเคียงเพราะกฎหมาย GDPR ของสหภาพยุโรปเป็นกฎหมายที่มีความเข้มงวดด้านความเป็นส่วนตัวและมีความปลอดภัยมากที่สุดของโลก การละเมิดข้อมูลส่วนบุคคล อาจเกิดจากการกระทำของบุคคลภายนอก เช่น การขโมยอัตลักษณ์เพื่อการนำไปสวมรอย (identity theft) การลักขโมยอุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคล เป็นต้น รวมทั้งอาจเกิดจากการกระทำ หรือละเว้นกระทำการของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วน

[38] สุขวสา ถมังรักษ์สัตว์. อ้างแล้วเชิงอรรถที่ 13. หน้า 131-145.

บุคคลก็ได้ เช่น การส่งข้อมูลส่วนบุคคลผิดตัว ผู้รับการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต[39]

นอกจากนี้ บทบัญญัติในพระราชบัญญัตินี้ยังกำหนดหน้าที่บางประการแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล เช่น หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลอันเป็นการกำหนดมาตรการเชิงป้องกัน และ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการบันทึกรายการเพื่อการตรวจสอบ เป็นต้น หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลหากมีการฝ่าฝืนบทบัญญัติจนเป็นเหตุให้เจ้าของข้อมูลได้รับความเสียหาย ก็ถือเป็นการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดมาตรการเชิงป้องกัน การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า เพราะการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบย่อมเกิดค่าใช้จ่ายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล[40]

อีกทั้ง การบอกกล่าวการเกิดเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคล และการบอกกล่าวการเกิดเหตุละเมิดสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งค่าใช้จ่ายเพื่อการเฝ้าระวัง การเยียวยาแก้ไขการละเมิดข้อมูลส่วนบุคคล ย่อมเกิดเป็นความเสียหายทางการเงินแก่ผู้ประกอบการ และหากไม่ได้รับการเยียวยาก็จะกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลก็คือประชาชน[41]

---

[39] ปัทมา มัญชุนากร. (2564). ***ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษา กรณีผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

[40] จีระศักดิ์ เสมมีสุข. (2564). การประกันภัยความรับผิดทางไซเบอร์: ศึกษาความคุ้มครองกรณีการละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 14(3). หน้า 348-366.

[41] เรื่องเดียวกัน, หน้า 348-366.

2.6.1 ความหมายของเหตุละเมิดข้อมูลส่วนบุคคลการละเมิดตามกฎหมายประมวลกฎหมายแพ่งและพาณิชย์

ละเมิด คือ การกระทำโดยจงใจหรือประมาทเลินเล่อต่อ บุคคลภายนอกโดยผิดกฎหมาย เป็นเหตุให้เขา (ผู้ถูกกระทำ) เสียหายแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดีทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดีกฎหมายถือว่าผู้นั้นทำละเมิดจะต้องรับผิดชอบชดใช้ค่าสินไหมทดแทนเพื่อการละเมิดนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420[42]

สรุปการกระทำใดจะเป็นละเมิดต้องประกอบด้วย หลัก 3 ประการ

1) กระทำต่อบุคคลอื่นโดยผิดกฎหมาย ซึ่งหมายถึงการประทุษกรรม กระทำต่อบุคคลโดยผิดกฎหมายด้วยอาการฝ่าฝืนต่อความหมายที่ห้ามไว้หรือละเว้นไม่กระทำในสิ่งที่กฎหมายบัญญัติให้กระทำหรือตนมีหน้าที่ตามกฎหมายจะต้องกระทำโดยจงใจหรือประมาทเลินเล่อ เป็นต้น ว่า ฆ่าเขาตายทำร้าย ร่างกายเขา ขับรถโดยประมาทชนคนตายและทรัพย์สินของเขาเสียหาย ฯลฯ

2) กระทำโดยจงใจหรือประมาทเลินเล่อ กระทำโดยจงใจ คือ การะทำโดยรู้สำนึกและในขณะเดียวกัน ก็รู้ว่าจะทำให้เขาเสียหาย เช่น เจตนาฆ่าหรือเจตนาทำร้าย ฯลฯ อย่างไร ก็ดีการกระทำโดยจงใจในเรื่องละเมิดถือหลักเบาบางกว่าทางอาญา สำหรับอาญานั้น ต้องกระทำโดยรู้สึกสำนึกในการที่ทำและในขณะเดียวกันผู้กระทำต้องประสงค์ต่อผลหรือย่อมเล็งเห็นผลด้วย ส่วนจงใจในเรื่องละเมิดบางกรณีไม่ผิดในทางอาญาแต่เป็นละเมิดต้องชดใช้ค่าเสียหายให้แก่เขา เช่น จำเลยรื้อห้องน้ำห้องครัวซึ่งโจทย์ปลูกล้ำออกไปนอกที่เช่าของวัดโดยวัดต้องการจะขุดคูได้บอกให้โจทย์รื้อแล้ว โจทย์ไม่ยอมรื้อการที่จำเลยรื้อแล้วกองไว้หลังบ้านโจทย์มิได้เจตนาชั่วร้ายทำให้ทรัพย์ของโจทย์อันตรายเสียหายไม่เป็นความผิดฐานทำให้เสียทรัพย์แต่เป็นละเมิด เพราะรู้ว่าแล้วว่าการรื้อนั้นจะทำให้ทรัพย์ของโจทย์ เสียหาย (ฎีกาที่ 1617-1618/2500)

คำว่าประมาทเลินเล่อในทางแพ่ง หมายความถึง การกระทำที่ขาดความ ระมัดระวังจนเป็นเหตุให้เกิดความเสียหายนั้นและหมายความถึงการไม่ป้องกัน ผลที่เกิดขึ้นโดยประมาทเลินเล่อแม้ตนเองไม่ได้กระทำให้เกิดผลนั้นขึ้นระดับความระมัดระวังของบุคคลต้องถือระดับบุคคลธรรมดา ตัวอย่าง เช่น นาย ก. ขับรถยนต์ไปในถนนที่มีคนเดินจอแจด้วย ความเร็วและไม่ได้ให้สัญญาณแตรแล้วเฉี่ยวชนถูกคนเดินถนนได้รับบาดเจ็บ ดังนี้ ถือว่า นาย ก. กระทำละเมิดโดยประมาทเลินเล่อ

3) ทำให้บุคคลอื่นเสียหาย โดยปกติผู้กระทำต้องรับผิดเฉพาะการกระทำของตนแต่อย่างไรก็ดี ในเรื่องละเมิดถ้าได้มีการกระทำละเมิดร่วมกันหรือแม้มิได้ร่วมแต่เป็นผู้ยุยง ส่งเสริม

---

[42] ประมาลกฎหมายแพ่งและพาณิชย์.มาตรา420.

หรือช่วยเหลือในการกระทำละเมิดดังนี้บุคคลเหล่านี้จะต้องร่วมกัน รับผิดใช้ค่าสินไหมทดแทนความเสียหายนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 432[43]

พระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539

การละเมิดตามพระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539[44] เป็นกฎหมายที่ออกมาใช้บังคับด้วยเหตุผลว่า การปฏิบัติงานของเจ้าหน้าที่มิได้เป็นไปเพื่อประโยชน์เฉพาะตัว ในการดำเนินงานบางครั้งอาจเกิดความเสียหายขึ้นโดยความไม่ตั้งใจและผิดพลาดเล็กน้อยแต่กลับต้องรับผิดเป็นการเฉพาะตัว และที่ผ่านมายังใช้หลักของลูกหนี้ร่วมทำให้เจ้าหน้าที่ต้องร่วมรับผิดในการกระทำของผู้อื่น ด้วยซึ่งเป็นระบบที่มุ่งจะให้ได้รับเงินชดใช้ค่าเสียอย่างครบถ้วนโดยไม่คำนึงถึงความเป็นธรรมที่จะมีต่อแต่ละคน จึงก่อให้เกิดความไม่เป็นธรรม และยังเป็นการบั่นทอนขวัญกำลังใจของเจ้าหน้าที่จนบางครั้งเป็นปัญหาในการบริหารงานเพราะเจ้าหน้าที่ไม่กล้าตัดสินใจในการทำงานเท่าที่ควร ดังนั้น กฎหมายฉบับนี้จึงสมควรให้เจ้าหน้าที่รับผิดทางละเมิดในการปฏิบัติหน้าที่เฉพาะเมื่อเป็นการจงใจให้เกิดความเสียหายหรือประมาทเลินเล่ออย่างร้ายแรงเท่านั้น และให้แบ่งแยกความรับผิดของแต่ละคน ทั้งนี้ เพื่อให้เกิดความเป็นธรรมและเพิ่มพูนประสิทธิภาพในการปฏิบัติงานของรัฐ

ดังนั้น การปฏิบัติงานของเจ้าหน้าที่ในหน้าที่ของตนนั้นหากเกิดความเสียหายขึ้น เจ้าหน้าที่ผู้ปฏิบัติงานได้รับการคุ้ม ครองตามกฎหมาย คือ พระราชบัญญัติความรับผิดทาง ละเมิดของเจ้าหน้าที่ พ.ศ. 2539 แต่ความเสียหายที่เกิดขึ้นจากการปฏิบัติหน้าทีนั้นต้องไม่ได้ เกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ของเจ้าหน้าที่ การที่มีกฎหมายให้ค วามคุ้มครองแก่เจ้าหน้าที่ผู้ปฏิบัติงานตามหน้าที่ดังกล่าวนั้นเนื่องจากในการปฏิบัติหน้าที่ราชการ บางกรณีอาจมีโอกาสเสี่ยงที่จะเกิดความผิดพลาดหรือเป็นเหตุสุดวิสัยโดยมิได้เกิดจากความ จงใจหรือประมาทเลินเล่ออย่างร้ายแรงส่งผลให้เกิดความเสียหายพระราชบัญญัติความรับผิด ทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539 จึงบัญญัติคุ้มครองการปฏิบัติหน้าที่ของเจ้าหน้าที่ไว้ ดังนี้

มาตรา 5 วรรคหนึ่ง[45] “หน่วยงานของรัฐต้องรับผิดต่อผู้เสียหายในผลแห่งละเมิดที่เจ้าหน้าที่ของตนได้กระทำในการปฏิบัติหน้าที่ในกรณีนี้ผู้เสียหายอาจฟ้องหน่วยงานของรัฐดังกล่าวได้โดยตรงแต่จะฟ้องเจ้าหน้าที่ไม่ได้”

---

[43] ประมาลกฎหมายแพ่งและพาณิชย์.มาตรา 432.

[44] พระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539.

[45] พระราชบัญญัติความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539. มาตรา 5.

แต่หากเจ้าหน้าที่กระทำการนอกเหนือหรือไม่ได้ปฏิบัติงานในหน้าที่ปกติของตน เช่น เจ้าพนักงานการเงิน ไม่ได้มีหน้าที่ในการขับรถ แต่ได้ขับรถไปซึ่งมิใช่หน้าที่ของตน แล้วเกิดเฉี่ยวชนกับคุคลภายนอกได้รับความเสียหายเป็นต้นย่อมไม่ได้รับการคุ้มครองตามกฎหมาย

มาตรา 6 [46]บัญญัติว่า“ถ้าการกระทาละเมิดของเจ้าหน้าที่มิใช่การกระทาในการปฏิบัติหน้าที่ เจ้าหน้าที่ต้องรับผิดในการนั้น เป็นการเฉพาะตัว ในกรณีนี้ผู้เสียหายอาจฟ้องเจ้าหน้าที่ ได้โดยตรง แต่จะฟ้องหน่วยงานรัฐไม่ได้”

จะเห็นได้ว่าหากเจ้าหน้าที่ปฏิบัติหน้าที่อื่นนอกเหนือหน้าที่ของตนตามที่กฎ ระเบียบกำหนดไว้แล้วรัฐไม่คุ้มครองแต่ถ้าได้ปฏิบัติงานในหน้าที่ของตนโดยชอบแล้วเมื่อเกิดความผิดพลาดไม่ว่าบุคคลใดได้รับความเสียหายหรือทำให้รัฐเองเสียหายก็ตาม หน่วยงานของรัฐ จะต้องเข้ารับผิดชดใช้ค่าเสียหายแทนเจ้าหน้าที่ แต่ก็ต้องพิจารณาต่อไปว่า ความผิดพลาดที่เกิดขึ้นเนื่องมาจากการจงใจหรือประมาทเลินเล่ออย่างร้ายแรงของเจ้าหน้าที่หรือไม่ ตามความที่บัญญัติไว้ใน มาตรา 8 วรรคหนึ่ง ในกรณีที่หน่วยงานของรัฐต้องรับผิดใช้ค่าสินไหมทดแทนแก่ผู้เสียหาย เพื่อการละเมิดของเจ้าหน้าที่ ให้หน่วยงานของรัฐมีสิทธิเรียกให้เจ้าหน้าที่ผู้ทำละเมิดชดใช้ค่า สินไหมทดแทนดังกล่าวแก่หน่วยงานของรัฐได้ ถ้าเจ้าหน้าที่ได้กระทำการอันเป็นไปด้วยความจงใจ หรือประมาทเลินเล่ออย่างร้ายแรง

กรณีจะเป็นประมาทเลินเล่ออย่างร้ายแรงจะต้องเป็นประมาทเลินเล่อเสียก่อนโดย“จะเป็นส่วนที่อยู่กึ่งกลางระหว่างจงใจกับประมาทเลินเล่อธรรมดา” คณะกรรมการกฤษฎีกาเคยตอบข้อหารือกรมบัญชีกลางว่า การที่จะพิจารณาว่ากรณีใดจะเป็นการกระทำด้วยความประมาทเลินเล่ออย่างร้ายแรงของเจ้าหน้าที่หรือไม่นั้น เป็นหน้าที่ของเจ้าหน้าที่ผู้มีอำนาจดำเนินการตามกฎหมายและระเบียบทุกคน จนถึงคณะกรรมการวินิจฉัยร้องทุกข์หรือศาล ส่วนอย่างไรเป็นการประมาทเลินเล่ออย่างร้ายแรงย่อมขึ้นอยู่กับข้อเท็จจริงแต่ละกรณีไปความประมาทเลินเล่ออย่างร้ายแรงจะมีลักษณะไปในทางที่บุคคลนั้นได้กระทำไปโดยขาดความระมัดระวังที่เบี่ยงเบนไปจากเกณฑ์มาตรฐานอย่างมาก เช่น คาดเห็นได้ว่าความเสียหายอาจเกิดขึ้นได้หรือหากใช้ความระมัดระวังสักเล็กน้อย ก็คงได้คาดเห็นการอาจเกิดความเสียหายนั้นนั้นเอง[47]

การละเมิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ตามแนวทางของ General data Protection Regulation (GDPR) เหตุละเมิดข้อมูลส่วนบุคคล มีความหมายดังต่อไปนี้

---

[46] พระราชบัญญัติความรับผิด ทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539. มาตรา 6.

[47] กองกฎหมาย กรมทรัพยากรทางทะเลและชายฝั่ง. ***หลักการกระทำละเมิด ประมวลกฎหมายแพ่งและพาณิชย์.*** (ออนไลน์). เข้าถึงได้จาก: https://dmcrth.dmcr.go.th/lag/detail/1110/

“เหตุการละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดหรือฝ่าฝืนมาตรการความปลอดภัยที่นำไปสู่การทำลายโดยบังเอิญหรือไม่ชอบด้วยกฎหมาย ความเสียหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่มีอำนาจ หรือการเข้าถึง ซึ่งข้อมูลส่วนบุคคลที่มีการส่ง เก็บรักษา หรือประมวลผล

ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37[48] บัญญัติว่า ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ดังนี้ มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมี ความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคล ทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด”

หน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว มีประเด็นที่ต้องพิจารณาทางกฎหมายหลายประการ โดยเฉพาะการเริ่มนับระยะเวลา 72 ชั่วโมงว่าเริ่มเมื่อไหร่ เนื่องจากองค์กรอาจมีความรับผิดทางกฎหมายหากไม่แจ้งภายในระยะเวลาที่กฎหมายกำหนด

2.6.2 หลักการทั่วไปของการแจ้งเหตุละเมิด

หลักการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุข้อมูลรั่วไหล หรือถูกล่วงละเมิด (Data Breach Notification) โดยแยกเป็น 2 กรณี ดังนี้

1) การแจ้งต่อหน่วยงานกำกับ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หลักการนี้ปรากฏในกฎหมายสหภาพยุโรปมาตรา 33 (Notification of a personal data breach to the supervisory authority) และการแจ้งเหตุข้อมูลรั่วไหลหรือล่วงละเมิดต่อเจ้าของข้อมูล หลักการนี้ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปมาตรา 34 (Communication of a personal data breach to the data subject)

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (2)[49] ซึ่งจำแนกเป็นการแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการแจ้งต่อเจ้าของข้อมูล หลักการนี้ส่งผลให้เกิดภาระต้นทุนการทำให้สอดคล้องกับกฎหมาย เช่น ก่อนการแจ้งต้องมีการประเมินสถานการณ์ตรวจสอบข้อเท็จจริงและหลักฐานทางอิเล็กทรอนิกส์ (Forensic) ซึ่งต้องอาศัยงบประมาณและ

[48] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

[49] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

การจ้างผู้เชี่ยวชาญ รวมทั้งต้นทุนในการปฏิบัติการส่งข้อมูลการแจ้งต่าง ๆ[50] และมาตรา 37 (4)[51] "แจ้งเหตุการ ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำ ได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมี ความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคล ทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์ และวิธีการที่คณะกรรมการประกาศกำหนด"[52]

ถ้อยคำหนึ่งในมาตรา 37 (4)[53] ที่เป็นจุดเริ่มต้นสำคัญของการเริ่มนับระยะเวลา คือ "นับแต่ทราบเหตุ" (become aware) ซึ่งต้องทำความเข้าใจทั้งข้อเท็จจริงและข้อกฎหมายประกอบกัน เพื่อทำความเข้าใจจุดเริ่มต้นการนับระยะเวลาดังกล่าวมากขึ้น

ตาม GDPR "นับแต่ทราบเหตุ" ให้เริ่มต้นเมื่อ "ผู้ควบคุมข้อมูลส่วนบุคคล" มีความแน่ใจในว่าเหตุการณ์ข้อมูลรั่วไหลที่เกิดขึ้น (security incident) มีผลทำให้ข้อมูลส่วนบุคคลถูกละเมิด

ในกรณีนี้ต้องทำความเข้าใจก่อนว่าตามแนวทางของ GDPR นั้นไม่ใช่ภัยคุกคามทางไซเบอร์ทุกปะเภทหรือเหตุการณ์ข้อมูลรั่วไหลทุกประเภทจะเข้าเงื่อนไขของ "Data Breach" หรือที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ เรียกว่า "เหตุการละเมิดข้อมูลส่วนบุคคล"

ดังนั้น สิ่งแรกที่องค์กรต้องทำการประเมินก่อน คือ ผลของเหตุการณ์ข้อมูลรั่วไหลนั้นได้ส่งผลกระทบต่อความเสี่ยง หรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่

วินาทีที่มี "reasonable degree of certainty" คือ จุดเริ่มต้นนับหนึ่งของระยะเวลา ที่ต้องแจ้งอย่างช้าภายใน 72 ชั่วโมงตามเงื่อนไขที่ GDPR กำหนดหากเหตุการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ดังนั้น กระบวนการตรวจสอบเหตุการณ์ข้อมูลรั่วไหลเบื้องต้น ที่สามารถนำไปสู่ระดับความแน่นอนพอสมควร (reasonable degree of certainty) ว่าข้อมูลส่วนบุคคลได้ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้งาน (Security Triad: loss of

---

[50] คณาธิป ทองรวีวงศ์. (2564). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารรัชต์ภาคย์,*** 15(38). หน้า 42-56.

[51] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

[52] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 34.

[53] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

confidentiality, integrity and/or availability) จึงเป็นเงื่อนไขบังคับก่อนที่สำคัญของการเริ่มต้นนับระยะเวลา

นอกจากนี้ องค์กรยังมีหน้าที่ต้องจัดให้มีมาตรการเชิงเทคนิคและเชิงองค์กรเพื่อให้มั่นใจว่าองค์กรจะสามารถ "ทราบเหตุ"ได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถดำเนินการตามขั้นตอนต่าง ๆ ที่กฎหมายกำหนดอีกด้วย

ทั้งนี้เพื่อป้องกันมิให้องค์กรใช้เป็นข้ออ้างได้ว่า "ไม่สามารถตรวจพบหรือทราบเหตุ" เพราะเมื่อกฎหมายบังคับให้ต้องมีมาตรการที่เหมาะสมแล้ว โดยผลของการจัดให้มีมาตรการดังกล่าว องค์กรจึงมีหน้าที่ต้องรู้หรือควรรู้ว่าเกิดเหตุการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสมอีกด้วย

การพิจารณา "นับแต่ทราบเหตุ" ก็ยังคงเป็นข้อเท็จจริงที่ต้องพิจารณาเป็นรายกรณีไป ในบางกรณีก็อาจจะใช้เวลาพอสมควรเพื่อให้สามารถแน่ใจ (degree of certainty) ว่าเหตุการณ์ข้อมูลรั่วไหล (security incident) หรือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลด้วย ซึ่งมียกตัวอย่างกรณีศึกษาของการพิจารณาไว้ดังนี้[54]

ตัวอย่างที่ 1 กรณี USB key สูญหาย

กรณีที่ USB key ที่ถูกเข้ารหัสไว้สูญหาย กรณีนี้ย่อมมีความไม่แน่นอนว่าผู้ที่ได้ไปจะสามารถเข้าถึงข้อมูลส่วนบุคคลใน USB key หรือไม่และข้อมูลจะสูญเสียการเป็นความลับหรือไม่ (confidentiality breach) แต่ในกรณีนี้ย่อมเป็นที่แน่นอนว่าองค์กรได้สูญเสียความสามารถในการเข้าถึงข้อมูลหรือความพร้อมใช้ของข้อมูลไปแล้ว (availability breach) "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรรู้ว่า USB key ได้หายไป

ตัวอย่างที่ 2 ข้อมูลถูกเปิดเผยไปยังบุคคลภายนอก

มีบุคคลภายนอกได้แจ้งให้องค์กรทราบว่าเขาได้รับข้อมูลส่วนบุคคลของลูกค้าขององค์กรโดยอาจจะเกิดจากการส่งอีเมลผิดหรือจดหมายผิด และบุคคลภายนอกนั้นได้แสดงหลักฐานให้เห็นว่าเขาได้รับข้อมูลมาโดยไม่ถูกต้อง กรณีนี้ต้องถือว่าเกิดการสูญเสียการเป็นความลับของข้อมูลส่วนบุคคลขึ้นแล้ว (confidentiality breach) "นับแต่ทราบเหตุ" [55]จึงเริ่มต้นตั้งแต่องค์กรได้รับทราบหลักฐานของการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

ตัวอย่างที่ 3 เครือข่ายถูกโจมตีหรือถูกเข้าถึง

---

[54] คณาธิป ทองรวีวงศ์. อ้างแล้วเชิงอรรถที่ 50. หน้า 42-56.

[55] ศุภวัชร์ มาลานนท์. (2565).***การเริ่มนับระยะเวลา แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/992923 [2566, 27 มิถุนายน]

ในกรณีที่มีตรวจพบว่าอาจจะมีการเข้าถึงเครือข่ายขององค์กร โดยไม่ชอบด้วยกฎหมาย และองค์กรได้ตรวจสอบระบบแล้วพบว่ามีการเข้าถึงโดยไม่ชอบด้วยกฎหมายดังกล่าวได้ส่งผลกระทบต่อข้อมูลส่วนบุคคลในองค์กร "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าข้อมูลส่วนบุคคลได้รับผลกระทบ

ตัวอย่างที่ 4 อาชญากรรมทางคอมพิวเตอร์/การเรียกค่าไถ่

องค์กรถูกเรียกค่าไถ่จากแฮกเกอร์เพื่อแลกกับการไม่เผยแพร่ข้อมูลออกสู่สาธารณะ องค์กรจึงเร่งตรวจสอบระบบของตนเองว่าถูกละเมิดหรือโจมตีโดยบุคคลภายนอกหรือไม่ ข้อเท็จจริงจากการตรวจสอบยืนยันว่ามีการถูกเข้ารหัสข้อมูลโดยบุคคลภายนอกจริง "นับแต่ทราบเหตุ" จึงเริ่มต้นตั้งแต่องค์กรสามารถยืนยันว่าระบบของตนเองถูกโจมตีและมีข้อมูลส่วนบุคคลได้รับผลกระทบ

ตัวอย่างที่ 5 เหตุการละเมิดเกิดจาก "ผู้ประมวลผลข้อมูลส่วนบุคคล"

หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานบังคับใช้กฎหมายเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ส่วน "ผู้ประมวลผลข้อมูลส่วนบุคคล" มีหน้าที่แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นเท่านั้น[56]

ใน GDPR ไม่ได้ระบุชัดเจนว่า "นับแต่ทราบเหตุ" จะเริ่มจากการที่ "ผู้ประมวลผลข้อมูลส่วนบุคคล" ทราบเหตุหรือจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งจากผู้ประมวลผลข้อมูลส่วนบุคคล แต่ข้อตกลงในสัญญาระหว่างกัน (Data Processing Agreement) ต้องกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้ชัดเจนว่าต้องดำเนินการอย่างไรบ้างเพื่อสนับสนุนและให้ความร่วมมือกับองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลขึ้น

ซึ่งเงื่อนไขหนึ่งของหน้าที่ "แจ้ง" ที่กล่าวมาทั้งหมด เป็นเหตุการละเมิดข้อมูลส่วนบุคคลในส่วนของเงื่อนไขการเริ่มนับระยะเวลา 72 ชั่วโมงเท่านั้น การที่ต้องแจ้งหรือไม่ต้องแจ้งและต้องแจ้งใครบ้าง วิธีการแจ้งและมาตรการต่างๆ ที่ต้องดำเนินการเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ยังมีรายละเอียดที่ต้องพิจารณา จากการประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลประกอบอีกด้วย[57]

2.6.3 ตัวอย่างการละเมิดข้อมูลส่วนบุคคล

กรณีศึกษาที่ 1: การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Anthem, Inc. ในปีพ.ศ. 255

---

[56] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 39. หน้า 1.

[57] ศุภวัชร์ มาลานนท์. (2565). ***การเริ่มนับระยะเวลาแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/992923 [2566, 27 มิถุนายน]

ข้อเท็จจริง

ในปี พ.ศ. 2558 Anthem, Inc. ซึ่งเป็นบริษัทประกันภัยรายใหญ่ของสหรัฐอเมริกาได้ประกาศว่าข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัทได้ถูกละเมิดไปราว 3.7 ล้านชุดข้อมูล และเป็นข้อมูลส่วนบุคคลของชาวอเมริกันมากกว่า 80 ล้านคน ซึ่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวเกิดขึ้นเนื่องจากถูกแฮกเกอร์ (Hacker) นำข้อมูลส่วนบุคคลไป โดยการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้นมิได้เกิดขึ้นเพียงครั้งเดียว แต่เกิดขึ้นเรื่อย ๆ ระหว่างช่วงเดือนธันวาคม พ.ศ. 2557 จนถึงเดือนกุมภาพันธ์ พ.ศ. 2558 โดยข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ อีเมล หมายเลขประกันสังคม วันเกิด หมายเลขสมาชิกประกันภัย หมายเลขผู้ป่วย ข้อมูลพนักงาน และรายได้ของบริษัท ซึ่งจากการตรวจสอบพบว่าโดยมากข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นได้ถูกนำไปขายต่อให้กับตลาดมืด และไม่ได้มีการนำข้อมูลจำพวกประวัติสุขภาพไปใช้

นอกจากนั้นจากการตรวจสอบยังพบว่าการเกิดเหตุละเมิดนั้นอาจเป็นเพราะว่า Athem, Inc. ไม่ได้มีระบบรักษาความปลอดภัยที่เพียงพอ กล่าวคือ Athem, Inc. ไม่ได้มีมาตรการในการเข้ารหัสข้อมูล (Encryption) ที่มีการจัดเก็บซึ่งอาจทำให้ Hacker สามารถทำลายระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคล และเข้าถึงข้อมูลส่วนบุคคลได้โดยง่าย

บทวิเคราะห์

จากกรณีข้างต้นทำให้เห็นว่าการจัดการเกี่ยวกับระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นเรื่องสำคัญอย่างยิ่งสำหรับผู้ควบคุมข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งผู้ควบคุมข้อมูลส่วนบุคคลที่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ดังเช่นบริษัทประกันวินาศภัย และบริษัทประกันชีวิต เนื่องจากข้อมูลส่วนบุคคลเหล่านั้นสามารถทำให้เกิดความเสียหาย หรือเกิดผลกระทบกับสิทธิและเสรีภาพของบุคคลได้ง่าย

การเข้ารหัสข้อมูล (Encryption) เป็นวิธีหนึ่งที่จะช่วยให้บริษัทฯ สามารถจัดการกับข้อมูลส่วนบุคคล และป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้

ในกรณีนี้ Athem, Inc. ได้มีขั้นตอนการดำเนินการจัดการ และแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่รวดเร็ว และน่านำไปเป็นแบบอย่าง ตามที่เจ้าหน้าที่ FBI ได้กล่าวให้สัมภาษณ์ไว้ โดยเมื่อพนักงานของ Athem, Inc. พบข้อสงสัยเกี่ยวกับฐานข้อมูลของบริษัท บริษัทก็เริ่มดำเนินการตรวจสอบทันที และเมื่อบริษัทหาสาเหตุ และรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลได้แล้ว บริษัทก็ดำเนินการแจ้ง FBI ของสหรัฐอเมริกา พร้อมทั้งส่งจดหมายแจ้งเจ้าของข้อมูลส่วนบุคคลที่อาจได้รับผลกระทบทันที โดยในการแจ้งรายละเอียดเรื่องการละเมิดข้อมูลส่วนบุคคลนั้นบริษัทได้มีการแจ้งไปถึงประเภทข้อมูลส่วนบุคคลที่ถูกขโมยไป และหลังจากนั้น Athem, Inc. ก็ได้

จ้างบริษัทจัดการด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศหลายรายให้เข้าร่วมจัดการกับระบบรักษาความปลอดภัยของบริษัทเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

กรณีศึกษาที่ 2 การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Capital One[58]

ข้อเท็จจริง

เมื่อเดือนกรกฎาคม พ.ศ. 2562 ที่ผ่านมา Capital One ซึ่งเป็นสถาบันการเงินของสหรัฐอเมริกาได้ถูกแฮกเกอร์ (Hacker) เข้าสู่ระบบฐานข้อมูลแบบ Cloud ของบริษัทโดยที่บุคคลดังกล่าวเป็นพนักงานของบริษัท Amazon Web Services (AWS) ซึ่งเป็นผู้ให้บริการด้านการจัดการข้อมูลบนระบบ Cloud ที่ Capital One ใช้บริการอยู่ โดยที่พนักงานดังกล่าวสามารถเข้าถึงข้อมูลทั้งหมดของ Capital One ได้ และได้นำเรื่องที่ตนสามารถแฮกข้อมูลของ Capital One ได้ไปโพสต์ลงในกรุ๊ปของ Github ซึ่งเป็นเว็บไซต์ที่ให้บริการพื้นที่ทางอินเทอร์เน็ตสำหรับเก็บการควบคุมการปรับปรุงแก้ไขเอกสารออนไลน์โดยใช้กิต (Git)[59] อันทำให้ Capital One ได้รับทราบถึงการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

ในการแฮกระบบฐานข้อมูลของ Capital One ในครั้งนี้ทำให้ข้อมูลของลูกค้าบัตรเครดิตเป็นจำนวนมากถูกขโมยไป โดยเจ้าของข้อมูลส่วนบุคคลที่ถูกขโมยไปเป็นชาวอเมริกันประมาณ 100 ล้านคน และเป็นลูกค้าชาวแคนาดาอีกประมาณ 6 ล้านคน ซึ่งข้อมูลส่วนบุคคลที่ถูกแฮกไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล วันเกิด หมายเลขประกันสังคม ข้อมูลที่สามารถเชื่อมไปยังบัญชีธนาคาร และสถานะของบัตรเครดิตของลูกค้า

แต่อย่างไรก็ตาม จากการตรวจสอบการละเมิดข้อมูลส่วนบุคคลนี้ พบว่าข้อมูลที่ถูกแฮกไปนั้นไม่ได้ถูกนำไปใช้ หรือเผยแพร่ให้แก่บุคคลอื่นใดเลย เพียงแต่มีการไปโพสต์โดยแฮกเกอร์ว่ามีการเข้าถึงข้อมูลของ Capital One ได้เท่านั้น และนอกจากนั้นจากการตรวจสอบยังทำให้พบอีกว่าการที่พนักงานของ AWS

สามารถเข้าถึงข้อมูลในฐานระบบของ Capital One ได้ทุกข้อมูลนั้นเป็นเพราะการใช้งาน และตั้งค่าระบบ could ที่เหมาะสม ไม่มีการตั้งค่าในเรื่องของสิทธิในการเข้าถึงข้อมูลของ

---

[58] Howard Poston. (2019). ***Lessons learned: The Capital One breach***. (Online). Available: https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/ [2023, June 30]

[59] Pakin Phuhinkong. (2017). ***Git คือ Version Control แบบ Distributed ตัวหนึ่ง เป็นระบบที่ใช้จัดเก็บและควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ชนิดใดก็ได้ ไม่ว่าจะเป็น Text File หรือ Binary File***. (ออนไลน์). เข้าถึงได้จาก: https://medium.com/@pakin/git-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-git-is-your-friend-c609c5f8efea [2566, 27 มิถุนายน]

พนักงาน และบุคคลที่เกี่ยวข้องซึ่งโดยทั่วไปแล้วบริษัทควรจะต้องจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานเท่าที่จำเป็นตามหน้าที่ของพนักงานแต่ละคนเท่านั้น

บทวิเคราะห์

จากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของ Capital One ทำให้เห็นว่าการใช้ระบบ Cloud ในการจัดการข้อมูลของบริษัทฯ ต้องใช้ความระมัดระวังอย่างยิ่งเนื่องจากการจัดการรักษาความปลอดภัยของการใช้ระบบ Cloud นั้นอาจไม่เหมือนกับการจัดการระบบรักษาความปลอดภัยของระบบที่ตั้งอยู่ในบริษัทฯ[60]

การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานแต่ละคนให้สอดคล้องกับความจำเป็น และหน้าที่การงานเป็นสิ่งที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เนื่องจากการให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลเกินความจำเป็นอาจทำให้เกิดโอกาสสำหรับผู้ที่เข้าถึงข้อมูลในการนำข้อมูลไปใช้โดยมิชอบได้

การจัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลก็เป็นวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลได้วิธีหนึ่ง เนื่องจากการจัดให้มีระบบติดตาม และบันทึกการเข้าถึงข้อมูลส่วนบุคคลนี้จะทำให้บริษัทฯ สามารถตรวจสอบได้ว่ามีบุคคลใดบ้างที่เข้าถึงข้อมูลส่วนบุคคล และบุคคลใดที่เข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งเนื่องจาก Capital One ไม่ได้จัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสม เพียงพอ ทำให้ Capital One ไม่สามารถตรวจจับการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้เลย จนกระทั่งมีการโพสต์ในเรื่องการเข้าถึงข้อมูลของ Capital One ในกลุ่ม Github ซึ่งเป็นการโพสต์โอ้อวดความสามารถของแฮกเกอร์เอง

2.7 ผู้ที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ถือเป็นประเด็นที่ต้องพิจารณาทางกฎหมายหลายประการ โดยมีการกำหนดจากการเริ่มนับระยะเวลา 72 ชั่วโมง เนื่องจากองค์กรอาจมีความรับผิดทางกฎหมายหากไม่แจ้งภายในระยะเวลาที่กฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด[61] ซึ่งในมาตรา มาตรา 37(4)[62] มีการเขียนไว้ว่า การแจ้งเหตุการละเมิดข้อมูลส่วน

---

[60] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[61] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[62] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

บุคคลแก่สำนักงานโดยไม่ชักช้าภายใน72 ชั่วโมง “ นับแต่ทราบเหตุ” เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ดังนั้น จุดเริ่มต้นสำคัญที่สุดของการเริ่มนับระยะเวลา คือ “นับแต่ทราบเหตุ” (become aware)

2.7.1 ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล หรือ (DATA CONTROLLER) หากมีการพิจารณาแล้วว่าเหตุการณ์ข้อมูลรั่วไหลที่เกิดขึ้น (security incident)[63] มีผลทำให้ข้อมูลส่วนบุคคลถูกละเมิด ดังนั้น สิ่งแรกที่องค์กรต้องทำการประเมินก่อน คือ อธิบายผลของเหตุการณ์ข้อมูลรั่วไหลนั้นได้ส่งผลกระทบต่อความเสี่ยง หรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่'[64]

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

มาตรา 37[65] “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

---

[63] มหาวิทยาลัยมหิดล วิทยาลัยนานาชาติ . (2565). ***ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller).*** (ออนไลน์). เข้าถึงได้จาก: https://muic.mahidol.ac.th/thai/%E0%B8%9C%E0%B8%B9%E0%B9%89%E0%B8%84%E0%B8%A7%E0%B8%9A%E0%B8%84%E0%B8%B8%E0%B8%A1%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84/ [2566,7มิถุนายน]

[64] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[65] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคล ได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น

การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อ สิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด

(5) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตั้งตัวแทนของ ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจ ให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 39[66] “มาตรา 39 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ ก็ได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูล ส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

---

[66] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 39.

(6) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง โดยอนุโลม ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่ มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26”

2.8 บทลงโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ หากฝ่าฝืนจะมีบทลงโทษ โดยมีการกำหนดโทษไว้ถึง 3 ประเภท ได้แก่ ในหมวดที่ 6 ความรับผิดทางแพ่ง หมวดที่ 7 ส่วนที่หนึ่ง โทษอาญา ส่วนที่สองโทษทางปกครอง โดยในส่วนความรับผิดทางแพ่งได้กำหนดให้มีค่าเสียหายเชิงลงโทษและต้องชดใช้ค่าสินไหมทดแทนรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย และในหมวดที่ 7 ส่วนที่สอง โทษทางปกครองซึ่งการกระทำผิดบางฐานกำหนดค่าปรับทางปกครองสูงถึงห้าล้านบาท[67]

2.8.1 โทษอาญา

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้กำหนดโทษ หรือความรับผิดไว้สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ในบางกรณี เช่น กรณีที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นจากการปฏิบัติหน้าที่ฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนำข้อมูลเหล่านั้นไปเปิดเผยแก่บุคคลอื่น

---

[67] ฉัตรสุมน พฤฒิภิญโญ. (2565). PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล. ***วารสารกฎหมายและนโยบายสาธารณสุข,*** 8(1). หน้า 203-214.

"มาตรา 80[68] ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

1) การเปิดเผยตามหน้าที่

2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้า ที่ตามกฎหมาย

4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ"

2.8.2 โทษทางปกครอง

โทษทางปกครองของ PDPA คือโทษปรับเป็นตัวเงิน ซึ่งมีตั้งแต่ 1 ล้านบาทไปจนถึง 5 ล้านบาท โดยกรณีที่จะโดนโทษปรับสูงสุด 5 ล้านบาทนี้ คือกรณีที่มีการฝ่าฝืนข้อกำหนดที่เกี่ยวกับการใช้หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปต่างประเทศในส่วนที่เป็นข้อมูลส่วนบุคคล sensitive และแน่นอนว่า โทษปรับนี้เป็นคนละส่วนต่างหากจากการชดใช้ค่าเสียหายทางแพ่งและโทษปรับทางอาญา[69]

ประกอบด้วยความรับผิดดังนี้

1) ไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศ หรือไม่แจ้งผลกระทบจากการถอนความยินยอม มีโทษปรับทางปกครองไม่เกินหนึ่งล้าน (1,000,000) บาท

2) ขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ส่ง หรือโอนข้อมูลส่วนบุคคล โดยไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ มีโทษปรับทางปกครองไม่เกินสามล้าน (3,000,000) บาท

---

[68] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 80.

[69] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

3) เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม มีโทษปรับทางปกครองไม่เกินห้าล้าน (5,000,000) บาท

4) ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่ปฏิบัติตามมีโทษปรับทางปกครองไม่เกินหนึ่ง (1,000,000) ล้านบาท

5) ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้าน (3,000,000) บาท

6) ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรอง หรือไม่มีมาตรการคุ่มครองที่เหมาะสมตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด มีโทษปรับทางปกครองไม่เกินห้าล้าน (5,000,000) บาท

7) ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 39 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 39 วรรคสอง และมาตรา 41 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 41 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้าน (1,000,000) บาท

8) ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ มีโทษปรับทางปกครองไม่เกินห้าแสน (500,000) บาท

9) กรณีที่เห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้

บทลงโทษในกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำาหนดจะถูกปรับเป็นจำานวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่น กรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบการไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำา Privacy Impact Assessment

บทกำหนดโทษข้อมูลส่วนบุคคลถือเป็นสิทธิของเจ้าของข้อมูล ดังนั้น การละเมิดสิทธิในข้อมูลส่วนบุคคลจึงเป็นสิ่งต้องห้าม หากผู้ใดละเมิดสิทธิของเจ้าของข้อมูลแล้วผู้นั้นสมควรอย่างยิ่งที่จะได้รับโทษโดยเฉพาะโทษทางอาญา ร่างพระราชบัญญัติฉบับนี้จึงกำหนดให้ผู้ใดก็ ตามที่กระการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้นั้นต้องรับโทษทาง

อาญา ในส่วนของพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 นั้นจะเห็นได้ว่ามีการร่างออกมาเพื่อมุ่งคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานเอกชนโดยตรง ซึ่งไม่ใช่แค่สถาบันทางการเงินอย่างเดียวเหมือน พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545[70] แต่ยังคลอบคลุมไปถึง หน่วยงานภาคเอกชนทั้งหมด ว่าจะต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล ในการจัดเก็บข้อมูลส่วน บุคคล การใช้และการเปิดเผยข้อมูล ซึ่งหากมีการละเมิดข้อมูลส่วนบุคคล หรือปิดเผยโดยเจ้าของ ข้อมูลไม่ได้ให้ความยินยอม ก็จะมีบทโทษสำหรับผู้ที่กระทำความผิดนั้น[71]

[70] พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

[71] จันทร์ทิพย์ แสงแปง. (2559). ***ปัญหาการคุ้มครองข้อมูลส่วนบุคคลศึกษากรณี การจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

บทที่ 3

กฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ของกฎหมายไทยและกฎหมายต่างประเทศ

ในส่วนของบทที่ 3 นี้ จะเป็นการกล่าวถึงกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลทั้งในกฎหมายไทย และกฎหมายต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา โดยแต่ละประเทศมีมาตรการที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแตกต่างกันออกไป ไม่ว่าจะเป็นแนวทางปฏิบัติ หลักเกณฑ์ หรือบทลงโทษต่างๆ โดยรายละเอียดของกฎหมายแต่ละประเทศมีดังต่อไปนี้

3.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของไทยนั้น ได้บัญญัติไว้หลายฉบับ ซึ่งแต่ละฉบับนั้นมีรายละเอียดที่แตกต่างกันออกไป จึงขออธิบายเกี่ยวกับกฎหมายฉบับต่างๆ ดังต่อไปนี้

3.1.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 24 พฤษภาคม 2562 และกฎหมายฉบับดังกล่าวมีผลบังคับใช้อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นมา และกฎหมายฉบับนี้จะมีผลกระทบทั้งต่อภาคประชาชน หน่วยงานรัฐ และหน่วยงานเอกชน เนื่องจากปัจจุบันมีการล่วงละเมิด สิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว แม้จะมีกฎหมายฉบับนี้ออกมาควบคุมในการรวบรวมและเก็บข้อมูลส่วนบุคคลแล้ว แต่ยังมีประเด็นที่น่าคิดว่าในทางปฏิบัติหรือการบังคับใช้กฎหมายฉบับนี้ เช่น ประเด็นเรื่องการเก็บข้อมูลส่วนบุคคล ซึ่งในส่วนของกฎหมายจะมีข้อมูลที่จำเป็นหรือบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บได้ หรือเป็นกรณี

การให้ความยินยอม (Consent) ของผู้เป็นเจ้าของข้อมูลส่วนบุคคลที่จะยินยอมให้เก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่[1]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถือเป็นกฎหมายกลางที่กำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ สร้างความเป็นไปตามมาตรฐานสากล และมีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดอย่างเหมาะสม เป็นหลักการพื้นฐานที่เกี่ยวกับข้อมูลส่วนบุคคล ซึ่งพยายามให้มีความสอดคล้องกับหลักมาตรฐานสากลตามที่สหภาพยุโรปได้มีการออกกฎระเบียบGeneral Data Protection Regulation (GDPR) เพื่อคุ้มครองประชาชนมิให้ถูกล่วงละเมิดในความเป็นส่วนตัว และนำข้อมูลส่วนบุคคลของประชาชนไปแสวงหาผลประโยชน์ หรือเปิดเผยโดยไม่ได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูลก่อน[2]

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้บัญญัติหลักการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ในมาตรา 37 ดังนี้

มาตรา 37[3] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้” มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด”

---

[1] ทัชชภร มหาแถลง. (2563). การคุ้มครองชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ***, 11(2). หน้า 80-97.

[2] อมรรัตน์ อริยะชัยประดิษฐ์. (2565). การศึกษาเปรียบเทียบโทษทางอาญากับโทษทางปกครองตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารมนุษยศาสตร์ และสังคมศาสตร์ มหาวิทยาลัย มหาสารคาม,*** 41(4). หน้า 129-141.

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37.

ความหมายของการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งออกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 [4]ได้กำหนดนิยามของคำว่า "การละเมิดข้อมูลส่วนบุคคล" ให้มีความหมายดังต่อไปนี้[5]

"การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด"[6]

เหตุการณ์ที่อาจถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

1) การที่บุคคลที่สามเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ

2) การกระทำ หรือการไม่กระทำการ โดยเจตนาหรือไม่เจตนา ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลข้อมูลส่วนบุคคล

3) การส่งข้อมูลส่วนบุคคลไปยังผู้รับผิดคน

4) การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

5) การสูญเสียความสามารถในการใช้ข้อมูลส่วนบุคคล (Ransomware)

6) เกิดการเจาะระบบ (Hack) ที่บริษัทใช้งาน

หน้าที่แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)[7] กำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่บุคคลตามกรณี ดังต่อไปนี้

1) ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า หรือเท่าที่สามารถกระทำได้ ภายใน 72 ชั่วโมง นับแต่ทราบเหตุแห่งการละเมิดข้อมูล

---

[4] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562. มาตรา 37.

[5] แคทรียา มาลาศรี. (2566). ***สรุปข้อมูลสำคัญที่ Data Controller ต้องรู้ ประกาศใหม่จาก PDPC หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ 2565***. (ออนไลน์). เข้าถึงได้จาก: https://t-reg.co/blog/news/guideline-for-data-breach-report-pdpa-law/. [2566,30 มิถุนายน]

[6] pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ [2566,30 มิถุนายน]

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37(4).

2) แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางเยียวยาโดยไม่ชักช้า[8]

ตารางที่ 1 ตารางระดับของเหตุละเมิดข้อมูลส่วนบุคคล

ระดับของเหตุละเมิดข้อมูลส่วนบุคคล	เงื่อนไข	
	แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ไม่เกิน 72 ชั่วโมงนับแต่ทราบการละเมิดข้อมูลส่วนบุคคล	**แจ้งเจ้าของข้อมูลส่วนบุคคลถึงการบริการจัดการการละเมิดข้อมูลส่วนบุคคล พร้อมกับการแจ้งแนวทางการเยียวยา**
การละเมิดข้อมูลส่วนบุคคลที่อาจมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✘
การละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✓

โดยสำนักงาน สคส. ได้ออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565[9] ซึ่งประกาศฯ

---

[8] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[9] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/

ดังกล่าวเป็นกฎหมายลำดับรองที่ออกตามความในมาตรา 37(4) ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในข้อ 4 ของประกาศดังกล่าว ได้กำหนดไว้ว่า “เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วยเหตุที่เกิดจากเหตุดังต่อไปนี้[10]

1) การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ

2) การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3) ภัยคุกคามทางไซเบอร์

4) ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น

โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

---

default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf. [2566, 30 มิถุนายน]

[10] ชวิน อุ่นภัทร, ปิยะบุตร บุญอร่ามเรือง. (2564). ***แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.*** รายงานการวิจัย. กรุงเทพฯ: ศูนย์วิจัยกฎหมายและการพัฒนาคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทาลายข้อมูลส่วนบุคคล ทาให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ขั้นตอนในการดำเนินงานเมื่อพบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล[11]

ควรพิจารณากำหนดแนวทางหรือวิธีการในการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ชัดเจน ทั้งนี้ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเองว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยพิจารณา

1) มาตรการเชิงองค์กร (organizational measures)

2) มาตรการเชิงเทคนิค (technical measures) และ

3) มาตรการทางกายภาพ (physical measures)

ในส่วนที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล มีรายละเอียดดังต่อไปนี้[12]

1) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการ

---

[11] สมาคมประกันวินาศภัยไทย. (2566). ***แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.*** กรุงเทพฯ: สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. หน้า 154-170.

[12] เรื่องเดียวกัน, หน้า 154-170.

ป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

2) เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

3) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

4) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

อย่างไรก็ตาม หากการละเมิดข้อมูลส่วนบุคคลไม่ก่อให้เกิดความเสี่ยง หรือไม่มีความเสี่ยง ก็ไม่จำเป็นต้องแจ้งทั้งสำนักงาน และเจ้าของข้อมูลส่วนบุคคล แต่ทั้งนี้ ในทางปฏิบัติอาจเป็นการยากที่ผลของการพิจารณาความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลนั้นเป็นกรณีที่ไม่ก่อให้เกิดผลกระทบใดต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

การประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล

ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้[13]

1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

2) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

---

[13] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

3) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

4) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจากัดต่างๆ ด้วยหรือไม่ เพียงใด

5) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

6) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล

7) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

8) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคลรวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

วิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้[14]

[14] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

1) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคล หรือลักษณะและจำนวนรายการของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

4) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากรกระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคาสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน[15]

กรณีแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าเกิน 72 ชั่วโมง

ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่า 72 ชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยเร็ว ทั้งนี้ ต้องไม่เกิน 15 วันนับแต่ทราบเหตุ

---

[15] ปัทมา มัญชุนากร. (2564). ***ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษา กรณีผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ทั้งนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกำหนดเวลาในมาตรา 37 (4)[16] ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อนึ่ง การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่น ๆ ที่เกี่ยวข้อง นั้น ไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

ข้อยกเว้นการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อประกอบการพิจารณาได้ หากผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าเหตุการละเมิดข้อมูลส่วนบุคคลนั้น

1) ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

2) ข้อมูลส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

3) ข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ

4) เหตุอื่นใดที่เชื่อถือได้

ในการยกข้อยกเว้นดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ให้ข้อมูลหรือส่งเอกสารหรือหลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่น ๆ ที่เกี่ยวข้อง พิจารณาด้วย

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล

[16] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 37(4).

ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำได้โดยไม่ชักช้า[17]

1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน

3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดข้อมูลส่วนบุคคล

4) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหา

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

ทั้งนี้ การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

การลงโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่[18]

มาตรา 79[19] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทาให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

---

[17] ชวิน อุ่นภัทร, ปิยะบุตร บุญอร่ามเรือง. อ้างแล้วเชิงอรรถที่ 10. หน้า 1.

[18] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

[19] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 79.

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาทหรือทั้งจำทั้งปรับ

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ ”

มาตรา 80 บัญญัติว่า “ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นามาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

1) การเปิดเผยตามหน้าที่

2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ”

มาตรา 81[20] บัญญัติว่า “ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือกระทำการของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และละเว้นไม่สั่งการหรือกระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย ”

การลงโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่[21]

มาตรา 82[22] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 23 มาตรา 30 วรรคสี่ มาตรา 39 วรรคหนึ่ง มาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 19 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรคหก หรือไม่ปฏิบัติตาม

---

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

[21] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

[22] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 82.

มาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 83[23] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสามต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท”

มาตรา 84[24] บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสามหรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท”

มาตรา 85[25] บัญญัติว่า “ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 86[26] บัญญัติว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท”

มาตรา 87[27] บัญญัติว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 วรรคหนึ่งหรือวรรคสาม โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท”

มาตรา 88[28] บัญญัติว่า “ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 39 วรรคหนึ่ง ซึ่งได้นามาใช้บังคับโดยอนุโลมตามมาตรา

---

[23] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 83.

[24] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 84.

[25] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 85.

[26] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 86.

[27] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 87.

[28] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 88.

39 วรรคสองและมาตรา 41 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 41 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท”

มาตรา 89[29] บัญญัติว่า “ผู้ใดไม่ปฏิบัติตามคาสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา 75 หรือไม่ปฏิบัติตามมาตรา 76 (1) หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 76 วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท”

มาตรา 90[30] บัญญัติว่า “คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองตามที่กำหนดไว้ในส่วนนี้ ทั้งนี้ ในกรณีที่เห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้

ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือพฤติการณ์ต่าง ๆ ประกอบด้วย ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการกำหนด

ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคาสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ให้คณะกรรมการผู้เชี่ยวชาญมีอานาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

คำสั่งลงโทษปรับทางปกครองและคำสั่งในการบังคับทางปกครอง ให้นำความในมาตรา 74 วรรคหก มาใช้บังคับโดยอนุโลม และให้นำความในมาตรา 74 วรรคสี่ มาใช้บังคับกับการบังคับทางปกครองตามวรรคสามโดยอนุโลม”

1) ผู้ควบคุมข้อมูลส่วนบุคคล

เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่แจ้งให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวมข้อมูลตามมาตรา 23 หรือไม่ดำเนินการตามคำขอเข้าถึงและคำขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าของข้อมูลภายใน 30 วัน ตามมาตรา 30 วรรคสี่ หรือไม่บันทึกรายการเพื่อให้เจ้าของข้อมูลตรวจสอบได้ ตามมาตรา 38 หรือไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา40 วรรคหนึ่ง หรือไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา

---

[29] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 89.

[30] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 86.

41 วรรคสอง หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงาน หรือเลิกสัญญาจ้างเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ตามมาตรา 41 วรรคสาม หรือไม่ขอความยินยอมตามแบบที่กำหนด ตามมาตรา 19 วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอม ตามมาตรา 19 วรรคห้า หรือไม่ปฏิบัติตามมาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 80[31])

เก็บรวบรวม ใช้ เปิดเผยข้อมูล ไม่เป็นไปตามวัตถุประสงค์ที่แจ้งไว้ต่อเจ้าของข้อมูลตามมาตรา 21 เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมายตามมาตรา 22 หรือไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 24 ไม่เก็บข้อมูลจากเจ้าของข้อมูลโดยตรงตามมาตรา 25 วรรคหนึ่ง ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 27 วรรคหนึ่ง บุคคลหรือนิติบุคคลที่ได้รับข้อมูลจากการเปิดเผยของผู้ควบคุมข้อมูลใช้ หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 27 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังต่างประเทศไม่เป็นไปตามหลักเกณฑ์การให้ความคุ้มครองตามที่คณะกรรมการประกาศกำหนดตามมาตรา 28 ผู้ควบคุมข้อมูลส่วนบุคคลยังดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลได้แจ้ง การคัดค้านให้ทราบแล้ว ตามมาตรา 32 วรรคสอง หรือไม่ดำเนินการตามหน้าที่ที่กำหนดไว้ตามมาตรา 36 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท (มาตรา 81[32])

ฝ่าฝืนเก็บรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิตามมาตรา 26 หรือฝ่าฝืนใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 27 วรรคหนึ่ง บุคคล หรือนิติบุคคลที่ได้รับข้อมูลจากการเปิดเผยของผู้ควบคุมข้อมูล ใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 27 วรรคสองหรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท (มาตรา 82)

2) ผู้ประมวลผลข้อมูลส่วนบุคคล

---

[31] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 80.

[32] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 40 วรรคหนึ่ง หรือไม่สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 วรรคสอง หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาจ้างเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ตามาตรา 41 วรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 83)[33]

ไม่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อปูองกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจและจัดทำาเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ตามมาตรา 39 โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรค หนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 36 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 37 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท (มาตรา 84[34])

ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท (มาตรา 85)

3) ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล หรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคล

ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 40 วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 40 วรรคสี่ ต้องโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท (มาตรา 86)

จะเห็นว่าแนวคิดการลงโทษทางอาญากับการลงโทษทางปกครองมีความแตกต่างกัน กล่าวคือ การลงโทษทางอาญาแก่ผู้กระทำาความผิดเป็นสิ่งที่ผู้มีอำานาจในรัฐต้องกระทำาเพื่อรักษาความสงบเรียบร้อยของรัฐเพื่อมิให้มีการล่วงละเมิดสิทธิของผู้อื่นตามกฎหมาย ซึ่งการจะลงโทษทางอาญาเมื่อมีกฎหมายบัญญัติว่าการกระทำาเป็นความผิดและมีบทลงโทษตามกฎหมายซึ่งตามพระราชบัญญัตินี้กำหนดเพียงโทษจำคุกและปรับ นอกจากนี้ การบังคับใช้กฎหมายอาญาใช้บังคับแก่ทุกคนภายในรัฐอย่างเสมอภาค โทษจะรุนแรงมากหรือน้อยขึ้นอยู่กับการกระทำาความผิดในขณะที่การลงโทษทางปกครองมีขอบเขตจำกัดอยู่เฉพาะบุคคลที่ก่อตั้งนิติสัมพันธ์กับฝ่ายปกครอง การจำกัดสิทธิและเสรีภาพหรือการแทรกแซงสิทธิและเสรีภาพของประชาชน โดยรัฐเกิดขึ้นเมื่อบุคคลที่รัฐเข้าไปแทรกแซงหรือจำกัดสิทธิและเสรีภาพนั้น เป็นบุคคลที่ได้รับการคุ้มครองตามกฎหมาย ซึ่งอาจเป็นกรณีเฉพาะรายหรือในลักษณะทั่วไปตามกฎหมาย ซึ่งในการลงโทษทาง

---

[33] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 15. หน้า 1.

[34] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 84.

ปกครองตามพระราชบัญญัตินี้จะเป็นการปรับด้วยจำนวนเงิน โดยประเทศไทยไม่ได้มีการแบ่งแยกแนวคิดโทษปรับทางปกครองและมาตรการบังคับทางปกครองออกจากกันอย่างชัดเจน กล่าวคือ หากเป็นการปรับในเชิงลงโทษทางปกครองจะเป็นการลงโทษบุคคลด้วยการชำระเงินตามที่เจ้าหน้าที่กำหนดเพื่อลงโทษพฤติกรรมผู้กระทำผิดในอดีต แต่หากเป็นการปรับตามมาตรการบังคับทางปกครองจะกำหนดให้บุคคลที่ฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งทางปกครองชำระเงินจนกว่าจะมีการปฏิบัติตามคำสั่งเพื่อบังคับพฤติกรรมของบุคคลที่จะก่อขึ้นต่อไปในอนาคต บทกำหนดโทษทางปกครองตามกฎหมายนี้จึงเป็นการปรับในเชิงลงโทษทางปกครองและมาตรการบังคับทางปกครอง เพื่อบังคับพฤติกรรมของบุคคลขณะเดียวกัน ซึ่งอาจทำให้เกิดความสับสนได้ นอกจากนี้ในการบังคับโทษปรับทางปกครองจะคำนึงถึงเรื่องประโยชน์สาธารณะ จึงไม่อาจอ้างหลักความเสมอภาคในการใช้กฎเกณฑ์เพื่อมาคุ้มครองปัจเจกชนนั้น

โทษที่เกี่ยวข้อง

หากไม่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด อาจถูกโทษปรับทางปกครองไม่เกิน 3 ล้านบาท ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 83[35] ทั้งนี้ ในกรณีที่บริษัทไม่เห็นด้วยกับการลงโทษทางปกครองข้างต้น บริษัทสามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาความของศาลปกครอง

ข้อเสนอแนะ

องค์กรต่าง ๆ ควรจัดทำบันทึกเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุฯ และข้อยกเว้นกรณีที่ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ใช้อ้างอิงไว้ ไม่ว่าองค์กรจะได้รับยกเว้นให้ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลด้วยหรือไม่ก็ตาม เพื่อเป็นหลักฐาน ในกรณีมีข้อพิพาท

โทษทางอาญาของกรรมการหรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล[36]

ในกรณีที่บริษัทกระทำความผิดที่มีโทษทางอาญาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล[37] นอกจากโทษทางอาญาที่บริษัทอาจจะต้องรับแล้ว กรรมการ หรือผู้จัดการ หรือบุคคลซึ่ง

---

[35] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 83.

[36] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 81.

[37] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 79 และ 80.

รับผิดชอบในการดำเนินงานของบริษัทก็ต้องรับผิดในโทษอาญาเช่นเดียวกับบริษัทด้วย หากพิสูจน์ว่า การกระทำผิดดังกล่าวมีองค์ประกอบ ดังต่อไปนี้ ได้[38]

ผู้กระทำความผิด

ก) กรรมการของบริษัท

ข) ผู้จัดการของบริษัท หรือ

ค) บุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทการกระทำความผิด

ก) การสั่งการ หรือการกระทำการของกรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท หรือ

ข) การละเว้นไม่สั่งการ หรือไม่กระทำการ ในกรณีที่กรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทมีหน้าที่ต้องสั่งการหรือกระทำการ

และการกระทำตาม ก. หรือ ข. นั้นเป็นเหตุให้บริษัทกระทำความผิด

ตัวอย่าง

ผู้รับมอบอำนาจบริษัทสั่งให้นำข้อมูลส่วนบุคคลที่บริษัท เก็บรวบรวมมาภายใต้วัตถุประสงค์ในการพิจารณารับประกันภัยรถยนต์ ไปใช้ประมวลผลข้อมูลภายใต้วัตถุประสงค์เพื่อทำกิจกรรมส่งเสริมการขาย โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่นนี้เป็นกรณีที่บริษัท ผู้ควบคุมข้อมูลส่วนบุคคลกระทำความผิดโดยคำสั่งของบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท ดังนั้น ในกรณีนี้ทั้งบริษัท และผู้รับมอบอำนาจบริษัทจะต้องรับโทษทางอาญาที่เกี่ยวข้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

โทษทางปกครอง

นอกจากโทษทางปกครองที่กำหนดไว้สำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือตัวแทนของบุคคลดังกล่าว ตามที่ได้อธิบายไว้ที่ข้างต้นแล้ว บุคคลใด ๆ (ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงกรรมการ หรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท) ที่ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือเจ้าพนักงานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อาจต้องรับผิดหากบุคคลดังกล่าวกระทำการดังต่อไปนี้[39]

---

[38] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

[39] เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก: https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%

1) ไม่ปฏิบัติตามคำสั่งให้ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมทั้งไม่มาชี้แจงข้อเท็จจริงต่อคณะกรรมการผู้เชี่ยวชาญ

2) ไม่มาให้ข้อมูล หรือไม่ส่งเอกสารหรือหลักฐาน เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่พนักงานเจ้าหน้าที่ตามหนังสือที่ได้แจ้งไปภายใต้อำนาจหน้าที่

3) ไม่อำนวยความสะดวกตามสมควรแก่พนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่

ตัวอย่าง

1) ในกรณีที่พนักงานเจ้าหน้าที่ได้รับคำสั่งจากศาลที่มีเขตอำนาจ เพื่อเข้าตรวจสอบและรวบรวมข้อเท็จจริง โดยยึด หรืออายัดหลักฐานที่พนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่าใช้เพื่อกระทำความผิด เช่นนี้ หากผู้จัดการสาขา ขัดขวางไม่ให้เจ้าพนักงานยึดเอาหลักฐานนั้นไป ผู้จัดการสาขาคนดังกล่าวอาจจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

2) ในกรณีที่คณะกรรมการผู้เชี่ยวชาญสั่งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของบริษัทไปให้รายละเอียดเรื่องที่มีผู้ร้องเรียนบริษัท เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แต่ DPO ไม่ไปให้ข้อเท็จจริงโดยไม่มีเหตุผล ดังนี้ DPO อาจจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

ข้อสังเกต

1) พนักงานเจ้าหน้าที่ จะเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลได้จะต้องเป็นไปตามเงื่อนไขที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด กล่าวคือ

2) ต้องมีคำสั่งอนุญาตของศาลที่มีเขตอำนาจ

3) เข้าไประหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก หรือในเวลาทำการของสถานที่นั้น

4) แสดงบัตรประจำตัวต่อผู้ที่เกี่ยวข้อง

โทษทางปกครองในกรณีนี้ สามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาคดีปกครอง ตามลำดับ

A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/ [2566,7 กรกฎาคม]

3.1.2 ประมวลกฎหมายแพ่งและพาณิชย์

ตามประมวลกฎหมายแพ่งและพาณิชย์ของไทยนั้น ได้บัญญัติหลักเกณฑ์เกี่ยวกับความรับผิดทางละเมิดไว้ในบรรพ 2 หนี้ ลักษณะ 5 ละเมิด (มาตรา 420 - 452) ซึ่งในมาตรา 420[40] บัญญัติว่า "ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น" ซึ่งหลักกฎหมายเบื้องต้นในการพิจารณาว่าการกระทำใดเป็นการละเมิดหรือไม่นั้น จะต้องพิจารณาจากองค์ประกอบได้ดังต่อไปนี้

1) มีการกระทำ หมายถึง การเคลื่อนไหวร่างกายโดยรู้สำนึกในการเคลื่อนไหวนั้นและอยู่ในบังคับของจิตใจผู้กระทำ และรวมถึงการงดเว้นการกระทำที่ตนมีหน้าที่ตามกฎหมายที่ต้องกระทำและการงดเว้นนั้นเป็นเหตุให้เกิดความเสียหายขึ้น

2) โดยจงใจหรือประมาทเลินเล่อ

โดยจงใจ หมายถึง รู้สำนึกถึงผลหรือความเสียหายจากการกระทำของตนโดยประมาทเลินเล่อ หมายถึง เป็นการกระทำโดยปราศจากความระมัดระวัง ซึ่งบุคคลในภาวะเช่นนั้นจำต้องมีโดยต้องเปรียบเทียบกับบุคคลที่ต้องมีความระมัดระวังตามพฤติการณ์ และตามฐานะในสังคมเช่นเดียวกับผู้กระทำความเสียหาย

3) โดยผิดกฎหมาย เป็นการกระทำโดยไม่มีอำนาจหรือไม่มีสิทธิหรือโดยมิชอบด้วยกฎหมาย (unlawful) และรวมความถึงการใช้อำนาจที่มีอยู่เกินส่วนหรือใช้อำนาจตามกฎหมายเพื่อกลั่นแกล้งผู้อื่น

4) เกิดความเสียหายแก่บุคคลอื่น

ความเสียหายนั้นจะเป็นความเสียหายที่เกิดแก่ชีวิต ร่างกาย อนามัยเสรีภาพ ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ได้ แต่ต้องเป็นความเสียหายที่แน่นอนไม่ว่าจะเกิดขึ้นแล้วในปัจจุบันหรือจะเกิดขึ้นในอนาคตก็จะต้องเป็นความเสียหายที่จะเกิดขึ้นอย่างแน่นอน และความเสียหายจะต้องเกิดจากผลโดยตรงของผู้กระทำด้วย

ทั้งนี้ จะต้องครบองค์ประกอบดังกล่าวข้างต้นทุกข้อ จึงจะถือว่าเป็นการกระทำ "ละเมิด" ซึ่งผู้ทำละเมิดจะต้องรับผิดชดใช้ค่าสินไหมทดแทนให้แก่ผู้เสียหาย

การคุ้มครองข้อมูลส่วนบุคคลตามหลักกฎหมายแพ่งและพาณิชย์นั้นเป็นการมุ่งคุ้มครองในลักษณะที่จะเป็นการเยียวยาแก้ไขในสิ่งที่บุคคลผู้นั้นได้กระทำลงไปแล้ว โดยให้มีการใช้ค่าสินไหมทดแทนแก่บุคคลผู้ที่ได้รับความเสียหายนั้นๆ โดยมีมาตรา 420 เป็นหลักการทั่วไปในการให้ความคุ้มครองสิทธิส่วนบุคคล

---

[40] ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 420.

อย่างไรก็ดี นอกจากการคุ้มครองสิทธิส่วนบุคคล ตามมาตรา 420 แล้วยังมีการคุ้มครองสิทธิส่วนบุคคลตามมาตรา 423[41] อีกด้วย บัญญัติไว้ว่า “ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสาส์นอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสาส์นนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสาส์นเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่”

ความรับผิดทางแพ่ง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนด ความรับผิดทางแพ่งไว้ในมาตรา 77 เป็นพิเศษแตกต่างไปจากหลักกฎหมายละเมิดทั่วไปตามประมวลกฎหมายแพ่งและพาณิชย์ ดังนั้น ในส่วนนี้จึงจะอธิบายรายละเอียด เช่น องค์ประกอบ ข้อยกเว้น ผลของการฝ่าฝืนหรือไม่ปฏิบัติตาม และอายุความของมาตราดังกล่าว ดังนี้

องค์ประกอบของความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77[42]

1) ผู้กระทำละเมิดมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

2) บุคคลดังกล่าวดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การดำเนินการอันฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

โดยมีข้อแตกต่างของความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77[43] กับหลักกฎหมายละเมิดทั่วไปตามประมวลกฎหมายแพ่งและพาณิชย์ คือ ความรับผิดทางแพ่งข้างต้น ไม่จำเป็นต้องพิสูจน์ว่าการกระทำฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่

---

[41] ประมวลกฎหมายแพ่งและพาณิชย์. มาตรา 423.

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 77.

[43] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 77.

ข้อยกเว้นความรับผิด

1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย

2) ความเสียหายเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

3) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ตัวอย่าง

เจ้าพนักงานควบคุมโรคติดต่อ มีหนังสือให้บริษัทเปิดเผยข้อมูลส่วนบุคคลของผู้เอาประกันภัยอุบัติเหตุการเดินทาง ที่เดินทางไปและกลับจากประเทศที่เป็นกลุ่มเสี่ยงโรคติดต่ออันตราย เพื่อใช้ประกอบการควบคุมโรคติดต่ออันตราย ตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 กรณีนี้แม้ว่าบริษัทจะไม่ได้ปฏิบัติตามหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด บริษัทก็ได้รับยกเว้นความรับผิดทางแพ่ง

ผลของการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เมื่อผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ฝ่าฝืนหรือไม่ปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องรับผิดทางแพ่งและต้องชำระค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล

ทั้งนี้ ค่าสินไหมทดแทน หมายความรวมถึง ค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

นอกจากนี้ ค่าสินไหมทดแทนข้างต้น ที่เป็นค่าสินไหมทดแทนที่แท้จริงแล้ว ศาลยังมีอำนาจกำหนดค่าสินไหมทดแทนเพื่อการลงโทษ[44] ตามที่ศาลเห็นสมควรด้วย แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง โดยในการกำหนดค่าสินไหมทดแทนเชิงการลงโทษนั้น ศาลจะคำนึงถึงพฤติการณ์ต่าง ๆ เช่น [45]

1) ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ

2) ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ

3) สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

---

[44] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 78.

[45] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

4) การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น

5) การที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

ข้อสังเกต

ค่าสินไหมทดแทนสำหรับความรับผิดทางแพ่งภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลนี้ อาจจะมีปัญหาในทางปฏิบัติเกี่ยวกับการคำนวณค่าสินไหมทดแทน เพราะหากความเสียหายที่เกิดขึ้น เกิดแต่เพียงความเสียหายจากการละเมิดสิทธิความเป็นส่วนตัว แต่ไม่ได้เกิดความเสียหายต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล จะเป็นการยากที่จะคำนวณค่าสินไหมทดแทนเป็นตัวเงิน

อายุความฟ้องเรียกค่าสินไหมทดแทน[46]

สิทธิค่าเสียหายในทางแพ่งนี้จะหมดอายุความเมื่อพ้น 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิด หรือเมื่อพ้น 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

ในส่วนนี้จะกล่าวถึงหลักกฎหมายระหว่างประเทศและต่างประเทศ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดาที่เกี่ยวข้องกับการคุ้มครองการจัดเก็บข้อมูลส่วนบุคคล รวมถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ได้แก่ กฎหมายที่คุ้มครองข้อมูลส่วนบุคคลโดยตรง และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไป โดยมีรายละเอียดดังต่อไปนี้

3.2.1 กฎหมายของสหภาพยุโรป General data Protection Regulation (GDPR)

หลักการคุ้มครองข้อมูลตามกฎหมาย General Data Protection Regulation 2016 ที่สำคัญมีดังนี้[47]

1) ขอบเขตการบังคับใช้เชิงพื้นที่กฎหมาย GDPR บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ใน EU ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน กล่าวคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลใน EU ไม่ว่าการประมวลผลจะทำใน EU หรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง EU

---

[46] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. มาตรา 78.

[47] อมรรัตน์ อริยะชัยประดิษฐ์. อ้างแล้วเชิงอรรถที่ 2. หน้า 129-141.

และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นใน EU หากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิก EU (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนใน EU ด้วย

2) บทลงโทษ กรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4 % ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่น กรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบ การไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำ Privacy Impact Assessment

3) การให้ความยินยอม หลักความยินยอมมีความเข้มแข็งมากขึ้นในรูปแบบที่เข้าใจได้และสามารถเข้าถึงได้สะดวก (Intelligible and easily access) ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอคำยินยอม การขอความยินยอมต้องมีความชัดเจนและใช้ภาษาที่ง่ายต่อการเข้าใจ นอกจากนี้ การยกเลิกการให้ความยินยอมต้องก็ต้องดำเนินการได้ด้วยความสะดวก

3.2.1.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของสหภาพยุโรป (EU: European Union)

General Data Protection Regulation (หรือที่เรียกว่า GDPR) เป็นกฎหมายของสหภาพยุโรป (EU: European Union) ที่มีวัตถุประสงค์เพื่อให้ บริษัท หรือธุรกิจที่จัดเก็บและจัดการข้อมูลส่วนบุคคลจะต้องเพิ่มมาตรการการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลตามฐานที่ชอบด้วยกฎหมาย

3.2.1.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล หรือ Data breach notification ถือเป็นหน้าที่ตามกฎหมายที่สำคัญของผู้ควบคุมข้อมูลส่วนบุคคลในทุก ๆ ประเทศ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้วางหลักในเรื่องการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลไว้ในทิศทางเดียวกันกับ GDPR[48]

1) ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงหลังจากได้รับเรื่องแล้ว การแจ้งในกรณีที่มีการ

---

[48] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

ละเมิดข้อมูลส่วนบุคคลต้องแจ้งต่อหน่วยงานที่มีหน้าที่กำกับดูแลภายใต้อำนาจตามมาตรา 55 เว้นแต่การละเมิดข้อมูลส่วนบุคคลจะไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ในกรณีที่การแจ้งเตือนไปยังหน่วยงานที่มีหน้าที่กำกับดูแล ไม่ได้ดำเนินการภายใน 72 ชั่วโมงจะต้องมีให้เหตุผลสำหรับเหตุที่เกิดความล่าช้า

2) หน่วยประมวลผลจะแจ้งให้ผู้ตรวจสอบทราบโดยไม่ชักช้าหลังจากรับเหตุการละเมิดข้อมูลส่วนบุคคล

3) การแจ้งกรณีที่มีการละเมิดข้อมูลส่วนบุคคลตามข้อ 1 จะต้องประกอบด้วย[49]

1) อธิบายลักษณะของการละเมิดข้อมูลส่วนบุคคล รวมถึงการให้ข้อมูลที่เกี่ยวข้อง ควรระบุรายละเอียดหรือสามารถจำแนกเป็นหมวดหมู่หรือระบุจำนวนตัวเลขได้โดยประมาณ

2) ระบุชื่อและรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลหรือวิธีติดต่ออื่น ๆ ที่สามารถรับข้อมูลเพิ่มเติมได้

3) อธิบายถึงผลที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

4) อธิบายถึงมาตรการที่ดำเนินการหรือเสนอให้ผู้ตรวจสอบดำเนินการ เพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลรวมถึงมาตรการที่เหมาะสมเพื่อบรรเทาผลกระทบที่อาจจะเกิดขึ้น

5) ควรให้ข้อมูลในขณะที่เกิดเหตุเท่าที่จะพอได้ในเวลานั้น เพื่อจะสามารถดำเนินการในขั้นตอนต่อไปได้โดยไม่ล่าช้า

6) ผู้ตรวจสอบจะต้องบันทึกข้อมูลการละเมิดข้อมูลส่วนบุคคล ซึ่งประกอบด้วยข้อเท็จจริงที่เกี่ยวข้องกับการละเมิดผลกระทบและการดำเนินการแก้ไข และนำส่งเอกสารอื่น ๆที่เกี่ยวข้องให้หน่วยงานที่กำกับดูแลสามารถตรวจสอบได้ [50]

ข้อมูลส่วนบุคคลที่ถูกละเมิด

---

[49] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

[50] กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-union-eu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222 [2566,9 กรกฎาคม]

1) เมื่อการละเมิดข้อมูลส่วนบุคคลมีแนวโน้มที่จะส่งผลให้มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ผู้ตรวจสอบจะต้องแจ้งข้อมูลการละเมิดให้ทราบโดยไม่ชักช้า

2) การแจ้งข้อมูลในทราบตามข้อ 1 จะต้องอธิบายในภาษาที่ชัดเจนและเข้าใจง่าย ลักษณะของการละเมิดข้อมูลส่วนบุคคลและจะต้องมีข้อมูลอย่างน้อย ตามมาตรการในข้อ 3

3) การสื่อสารให้ทราบเรื่องข้อมูลตามข้อ 1 จะไม่จำเป็นหากตรงตามเงื่อนไขใด ๆ ต่อไปนี้

ผู้ตรวจสอบ องค์กร ได้ใช้มาตรการป้องกันทางเทคนิคที่เหมาะสมและมาตรการเหล่านั้นถูกนำไปใช้กับข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิด โดยเฉพาะอย่างยิ่งสิ่งที่ทำให้ข้อมูลส่วนบุคคลไม่สามารถเข้าใจได้สำหรับบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึง เช่น การเข้าใช้รหัส ผู้ตรวจสอบจะต้องดำเนินตามมาตรการ ซึ่งทำให้มั่นใจได้ว่าจะไม่เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่ระบุไว้ในข้อ ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล เจ้าของข้อมูลควรจะต้องมีการสื่อสารต่อสาธารณชนหรือมาตรการที่ได้รับหลังการแจ้งเหตุเพื่อให้ผู้อื่นได้รับความคุ้มครองอย่างมีประสิทธิภาพและเท่าเทียมกัน และหากผู้ตรวจสอบไม่แจ้งการละเมิดข้อมูลส่วนบุคคลไปยังหน่วยงานที่กำกับดูแลได้พิจารณาซึ่งจะทำให้เกิดความเสี่ยงสูง ที่อาจจะต้องให้ดำเนินการหรือให้เป็นไปตามเงื่อนไขในข้อ [51]

---

[51] GDPR Chapter 4 Controller and processor

Art. 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

เมื่อบริษัทฯ พบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลข้างต้น การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยที่การดำเนินการตรวจสอบข้อเท็จจริงของการละเมิดข้อมูลส่วนบุคคลตามที่ระบุไว้ในกฎหมายลำดับรองนั้นจะต้องดำเนินการภายในระยะเวลา 72 ชั่วโมงด้วยเช่นกัน อย่างไรก็ดีตามหลักการที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR[52] มีการขยายความชัดเจนในเรื่องนี้ออกไปอีก โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ช่วงระยะเวลาไม่นานในการตรวจสอบข้อเท็จจริงและทำการยืนยันว่าเหตุละเมิดข้อมูลส่วนบุคคลที่พบหรือรับแจ้งนั้นได้เกิดขึ้นจริงหรือไม่ และภายในช่วงระยะเวลาไม่นานนั้นยังถือไม่ได้ว่าบริษัทฯได้ 'รับทราบ' การละเมิดข้อมูลส่วนบุคคลแล้ว

ดังนั้น จากการพิจารณาการตีความ GDPR ดังกล่าว บริษัทฯ ย่อมสามารถจัดให้มีระบบงานหรือขั้นตอนภายในซึ่งมีกระบวนการที่ใช้ระยะเวลาไม่นานนัก โดยคำนึงถึงโครงสร้างองค์กรของตนเพื่อการตรวจสอบยืนยันการเกิดเหตุตามข้อเท็จจริงดังกล่าว และช่วงเวลานั้นบริษัทฯ ยังไม่สามารถพิจารณาได้ว่าได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเพื่อเริ่มนับกำหนดระยะเวลา 72 ชั่วโมงที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ และหน่วยงานรัฐที่เกี่ยวข้อง[53]

3.2.2 กฎหมายของสาธารณรัฐสิงคโปร์ (The Personal Data Protection Act.)

3.2.2.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศสิงคโปร์

ประเทศสิงคโปร์มีการบังคับใช้รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2555 (Personal Data Protection Act 2012) โดยได้ผ่านการรับรองจากรัฐสภาเมื่อวันที่ 15 กุมภาพันธ์ 2555 และผ่านการรับรองจากประธานาธิบดีเมื่อวันที่ 20 พฤศจิกายน พ.ศ. 2555

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA ตั้งแต่ปี 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี 2556

4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [2]That documentation shall enable the supervisory authority to verify compliance with this Article.

Art. 34 GDPR Communication of a personal data breach to the data subject

[52] Guidelines 9/2022 on personal data breach notification under GDPR

[53] สมาคมประกันวินาศภัยไทย. อ้างแล้วเชิงอรรถที่ 11. หน้า 154-170.

2) ตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ PDPC ให้คำปรึกษา รวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล ช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มที่

ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสาธารณรัฐสิงคโปร์ บังคับใช้เฉพาะภาคเอกชนเท่านั้น

1) การขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต

2) คุ้มครองข้อมูลส่วนบุคคลต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมาย

3) ให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

สำหรับประเทศอย่างสาธารณรัฐสิงคโปร์ นั้น ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA เช่นเดียวกับของประเทศไทย ซึ่งที่นี่ประกาศใช้ตั้งแต่ปี 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี 2556 โดยมีระยะเวลาเตรียมความพร้อมถึง 18 เดือนด้วยกัน โดยระหว่างนั้นได้มีการจัดอบรม เผยแพร่ความรู้ เพื่อเตรียมความพร้อมให้กับภาคเอกชนและประชาชนอย่างต่อเนื่อง เพื่อสร้างความเข้าใจอันดีเกี่ยวกับข้อดีของ PDPA ที่จะมีผลบังคับใช้ภายในประเทศ

นอกจากนี้ สาธารณรัฐสิงคโปร์ยังมีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ PDPC ซึ่งถือเป็นอีกหนึ่งข้อดีของการนำ PDPA เข้ามาบังคับใช้ โดย PDPC จะเข้ามามีบทบาทในเรื่องการให้คำปรึกษา รวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุเอาไว้ นอกจากนี้ยังจะเป็นการช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มที่

ข้อกำหนดที่น่าสนใจของ PDPA

1) เป็นการบังคับใช้เฉพาะภาคเอกชนเท่านั้น

2) การขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะเป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต

3) การความคุ้มครองข้อมูลส่วนบุคคลจะต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมาย

4) ให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์[54]

3.2.2.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

สิทธิในการร้องเรียนต่อคณะกรรมการด้านข้อมูลส่วนบุคคลเป็นมาตรการเยียวยาเจ้าของข้อมูล จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย[55]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสาธารณรัฐสิงคโปร์ หรือไม่ ถือว่าอยู่ภายใต้กฎหมายดังกล่าว

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลต้องได้รับความยินยอม จากเจ้าของข้อมูลก่อนทำการเก็บบันทึก การใช้ และการเปิดเผยข้อมูลส่วนบุคคล และจะต้องใช้ข้อมูลนั้น เพื่อวัตถุประสงค์ตามที่แจ้งเท่านั้น รวมถึงจะต้องจัดให้เจ้าของข้อมูลเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลได้ และจะต้องยุติหรือหยุดการจัดเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็น

กรณีของสาธารณรัฐสิงคโปร์ ในหลักของความยินยอม กฎหมายกำหนดให้การทำความยินยอมควรจะทำ เป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ และเจ้าของข้อมูล

---

[54] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

[55] ลัฐกา เนตรทัศน์. (2566). ***สรุปภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย สิงคโปร์ และฟิลิปปินส์.*** (ออนไลน์). เข้าถึงได้จาก: https://lawforasean.krisdika.go.th/File/files/dataprotectionoverview.pdf

สามารถถอนหรือยกเลิกการให้ ความยินยอมในการใช้ข้อมูลเมื่อใดก็ได้ด้วยการแจ้งต่อองค์กรที่จัดเก็บข้อมูลประกอบเหตุผลในการถอน ความยินยอม[56]

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลจะต้อง มีการจัดการเพื่อรักษาความปลอดภัยอย่างเหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลและเพื่อป้องกัน การเข้าถึง การจัดเก็บ การใช้การเปิดเผย การคัดลอก การแก้ไข การลบข้อมูลหรือความเสี่ยงอื่นในทำนอง เดียวกัน ซึ่งกระทำโดยมิชอบด้วยกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2555 (Personal Data Protection Act 2012)

การแจ้งเตือนการละเมิดข้อมูล

“บุคคลที่ได้รับผลกระทบ” หมายถึง บุคคลใดๆ ที่ข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิดข้อมูลที่เกี่ยวข้อง

“การละเมิดข้อมูล” ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล หมายถึง

(ก) การเข้าถึง รวบรวม ใช้ เปิดเผย คัดลอก แก้ไข หรือกำจัดข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือ

(ข) การสูญเสียสื่อหรืออุปกรณ์จัดเก็บข้อมูลใด ๆ ที่ข้อมูลส่วนบุคคลถูกเก็บไว้ในสถานการณ์ที่การเข้าถึงโดยไม่ได้รับอนุญาต การรวบรวม การใช้ การเปิดเผย การคัดลอก การปรับเปลี่ยนหรือการกำจัดข้อมูลส่วนบุคคลที่มีแนวโน้มจะเกิดขึ้น[57]

การละเมิดข้อมูลที่แจ้งให้ทราบ[58]

การละเมิดข้อมูล คือ การละเมิดข้อมูลที่สามารถแจ้งได้หากการละเมิดข้อมูล

---

[56] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

[57] Interpretation of this Part26A. In this Part, unless the context otherwise requires

“affected individual” means any individual to whom anypersonal data affected by a data breach relates;

“data breach”, in relation to personal data, means

[58] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

1) ส่งผลให้เกิดหรือมีแนวโน้มที่จะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ หรือเป็นหรือมีแนวโน้มว่าจะมีขนาดที่มีนัยสำคัญ

2) โดยไม่จำกัดส่วนย่อยการละเมิดข้อมูลจะถือว่าส่งผลเสียต่อบุคคลอย่างมีนัยสำคัญหากการละเมิดข้อมูลเกี่ยวข้องกับข้อมูลส่วนบุคคลที่กำหนดไว้หรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลนั้น หรือในกรณีอื่น ๆ ที่กำหนด

3) โดยไม่จำกัดส่วนย่อย (1)(b) การละเมิดข้อมูลถือว่ามีนัยสำคัญหากการละเมิดข้อมูลส่งผลกระทบไม่น้อยกว่าจำนวนที่กำหนดของผู้ได้รับผลกระทบ หรือ

(b) ในกรณีอื่น ๆ ที่กำหนด

4) แม้จะมีส่วนย่อย (1) (2) และ (3) การละเมิดข้อมูลที่เกี่ยวข้องกับการเข้าถึง รวบรวม ใช้ เปิดเผย คัดลอกหรือแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตเฉพาะภายในองค์กรจะถือว่าไม่สามารถแจ้งได้ การละเมิดข้อมูล[59]

หน้าที่ดำเนินการประเมินการละเมิดข้อมูล

1) ส่วนนี้ใช้กับการละเมิดข้อมูลที่เกิดขึ้นในหรือหลังวันที่ 1 กุมภาพันธ์ พ.ศ. 2564

2) ภายใต้หัวข้อย่อย (3) เมื่อองค์กรมีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลซึ่งส่งผลกระทบต่อข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรืออยู่ภายใต้การควบคุมขององค์กร องค์กรต้องดำเนินการประเมินอย่างสมเหตุสมผลและรวดเร็วว่า การละเมิดข้อมูลถือเป็นการละเมิดข้อมูลที่สามารถแจ้งได้

3) เมื่อตัวกลางข้อมูล (นอกเหนือจากตัวกลางข้อมูลที่กล่าวถึงในมาตรา 26E) มีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลเกิดขึ้นเกี่ยวกับข้อมูลส่วนบุคคลที่ตัวกลางข้อมูลกำลังดำเนินการในนามของและเพื่อวัตถุประสงค์ขององค์กรอื่น

(ก) ตัวกลางข้อมูลต้องแจ้งให้องค์กรอื่นทราบถึงการละเมิดข้อมูลโดยไม่ชักช้า และ

(ข) ว่าองค์กรอื่นจะต้องดำเนินการเมื่อได้รับแจ้งจากตัวกลางข้อมูล

(ค) ว่าองค์กรอื่นจะต้องดำเนินการประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่ได้รับแจ้งหรือไม่ เมื่อได้รับแจ้งจากตัวกลาง

(4) องค์กรต้องดำเนินการประเมินตามข้อ (2) หรือ (3)(b) ตามข้อกำหนดที่กำหนดไว้[60]

---

[59] Notifiable data breaches Personal Data Protection Act 2012 26B.

(1) A data breach is a notifiable data breach if the data breach

[60] Duty to conduct assessment of data breach26C.

หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล มีรายละเอียดที่ต้องแจ้งดังนี้[61]

1) ในกรณีที่องค์กรประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่แจ้งได้ องค์กรต้องแจ้งให้คณะกรรมการทราบทันทีที่ทำได้ แต่ไม่ช้ากว่า 3 วัน ตามปฏิทินหลังจากวันที่องค์กรทำการประเมินนั้น

2) ภายใต้หัวข้อย่อย (5), (6) และ (7) ในหรือหลังจากแจ้งต่อคณะกรรมาธิการตามอนุมาตรา (1) แล้ว องค์กรต้องแจ้งบุคคลที่ได้รับผลกระทบแต่ละรายที่ได้รับผลกระทบจากการละเมิดข้อมูลที่ต้องแจ้งให้ทราบซึ่งกล่าวถึงในลักษณะใด ๆ ที่สมเหตุสมผลในสถานการณ์

3) ประกาศตามอนุมาตรา (1) หรือ (2) ต้องมีข้อมูลทั้งหมดที่แจ้งต่อคณะกรรมการหรือผู้ได้รับผลกระทบ (แล้วแต่กรณี) เท่าที่ทราบและความเชื่อขององค์กรอย่างดีที่สุด กำหนดไว้เพื่อการนี้

4) การแจ้งตามอนุมาตรา (๑) ต้องทำตามแบบและยื่นตามที่คณะกรรมการกำหนด

5) หมวดย่อย (2) ใช้ไม่ได้กับองค์กรที่เกี่ยวข้องกับบุคคลที่ได้รับผลกระทบหากองค์กร

(a) ในหรือหลังจากการประเมินว่าการละเมิดข้อมูลเป็นการละเมิดข้อมูลที่สามารถแจ้งได้ ดำเนินการใดๆ ตามข้อกำหนดที่กำหนดไว้ ซึ่งทำให้ไม่น่าเป็นไปได้ที่การละเมิดข้อมูลที่แจ้งจะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ หรือ

(b) ได้ดำเนินการ ก่อนเกิดการละเมิดข้อมูลที่สามารถแจ้งได้ มาตรการทางเทคโนโลยีใดๆ ที่ทำให้ไม่น่าเป็นไปได้ที่การละเมิดข้อมูลที่แจ้งได้จะส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคลที่ได้รับผลกระทบ

6) องค์กรต้องไม่แจ้งบุคคลที่ได้รับผลกระทบตามอนุมาตรา (2) หาก

(ก) หน่วยงานบังคับใช้กฎหมายที่กำหนดเพื่อสั่ง หรือ

(b) คณะกรรมาธิการสั่งเช่นนั้น

7) ในการสมัครเป็นลายลักษณ์อักษรขององค์กร คณะกรรมาธิการอาจสละข้อกำหนดในการแจ้งให้บุคคลที่ได้รับผลกระทบทราบภายใต้มาตราย่อย (2) ภายใต้เงื่อนไขใด ๆ ที่คณะกรรมการเห็นสมควร

8) องค์กรไม่ได้แจ้งต่อคณะกรรมการตามอนุมาตรา (1) หรือบุคคลที่ได้รับผลกระทบตามอนุมาตรา (2) ด้วยเหตุผลเพียงอย่างเดียวเท่านั้น ให้ถือว่าละเมิด

---

[61] ลัฐกา เนตรทัศน์. (2566). ***สรุปภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย สิงคโปร์ และฟิลิปปินส์.*** (ออนไลน์). เข้าถึงได้จาก: https://lawforasean.krisdika.go.th/File/files/dataprotectionoverview.pdf

(ก) หน้าที่หรือภาระผูกพันใด ๆ ตามกฎหมายที่เป็นลายลักษณ์อักษรหรือหลักนิติธรรม หรือสัญญาใด ๆ เกี่ยวกับความลับหรือข้อจำกัดอื่น ๆ ในการเปิดเผยข้อมูล หรือ

(b) กฎความประพฤติทางวิชาชีพใด ๆ ที่ใช้กับองค์กร

9) ส่วนย่อย (1) และ (2) ใช้ควบคู่ไปกับภาระผูกพันขององค์กรภายใต้กฎหมายที่เป็นลายลักษณ์อักษรอื่น ๆ เพื่อแจ้งให้บุคคลอื่น (รวมถึงหน่วยงานสาธารณะใด ๆ) ทราบถึงการละเมิดข้อมูลหรือเพื่อให้ข้อมูลใด ๆ ที่เกี่ยวข้องกับ การละเมิดข้อมูล

ภาระหน้าที่ของตัวกลางข้อมูลของหน่วยงานของรัฐ

1) เป็นตัวกลางในการประมวลผลข้อมูลส่วนบุคคลในนามของและเพื่อวัตถุประสงค์ของหน่วยงานสาธารณะ และ

2) มีเหตุผลที่จะเชื่อว่ามีการละเมิดข้อมูลเกิดขึ้นเกี่ยวกับข้อมูลส่วนบุคคลนั้น องค์กรต้องแจ้งให้หน่วยงานสาธารณะทราบถึงการละเมิดข้อมูลโดยไม่ชักช้า[62]

3.2.3 กฎหมายของประเทศญี่ปุ่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคงของประเทศญี่ปุ่น หรือที่เรียกว่า “Act on the Protection of Personal Information (APPI)” เวอร์ชันเริ่มต้นซึ่งพัฒนาขึ้นในปี 2546 เป็นหนึ่งในกฎหมายคุ้มครองข้อมูลฉบับแรกที่เริ่มใช้ในเอเชีย APPI ได้รับการแก้ไขอย่างมีนัยสำคัญในปี 2559 และฉบับแก้ไขมีผลบังคับใช้ในวันที่ 30 พฤษภาคม 2560 หนึ่งปีต่อมาในวันที่ 25 พฤษภาคม 2561 ซึ่ง GDPR มีผลบังคับใช้

การอภิปรายเกี่ยวกับการตัดสินใจที่เพียงพอเริ่มขึ้นหลังจากนั้นไม่นานระหว่างคณะกรรมาธิการยุโรป และคณะกรรมาธิการการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่น หลังจากนั้นก็เริ่มออกกฎหมายเพิ่มเติมเพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคล เมื่อวันที่ 23 มกราคม 2019 ญี่ปุ่นกลายเป็นประเทศแรกในเอเชียที่ได้รับสถานะความเพียงพอจากคณะกรรมาธิการยุโรป การตัดสินใจนี้ระบุว่า APPI ร่วมกับบทบัญญัติที่เกี่ยวข้องอื่นๆ ในกฎหมายญี่ปุ่น ให้การคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกันโดยพื้นฐาน เช่นเดียวกับ GDPR

---

[62] Personal Data Protection Act 2012: Obligations of data intermediary of public agency 26E. Where an organisation

(a) is a data intermediary processing personal data on behalf of and for the purposes of a public agency; and

(b) has reason to believe that a data breach has occurred in relation to that personal data, the organisation must, without undue delay, notify the public agency of the occurrence of the data breach.

โดยกฎหมายทั้งสองฉบับมีข้อกำหนดสำหรับข้อมูลพิเศษหรือข้อมูลที่ละเอียดอ่อน กำหนดให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่สามารถใช้ในการระบุตัวบุคคล รวมถึงขอบเขตนอกอาณาเขต และกำหนดข้อผูกพันสำหรับผู้ปฏิบัติงานหรือผู้ควบคุม/ผู้ประมวลผลที่จัดการข้อมูลส่วนบุคคล นอกจากนี้ APPI และ GDPR ให้รายละเอียดเกี่ยวกับสิทธิ์ของเจ้าของข้อมูล รวมถึงสิทธิ์ในการลบ การได้รับแจ้ง การคัดค้าน การเข้าถึงข้อมูลส่วนบุคคล และการระบุความยินยอมเป็นหลักการสำคัญ กฎหมายทั้งสองยังกำหนดให้มีหน่วยงานกำกับดูแลและการออกมาตรการลงโทษทางการเงิน

อย่างไรก็ตาม ในขณะเดียวกัน APPI และ GDPR มีความแตกต่างกันอย่างมีนัยสำคัญ ในกรณีที่ GDPR ระบุความแตกต่างระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผล APPI จะอ้างถึงเฉพาะผู้ประกอบการธุรกิจที่จัดการข้อมูลส่วนบุคคลเท่านั้น GDPR แสดงคำจำกัดความโดยละเอียดของการประมวลผล แต่ APPI ชี้แจงเฉพาะว่านำไปใช้กับข้อมูลส่วนบุคคล ฐานข้อมูลข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่เก็บไว้ ข้อกำหนดบางประการใน APPI ใช้กับข้อมูลส่วนบุคคลที่เก็บไว้ดังกล่าว ในขณะที่ GDPR ไม่ได้สร้างความแตกต่างนี้ ในทางตรงกันข้าม GDPR มีบทบัญญัติเกี่ยวกับเด็ก ข้อมูลที่ใช้นามแฝง การประมวลผลเพื่อวัตถุประสงค์ในการวิจัย และข้อกำหนดเกี่ยวกับวิธีขอความยินยอม ซึ่งไม่ได้ระบุไว้ใน APPI[63]

GDPR ใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ซึ่งอาจเป็นธุรกิจหน่วยงานสาธารณะ สถาบัน และไม่ใช่สำหรับองค์กรที่แสวงหาผลกำไร APPI ใช้กับผู้ควบคุมข้อมูลส่วนบุคคล (PIC) ซึ่งถูกกำหนดให้เป็น 'บุคคลที่ให้ข้อมูลส่วนตัวฐานข้อมูลสารสนเทศ ฯลฯ เพื่อใช้ในธุรกิจ' กฎหมายทั้ง 2 ฉบับให้ความคุ้มครองบุคคลที่ยังมีชีวิตอยู่โดยคำนึงถึงการใช้ข้อมูลส่วนบุคคลของตน GDPR กำหนดว่าบุคคลได้รับการคุ้มครองโดยไม่คำนึงถึงสัญชาติและ/หรือถิ่นที่อยู่ ในขณะที่ APPI ไม่ได้กล่าวถึงประเด็นนี้อย่างชัดเจน

ขอบเขตอาณาเขต ทั้ง GDPR และ APPI มีขอบเขตนอกอาณาเขต โดยเฉพาะอย่างยิ่ง GDPR ใช้กับองค์กรนอกสหภาพยุโรปหากมีการเสนอสินค้าหรือบริการเพื่อหรือติดตามพฤติกรรมของบุคคลภายในสหภาพยุโรป ข้อกำหนดบางประการของ APPI ใช้บังคับกับผู้ประกอบธุรกิจที่เกี่ยวข้องกับการจัดหาสินค้าหรือบริการแก่บุคคลในประเทศญี่ปุ่น ได้รับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลในญี่ปุ่นและจัดการในต่างประเทศ

ขอบเขตของวัสดุGDPR ใช้กับการประมวลผลข้อมูลส่วนบุคคล ในขณะที่ APPI ใช้กับการจัดการข้อมูลส่วนบุคคลสำหรับธุรกิจวัตถุประสงค์ ทั้ง GDPR และ APPI ใช้กับข้อมูลส่วน

---

[63] Comparing privacy laws: GDPR v. APPI

บุคคลและข้อมูลส่วนบุคคลตามลำดับ อย่างไรก็ตาม เฉพาะ APPI เท่านั้นรวมถึงข้อมูลที่ประมวลผลโดยไม่ระบุตัวตนภายในขอบเขตของมัน[64]

APPI ใช้กับ 'ข้อมูลส่วนบุคคล' ซึ่งกำหนดไว้เป็น 'ข้อมูลเกี่ยวกับบุคคลที่มีชีวิต' (ดูหัวข้อ 2.1.) APPI ยังกำหนดข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลประกอบเป็นฐานข้อมูลข้อมูลส่วนบุคคล APPI กำหนดข้อมูลส่วนบุคคลที่ต้องการเป็นพิเศษดูแลและจัดเตรียมข้อกำหนดเฉพาะสำหรับการจัดการ APPI ใช้กับ PIC ที่ใช้ข้อมูลส่วนบุคคลในธุรกิจ

APPI ไม่ได้กำหนดว่ากิจกรรมใดเป็นส่วนหนึ่งของ การจัดการข้อมูลส่วนบุคคล มันชี้แจงว่า APPI ใช้กับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่เก็บไว้และ 'ฐานข้อมูลข้อมูลส่วนบุคคล' ซึ่งหมายถึง 'ส่วนรวม' เนื้อหาประกอบด้วยข้อมูลส่วนบุคคล

ทั้ง GDPR และ APPI รวมคำจำกัดความของ 'ข้อมูลส่วนบุคคล' และ 'ข้อมูลส่วนบุคคล' ตามลำดับ นอกจากนี้ APPIกำหนด 'ข้อมูลส่วนบุคคล' เกี่ยวกับฐานข้อมูลข้อมูลส่วนบุคคลและ 'ข้อมูลส่วนบุคคลที่เก็บไว้

ข้อมูลส่วนตัว (ข้อมูลส่วนบุคคล)

GDPR ให้คำจำกัดความของข้อมูลที่ละเอียดอ่อน ('ข้อมูลส่วนบุคคลประเภทพิเศษ') และห้ามไม่ให้มีการประมวลผล เว้นแต่หนึ่งในนั้นข้อยกเว้นมีผลบังคับใช้ ภายใต้ APPI ข้อมูลส่วนบุคคลที่ต้องการการดูแลเป็นพิเศษอาจได้รับการจัดการตามที่ผู้ว่าจ้างมอบให้ยินยอมหรือเมื่อมีการยกเว้น APPI ใช้กับข้อมูลที่ประมวลผลโดยไม่ระบุชื่อ ในขณะที่ GDPR ไม่รวมข้อมูลที่ไม่ระบุตัวตนอย่างชัดเจนจากขอบเขตของมันของการสมัคร[65]

ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลต้องปฏิบัติตามคำขอการใช้สิทธิของเจ้าของข้อมูล เช่น สิทธิในการลบ สิทธิ์ในการแก้ไข สิทธิ์ในการเข้าถึง ฯลฯ เว้นแต่จะใช้ข้อยกเว้น ผู้ประมวลผลข้อมูลต้องปฏิบัติตามด้วยสิทธิ์ของเจ้าของข้อมูลหากผู้ควบคุมข้อมูลต้องการผู้ควบคุมข้อมูลต้องปฏิบัติตามข้อจำกัดของวัตถุประสงค์และหลักความถูกต้องและแก้ไขข้อมูลของเจ้าของข้อมูลข้อมูลส่วนบุคคลหากไม่ถูกต้องหรือไม่ครบถ้วน ผู้ควบคุมข้อมูลต้องดำเนินการทางเทคนิค และมาตรการรักษาความปลอดภัยขององค์กร

PICs ต้องตอบสนองต่อความต้องการของ การหยุดใช้งานหรือการลบข้อมูลส่วนบุคคลที่เก็บไว้ข้อมูล ฯลฯ ในกรณีที่กฎหมายกำหนดPICs ต้องมั่นใจว่าข้อมูลส่วนบุคคลนั้นถูกต้องและ

---

[64] สมชาย ธรรมสุทธิวัฒน์และคณะ. (2563). รูปแบบความ ร่วมมือและยกระดับการป้องกันการทุจริตในประเทศไทย โดยศึกษาประสบการณ์ประเทศญี่ปุ่น และเกาหลีใต้. ***วารสารวิชาการธรรมทรรศน์***, 20(1). หน้า 1-10.

[65] เรื่องเดียวกัน, หน้า 1-10.

ทันสมัยวันที่เพื่อให้บรรลุวัตถุประสงค์การใช้งานและแก้ไขใดๆเก็บรักษาข้อมูลส่วนบุคคลของตัวการที่ไม่เป็นข้อเท็จจริง PICs จะต้องดำเนินการที่จำเป็นและเหมาะสมสำหรับความปลอดภัยของข้อมูลส่วนบุคคลรวมถึงการป้องกันไม่ให้การรั่วไหล สูญหาย หรือเสียหายของข้อมูลส่วนบุคคลที่จัดการ[66]

ภาระหน้าที่อื่นๆ ที่กำหนดไว้ใน PIC รวมถึง: การลบข้อมูลส่วนบุคคลโดยไม่ชักช้าเมื่อมีการใช้งานไม่จำเป็น ใช้การดูแลที่จำเป็นและเหมาะสมเหนือบุคคลที่ได้รับมอบหมายเพื่อดูแลความปลอดภัยการควบคุมข้อมูลส่วนบุคคลที่ได้รับการจัดการมอบหมายเปิดเผยข้อมูลส่วนบุคคลที่เก็บไว้แก่เจ้าหน้าที่โดยไม่ล่าช้าตามวิธีการที่คณะรัฐมนตรีกำหนดเว้นแต่การเปิดเผยข้อมูลจะอยู่ภายใต้มาตรา 28(2)(i) ถึง (iii) จัดการข้อร้องเรียนเกี่ยวกับการจัดการอย่างเหมาะสมและเหมาะสมข้อมูลส่วนบุคคล; และมุ่งสร้างระบบที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวภายใต้มาตรา 35(1)

ไม่มีคำจำกัดความของผู้ประมวลผลข้อมูลภายใต้ APPI ซึ่งแตกต่างกับ GDPR ที่ผู้ประมวลผลข้อมูลเป็นบุคคลธรรมดาหรือนิติบุคคล สาธารณะอำนาจหน้าที่ หน่วยงานหรือหน่วยงานอื่นที่ดำเนินการข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

GDPR โปรเซสเซอร์ควรช่วยเหลือข้อมูลผู้ควบคุมจะทำการประเมินผลกระทบของการปกป้องข้อมูลก่อนดำเนินการ การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล('DPO'): โปรเซสเซอร์ต้องกำหนด DPO เมื่อจำเป็นโดยกฎหมาย รวมถึงกรณีที่ผู้ประมวลผลประมวลผลข้อมูลส่วนบุคคลในขนาดใหญ่ การแจ้งให้ผู้ควบคุมข้อมูลทราบถึงข้อมูลใด ๆการละเมิด: โปรเซสเซอร์จำเป็นต้องแจ้งให้ผู้ควบคุมทราบการละเมิดโดยไม่ชักช้าเกินควรหลังจากทราบการละเมิด[67]

ภาระหน้าที่อื่นๆ ที่กำหนดไว้ใน PIC รวมถึง: การลบข้อมูลส่วนบุคคลโดยไม่ชักช้าเมื่อมีการใช้งานไม่จำเป็น ใช้การดูแลที่จำเป็นและเหมาะสมเหนือบุคคลที่ได้รับมอบหมายเพื่อดูแลความปลอดภัยการควบคุมข้อมูลส่วนบุคคลที่ได้รับการจัดการมอบหมายเปิดเผยข้อมูลส่วนบุคคลที่เก็บไว้แก่เจ้าหน้าที่โดยไม่ล่าช้า ตามวิธีการที่คณะรัฐมนตรีกำหนดเว้นแต่การเปิดเผยข้อมูลจะอยู่ภายใต้มาตรา 28(2)(i) ถึง (iii) จัดการข้อร้องเรียนเกี่ยวกับการจัดการอย่างเหมาะสมและเหมาะสมข้อมูลส่วนบุคคล; และมุ่งสร้างระบบที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวภายใต้มาตรา 35(1)

GDPR หน่วยงานคุ้มครองข้อมูลมีอำนาจแก้ไขซึ่งได้แก่ 'ว่ากล่าวตักเตือน สั่งการผู้ควบคุมและตัวประมวลผลให้ปฏิบัติตาม สั่งผู้ควบคุมเพื่อสื่อสารการละเมิดข้อมูลไปยังเจ้าของ

---

[66] Comparing privacy laws: GDPR v. APPI

[67] ธวัชชัย งามเลิศ. (2563). ***แนวทางป้องปรามผู้ประกอบวิชาชีพสื่อมวลชนในการละเมิดสิทธิส่วนบุคคล***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา, คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม. หน้า 1.

ข้อมูลกำหนดห้ามการประมวลผลสั่งการแก้ไขหรือลบข้อมูล ระงับการถ่ายโอนข้อมูล แต่ PPC มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษา[68]

3.2.3.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศประเทศญี่ปุ่น

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่น เรียกว่า Act on the Protection of Personal Information: APPI โดยบังคับใช้กับผู้ประกอบธุรกิจทั้งหมด ที่มีการเก็บข้อมูลส่วนบุคคล มีการประกาศใช้ในปี 2546 และประกาศใช้อย่างเต็มรูปแบบทุกภาคส่วนในปี 2548 ซึ่งปี 2562 ทางสหภาพยุโรป (EU) ได้รับรองมาตรฐานการคุ้มครองข้อมูลกับประเทศญี่ปุ่น ให้สามารถถ่ายโอนข้อมูลส่วนตัวระหว่างสองเขตเศรษฐกิจได้อย่างอิสระ ช่วยให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นสูงขึ้น ถือเป็นการเพิ่มขีดความสามารถในการแข่งขันและการทำธุรกิจ[69]

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นมีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้ ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครอง เจ้าของข้อมูลมีสิทธิในการตรวจสอบ การแก้ไขข้อมูล การไม่ยินยอมให้ประมวลผล คุ้มครองข้อมูลละเอียดอ่อน (sensitive data)[70]

ญี่ปุ่นได้ตรากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Act on Protection of Personal Information - APPI) มาตั้งแต่ปี พ.ศ.2546 และมีผลบังคับใช้กับผู้ประกอบการทั้งหมดที่เสนอขายสินค้าและบริการที่มีการดำเนินการกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่น ไม่ว่าจะมีที่ตั้งอยู่ในญี่ปุ่นหรือไม่ก็ตาม และหลังจากที่ได้มีการบังคับใช้ ก็ได้มีการตรากฎระเบียบอื่น ๆ เพื่อให้สอดคล้องกับ APPI รวมถึงได้มีการเปลี่ยนแปลงแก้ไข APPI เพื่อให้ทันต่อสถานการณ์และการพัฒนาทางเทคโนโลยีที่เปลี่ยนแปลงไป จึงนับได้ว่า ญี่ปุ่นมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ก้าวหน้ามากที่สุดประเทศหนึ่ง

---

[68] Comparing privacy laws: GDPR v. APPI

[69] ธวัชชัย งามเลิศ. อ้างแล้วเชิงอรรถที่ 67. หน้า 1.

[70] เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-3-countries-in-asia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=20220608_PDPACore_JUN_1stInfographicPost&fbclid=IwAR0rzFh2Bt6a_xFBX3kOoNJOrehXKEBMSMcAGuZAIveX427riipjnt2UkCE

ล่าสุด สืบเนื่องมาจากการที่มีจำนวนอาชญากรรมทางไซเบอร์และคดีเหตุการละเมิดข้อมูลส่วนบุคคลเพิ่มมากขึ้น ญี่ปุ่นจึงได้ตรากฎหมาย APPI ฉบับแก้ไขในปี พ.ศ.2563 ซึ่งมีความเข้มงวดมากขึ้น และมีขอบเขตที่กว้างขึ้น เช่น กำหนดกฎเกณฑ์เกี่ยวกับการส่งข้อมูลที่ครอบคลุมมากขึ้น[71]

3.2.3.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การดำเนินการกรณีมีการละเมิดเกิดขึ้น ทั้งนี้ กฎหมายฉบับดังกล่าวกำหนดให้เริ่มมีผลบังคับใช้ทั้งฉบับเมื่อวันที่ 1 เมษายน พ.ศ.2565 ที่ผ่านมา

ประเด็นสำคัญที่มีการเปลี่ยนแปลงในกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขและเราควรให้ความสนใจนั้นมีมากมาย ในที่นี้จะได้กล่าวถึงเฉพาะประเด็นที่สำคัญ ดังนี้[72]

1) การแจ้งการละเมิดข้อมูลส่วนบุคคลผู้ประกอบการมีหน้าที่แจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Commission – PIPC) และ เจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการละเมิดข้อมูลใดๆ ซึ่งมีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูล ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหว การละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์

2) ข้อกำหนดเกี่ยวกับการให้ข้อมูลกับบุคคลที่สามก่อนหน้านี้ เจ้าของข้อมูลต้องได้รับการแจ้งเกี่ยวกับข้อกำหนดการให้ข้อมูลกับบุคคลที่สาม แต่สำหรับกฎหมายใหม่ผู้ประกอบการต้องยืนยันว่าบุคคลที่สามผู้รับข้อมูลได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อนที่จะให้ข้อมูลไป โดยต้องมีการระบุรายละเอียดเกี่ยวข้อมูลที่จะมีการให้ด้วย และต้องเก็บหลักฐานไว้เป็นเวลา 3 ปี

3) การส่งต่อข้อมูลไปยังต่างประเทศก่อนที่จะมีการส่งต่อข้อมูลไปยังบุคคลที่สามซึ่งไม่ได้อยู่ในญี่ปุ่นนั้น ต้องมีการแจ้งให้เจ้าของข้อมูลทราบ โดยต้องมีการแจ้งข้อมูลทั้งในส่วนของชื่อของประเทศปลายทาง ระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง และมาตรการคุ้มครองข้อมูลที่ผู้นำเข้าข้อมูลใช้

นอกจากนี้ ผู้ประกอบการที่จะส่งออกข้อมูล จะต้องดำเนินการตรวจสอบยืนยันสถานะของข้อมูลส่วนบุคคลและระบบที่ใช้ในการดำเนินการกับข้อมูลของผู้นำเข้าข้อมูล

---

[71] ฉิชนันท์ คุปตานนท์. (2565). ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/999304

[72] ธวัชชัย งามเลิศ. อ้างแล้วเชิงอรรถที่ 67. หน้า 1.

การประเมินมาตรการบรรเทาผลกระทบกรณีมีปัญหาใด ๆ เกิดขึ้น รวมไปถึงการประเมินมาตรการที่จะใช้เพื่อให้มั่นใจว่าจะมีการดำเนินการกับข้อมูลอย่างเหมาะสม

4) โทษ

ภายใต้ APPI ฉบับแก้ไขนั้น ได้มีการปรับแก้ไขเพิ่มเติมโทษให้รุนแรงมากขึ้นไม่น้อย เช่น กรณีฝ่าฝืนคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดโทษบุคคลผู้กระทำผิด จากเดิมโทษจำคุกสูงสุดไม่เกิน 6 เดือน หรือโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษจำคุกสูงสุดไม่เกิน 1 ปี

หรือโทษปรับสูงสุดไม่เกินหนึ่งล้านเยน และกำหนดโทษสำหรับนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ประมาณยี่สิบเจ็ดล้านห้าแสนบาทไทย)

หรือ ในกรณีที่มีการส่งข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ก็มีการเปลี่ยนโทษปรับในส่วนของนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินห้าล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน จะเห็นได้ว่า แนวกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของญี่ปุ่น ได้กำหนดโทษที่หนักขึ้นกรณีมีการดำเนินการกับข้อมูลที่ไม่ถูกต้องตามกฎหมาย และสร้างกฎเกณฑ์ที่เข้มงวดมากขึ้นเพื่อให้องค์กรต่าง ๆ ซึ่งมีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่นต้องปฏิบัติตาม ดังนั้นแล้ว ผู้ประกอบการไทยที่ทำการค้ากับผู้ประกอบการในญี่ปุ่น จึงควรศึกษากฎหมายฉบับนี้ไว้ให้มากด้วย[73]

หน่วยงานกำกับดูแล ทั้ง GDPR และ APPI กำหนดให้มีการจัดตั้งหน่วยงานที่มีอำนาจสอบสวนและแก้ไขเพื่อกำกับดูแลการบังคับใช้กฎหมาย และเพื่อช่วยให้องค์กรต่างๆ เข้าใจและปฏิบัติตามกฎหมาย GDPR ยังให้อำนาจดังกล่าวด้วย มีอำนาจในการกำหนดบทลงโทษทางการเงิน ในขณะที่ PPC ที่ควบคุมโดย APPI ไม่มีอำนาจในการออกตัวเงิน

บทลงโทษ นอกจากนี้ ในสหภาพยุโรป หน่วยงานคุ้มครองข้อมูลแห่งชาติยังเป็นส่วนหนึ่งของ European Data Protection Board ซึ่งเป็นหน่วยงานที่รับรองการใช้ GDPR อย่างสม่ำเสมอทั่วยุโรปหน่วยงานคุ้มครองข้อมูลมีหน้าที่ในการส่งเสริมการรับรู้และการจัดทำคำแนะนำเกี่ยวกับ GDPR

GDPR ระบุว่าหน่วยงานคุ้มครองข้อมูลต้องดำเนินการ ความเป็นอิสระอย่างสมบูรณ์เมื่อปฏิบัติงาน หน่วยงานคุ้มครองข้อมูลมีอำนาจสอบสวนซึ่งรวมถึงความสามารถในการดำเนินการตรวจสอบการปกป้องข้อมูลเข้าถึงข้อมูลส่วนบุคคลทั้งหมดที่จำเป็นสำหรับการ

---

[73] ฉิชนันท์ คุปตานนท์. (2565). ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/999304

ปฏิบัติงานของงานได้รับการเข้าถึงสถานที่ใด ๆ ของข้อมูลผู้ควบคุมและผู้ประมวลผล รวมทั้งอุปกรณ์และวิธีการหน่วยงานคุ้มครองข้อมูลมีอำนาจแก้ไขซึ่ง ได้แก่ ว่ากล่าวตักเตือน สั่งการผู้ควบคุมและตัวประมวลผลให้ปฏิบัติตาม สั่งผู้ควบคุมเพื่อสื่อสารการละเมิดข้อมูลไปยังเจ้าของข้อมูลกำหนดห้ามการประมวลผลสั่งการแก้ไขหรือลบข้อมูล ระงับการถ่ายโอนข้อมูล GDPR ไม่ได้ควบคุมวิธีการที่หน่วยงานคุ้มครองข้อมูลได้รับทุน ซึ่งปล่อยให้ประเทศสมาชิกเป็นผู้ตัดสินใจ[74]

มีหน้าที่จัดทำแนวทางและPPC ส่งเสริมการใช้ APPI APPI ระบุว่าประธานและคณะกรรมาธิการใช้อำนาจอย่างเป็นทางการของตนโดยอิสระ'กปปส. มีอำนาจสอบสวนซึ่งรวมถึงความสามารถเพื่อขอข้อมูลและดำเนินการตรวจสอบในสถานที่PPC มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษา[75]

ได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) เริ่มมีผลบังคับใช้ในปี พ.ศ. 2548 ซึ่งเป็นการเปลี่ยนแปลงครั้งสำคัญในวิธีการปกป้องข้อมูลส่วนบุคคล เดิมทีผู้ประกอบการเอกชนหรือภาครัฐ หากได้มีการกระทำการข้อมูลส่วนบุคคลของบุคคลอื่นให้เกิดความเสียหาย บุคคลผู้ได้รับความเสียหายจะขอชดใช้ค่าเสียหายตามจะต้องครบองค์ประกอบความผิดตามกฎหมายละเมิด แต่เมื่อมีการบัญญัติถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้วนั้น จึงต้องมาใช้พระราชบัญญัติดังกล่าวแทน การกำหนดว่าการถ่ายโอนข้อมูล โดยทั่วไปแล้วการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม เป็นกรณีที่เจ้าของข้อมูลไม่ได้รับ ความยินยอมล่วงหน้าจากหน่วยงานจะไม่สามารถกระทำได้เว้นแต่จะมีข้อยกเว้น ดังนี้

1) การโอนที่ได้รับอนุญาตตามกฎหมาย หากเป็นกรณีที่ได้รับอนุญาตแล้วไม่จำเป็นต้อง ได้รับความยินยอมล่วงหน้าจากเจ้าของหลักในการถ่ายโอนข้อมูลส่วนบุคคล (รวมถึงข้อมูลที่มีลักษณะละเอียดอ่อน

2) กรณีที่จำต้องได้รับความยินยอมจากเจ้าของข้อมูล ที่ถือว่าเป็นข้อกำหนดหรือได้รับอนุญาตโดยเฉพาะตามกฎหมายหรือข้อบังคับของญี่ปุ่น จะต้องเป็นกรณีที่มีความจำเป็นสำหรับ การปกป้องชีวิต สุขภาพ หรือทรัพย์สินของบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลเป็นการยากเท่าที่จำเป็น

---

[74] ปัทมา มัญชุนากร. อ้างแล้วเชิงอรรถที่ 15. หน้า 1.

[75] Onetrust Data Guidance

3) มีความจำเป็นสำหรับการพัฒนาด้านสาธารณสุขและสุขอนามัย หรือการส่งเสริม การเลี้ยงดูที่ดีและการได้รับความยินยอมจากผู้ปกครองหรือบิดา มารดานั้นทำได้ยาก เท่าที่จำเป็น ซึ่งจะเห็นได้ว่าสำหรับกฎหมายในเรื่องการแบ่งปันข้อมูลส่วนบุคคลในประเทศญี่ปุ่นนั้น ถือได้ว่ามีหลักการคือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อน แต่อย่างไรก็ตาม หากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถาการณ์นั้นที่เกิดเหตุขึ้น[76]

3.2.4 กฎหมายของประเทศแคนาดา

3.2.4.1 หลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลของของประเทศแคนาดา

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2 ฉบับ คือ Privacy Act ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลในความครอบครองของหน่วยงานของรัฐ กับ Personal Information Protection and Electronic Document Act (PIPEDA) ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลในความครอบครองของเอกชนและมีเอกสารอิเล็กทรอนิกส์ด้วย ดังนั้น จึงได้ศึกษาเฉพาะหลักกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในความครอบครองของเอกชนซึ่งอยู่ใน Part 1 ของ PIPEDA ดังนี้

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) ซึ่งเป็นกฎหมายของรัฐบาลกลางแคนาดาที่มีผลบังคับใช้ในการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลในระหว่างการทำกิจกรรมทางการค้าในทุกจังหวัดของแคนาดา โดยมีกฎหมายความเป็นส่วนตัวที่คล้ายกันช่วยเติมเต็มในอัลเบอร์ตา บริติชโคลัมเบีย และควิเบก นอกจากนี้ PIPEDA ยังบังคับใช้กับการโอนย้ายข้อมูลส่วนบุคคลระหว่างประเทศและระหว่างจังหวัดอีกด้วย เนื่องจาก AWS ไม่สามารถมองเห็นหรือรับทราบเกี่ยวกับสิ่งที่ลูกค้าอัปโหลดไปยังเครือข่ายนั้นได้ ไม่ว่าข้อมูลดังกล่าวถือว่าอยู่ภายใต้กฎหมาย PIPEDA หรือไม่ ลูกค้าจึงมีความรับผิดชอบต่อการปฏิบัติตามกฎหมาย PIPEDA ของตนเอง

PIPEDA หรือ Canadian law relating to data privacy เป็นข้อกำหนดที่เกิดขึ้นและจะต้องปฏิบัติตามกฎหมายในประเทศแคนาดา โดย PIPEDA นี้จะถูกนำมาใช้ภายใต้องค์กรต่างๆ ในประเทศ ซึ่งสามารถแบ่งออกอย่างง่ายๆ ได้ 2 ประเภท คือ

---

[76] พงษ์มนัส ดีอด และคณะ. (2566). ***รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/article/article-4/

1) องค์กรเอกชนที่มีการเก็บข้อมูลส่วนบุคคล นำข้อมูลส่วนบุคคลไปใช้ ตลอดจนการเปิดเผยข้อมูลส่วนบุคคลตามกิจกรรมเชิงพาณิชย์ ที่ซึ่งกฎหมายระบุเอาไว้ว่า เป็นการทำธุรกรรมใดๆ ที่มีลักษณะเกี่ยวข้องกับการค้าขาย แลกเปลี่ยน การเช่า รวมถึงการเป็นสมาชิกในการระดมทุน

2) องค์กรต่างๆ ที่ทำงานอยู่ภายใต้รัฐบาลกลางของประเทศแคนาดา ไม่ว่าจะเป็นสนามบิน ท่าอากาศยาน สายการบิน ธนาคาร บริษัทขนส่งระหว่างเขตหรือระหว่างประเทศ บริษัทที่เกี่ยวข้องกับการสื่อสารโทรคมนาคม ตลอดจนวิทยุและโทรทัศน์องค์กรที่ว่ามาทั้งหมดนี้ หากจะต้องดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จะต้องได้รับการยินยอมจากเจ้าของข้อมูลเสียก่อน ซึ่งข้อมูลส่วนบุคคลจะนำมาใช้ได้ตามจุดประสงค์ที่ระบุไว้ตอนขอเก็บข้อมูลเท่านั้น หากจะนำไปใช้ในจุดประสงค์อื่นๆ จะต้องขอความยินยอมใหม่ และรายละเอียดต่างๆ ของข้อมูลที่เจ้าของข้อมูลให้ไปนั้นจะต้องได้รับการป้องกันอย่างเหมาะสม ที่สำคัญเจ้าของข้อมูล หรือประชาชนในประเทศแคนาดามีสิทธิ์ที่จะตรวจสอบความปลอดภัยในการเข้าถึงข้อมูลส่วนบุคคลเหล่านั้นได้อีกด้วยอนึ่ง PIPEDA มีหลักการที่เป็นหัวใจหลักๆ ของกฎหมายอยู่ 10 ข้อ[77]

(1) องค์กรต่างๆ มีหน้าที่รับผิดชอบต่อข้อมูลส่วนบุคคลภายใต้การควบคุมขององค์กร

(2) การเก็บข้อมูลทุกครั้งจะต้องมีจุดประสงค์ที่ชัดเจน

(3) ต้องมีการยินยอมจากเจ้าของข้อมูลในการเก็บ ใช้ และเปิดเผย ข้อมูลส่วนตัว

(4) ข้อมูลที่ใช้ได้ต้องเป็นไปตามจุดประสงค์ที่ขอความยินยอมในตอนแรก ถ้าจะใช้มากกว่านั้นต้องขอใหม่

(5) ต้องเก็บข้อมูลไว้จนกว่าจะบรรลุจุดประสงค์ตามที่ขอยินยอม

(6) ข้อมูลต้องถูกรักษาอย่างปลอดภัยและอัปเดตเท่าที่เป็นไปได้

(7) ต้องได้รับการป้องกันที่เหมาะสมกับระดับความอ่อนไหวของข้อมูล

(8) ต้องมีนโยบายที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลบอกแก่สาธารณะ

(9) เมื่อมีการเรียกร้องต้องเปิดให้ดู

---

[77] พงษ์มนัส ดีอด และคณะ. (2566). ***รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/article/article-4/

(10) บุคคลสามารถตรวจสอบความปลอดภัยของข้อมูลได้ทุกเมื่อตามที่ต้องการ[78]

Personal Information Protection and Electronic Documents Act (PIPEDA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ หรือ (PIPEDA) เป็นกฎหมายของรัฐบาลกลางแคนาดาที่เกี่ยวข้องกับความเป็นส่วนตัวของข้อมูล และมีบทบัญญัติต่างๆ เพื่ออำนวยความสะดวกในการใช้เอกสารอิเล็กทรอนิกส์

PIPEDA เริ่มใช้ครั้งแรกเมื่อวันที่ 13 เมษายน พ.ศ. 2543 และมีผลบังคับใช้เป็นขั้นๆ โดยเริ่มตั้งแต่วันที่ 1 มกราคม พ.ศ. 2544 และขยายไปยังองค์กรต่างๆ ในแคนาดาตั้งแต่วันที่ 1 มกราคม พ.ศ. 2547 PIPEDA ซึ่งเป็นที่รู้จักในปัจจุบัน ควบคุมวิธีที่ธุรกิจในแคนาดาสามารถรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ในการดำเนินกิจกรรมเชิงพาณิชย์ ทั่วทั้งแคนาดา PIPEDA ยังนำไปใช้กับข้อมูลส่วนบุคคลที่ข้ามพรมแดนระดับจังหวัดหรือระดับประเทศ โดยไม่คำนึงว่าข้อมูลดังกล่าวจะอาศัยอยู่ในจังหวัดหรือเขตแดนใด

3.2.4.2 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ข้อกำหนดการแจ้งเตือนการละเมิดข้อมูล

ข้อกำหนดการแจ้งเตือนการละเมิดภายใต้ PIPEDA มีผลบังคับใช้เมื่อวันที่ 1 พฤศจิกายน 2018 ขณะนี้องค์กรจำเป็นต้องแจ้งให้บุคคล OPC และองค์กรอื่นๆ ทราบเกี่ยวกับการละเมิดข้อมูล เช่น องค์กรบังคับใช้กฎหมายหรือองค์กรที่ประมวลผลการชำระเงิน การแจ้งเตือนการละเมิดจะต้องเกิดขึ้นโดยเร็วที่สุดหลังจากที่องค์กรพิจารณาว่ามีการละเมิดเกิดขึ้นภายใต้ PIPEDA องค์กรต่างๆ จะต้องเก็บรักษาบันทึกการละเมิดข้อมูลทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (สค. 2543, ค. 5)

ส่วนที่ 1 การคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชน (ต่อ)

ส่วนที่ 1.1 การละเมิดการป้องกันความปลอดภัย

รายงานต่อ Commissioner

10.1 (1) องค์กรต้องรายงานต่อคณะกรรมาธิการถึงการละเมิดมาตรการรักษาความปลอดภัยใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุม หากมีเหตุอันสมควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงจริง ๆ ที่จะก่อให้เกิดอันตรายร้ายแรงต่อบุคคล[79]

---

[78] สุธาทิพย์ อุปสุข. (2566). ***'เท่าที่เราจะอนุญาต' ชวนสำรวจ PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยและต่างแดน.*** (ออนไลน์). เข้าถึงได้จาก: https://creativetalklive.com/global-gpda-privacy-law/

[79] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

ข้อกำหนดของรายงาน

(2) รายงานจะต้องมีข้อมูลที่กำหนดและต้องทำในรูปแบบและวิธีการที่กำหนดโดยเร็วที่สุดหลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[80]

การแจ้งเตือนไปยังบุคคล

(3) เว้นแต่กฎหมายจะห้ามไว้เป็นอย่างอื่น องค์กรต้องแจ้งให้บุคคลหนึ่งทราบถึงการละเมิดมาตรการรักษาความปลอดภัยใดๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลภายใต้การควบคุมขององค์กร หากมีเหตุอันควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงอย่างแท้จริงต่ออันตรายที่มีนัยสำคัญต่อเฉพาะบุคคล.[81]

เนื้อหาของการแจ้งเตือน

(4) การแจ้งเตือนจะต้องมีข้อมูลที่เพียงพอเพื่อให้บุคคลเข้าใจถึงความสำคัญของการละเมิดและดำเนินการ (หากเป็นไปได้) เพื่อลดความเสี่ยงของอันตรายที่อาจเกิดขึ้นจากการละเมิดหรือเพื่อบรรเทาอันตรายนั้น ให้ประกอบด้วยข้อมูลอื่นที่กำหนดด้วย[82]

รูปแบบและลักษณะ

(5) การแจ้งต้องเห็นได้ง่ายและแจ้งแก่บุคคลนั้นโดยตรงตามแบบและลักษณะที่กำหนด เว้นแต่ในกรณีที่กำหนดไว้ให้แจ้งโดยอ้อมตามแบบและลักษณะที่กำหนด[83]

PART 1 Protection of Personal Information in the Private Sector (continued)

DIVISION 1.1 Breaches of Security Safeguards Report to Commissioner

10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

[80] Report requirements

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

[81] Notification to individual

(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

[82] Contents of notification

(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.

[83] Form and manner

ระยะเวลาการแจ้งเตือน

(6) การแจ้งเตือนจะได้รับทันทีที่ทำได้หลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[84]

คำจำกัดความของอันตรายที่มีนัยสำคัญ

(7) สำหรับวัตถุประสงค์ของมาตรานี้ อันตรายที่มีสาระสำคัญรวมถึงการทำร้ายร่างกาย ความอัปยศอดสู ความเสียหายต่อชื่อเสียงหรือความสัมพันธ์ การสูญเสียการจ้างงาน โอกาสทางธุรกิจหรืออาชีพ การสูญเสียทางการเงิน การขโมยข้อมูลประจำตัว ผลกระทบในทางลบต่อประวัติเครดิต และความเสียหายต่อหรือสูญหาย ของทรัพย์สิน.[85]

ความเสี่ยงที่แท้จริงของอันตรายที่มีนัยสำคัญ - ปัจจัยต่างๆ

(8) ปัจจัยที่เกี่ยวข้องในการพิจารณาว่าการละเมิดมาตรการรักษาความปลอดภัยก่อให้เกิดความเสี่ยงอย่างแท้จริงต่ออันตรายต่อบุคคลหรือไม่ ได้แก่

(a) ความละเอียดอ่อนของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด;

(b) ความเป็นไปได้ที่ข้อมูลส่วนบุคคลจะถูกนำไปใช้ หรือจะถูกนำไปใช้ในทางที่ผิด; และ

(c) ปัจจัยที่กำหนดอื่นใด[86]

2558 ค. 32, ส. 10

---

(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.

[84] Time to give notification

(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

[85] Definition of *significant harm*

(7) For the purpose of this section, *significant harm* includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

[86] Real risk of significant harm — factors

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information involved in the breach;

(b) the probability that the personal information has been, is being or will be misused; and

(c) any other prescribed factor.

การแจ้งเตือนไปยังองค์กร

10.2 (1) องค์กรที่แจ้งบุคคลเกี่ยวกับการละเมิดการป้องกันความปลอดภัยภายใต้หัวข้อย่อย 10.1(3) จะต้องแจ้งองค์กรอื่น สถาบันของรัฐ หรือส่วนหนึ่งของสถาบันของรัฐเกี่ยวกับการละเมิด หากองค์กรที่แจ้งเตือนเชื่อว่าองค์กรอื่น หรือหน่วยงานของรัฐหรือหน่วยงานที่เกี่ยวข้องอาจสามารถลดความเสี่ยงของอันตรายที่อาจเป็นผลจากอันตรายนั้นหรือบรรเทาอันตรายนั้นลงได้ หรือหากเป็นไปตามเงื่อนไขที่กำหนดไว้[87]

ระยะเวลาแจ้งเตือน

(2) การแจ้งเตือนจะได้รับทันทีที่ทำได้หลังจากที่องค์กรตัดสินว่ามีการละเมิดเกิดขึ้น[88]

การเปิดเผยข้อมูลส่วนบุคคล

(3) นอกเหนือจากสถานการณ์ที่กำหนดไว้ในส่วนย่อย 7(3) เพื่อวัตถุประสงค์ของข้อ 4.3 ของตารางที่ 1 และแม้จะมีหมายเหตุที่มาพร้อมกับข้อนั้น องค์กรอาจเปิดเผยข้อมูลส่วนบุคคลโดยที่บุคคลนั้นไม่ทราบหรือยินยอม ถ้า

(ก) มีการเปิดเผยต่อองค์กรอื่น สถาบันของรัฐ หรือส่วนหนึ่งของสถาบันของรัฐที่ได้รับแจ้งการละเมิดภายใต้มาตราย่อย (1) และ

(b) การเปิดเผยนี้จัดทำขึ้นเพื่อจุดประสงค์ในการลดความเสี่ยงของอันตรายต่อบุคคลซึ่งอาจเป็นผลมาจากการละเมิดหรือบรรเทาอันตรายนั้นเท่านั้น[89]

---

[87] Notification to organizations

10.2 (1) An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

[88] Time to give notification

(2) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

[89] Disclosure of personal information

(3) In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if

การเปิดเผยโดยไม่ได้รับความยินยอม

(4) แม้จะมีข้อ 4.5 ของตาราง 1 องค์กรอาจเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่รวบรวมไว้ในสถานการณ์ที่กำหนดไว้ในหัวข้อย่อย (3)

(2015, ค. 32, น. 10.)[90]

บันทึก

10.3 (1) ตามข้อกำหนดที่กำหนดไว้ องค์กรจะต้องเก็บและเก็บรักษาบันทึกการละเมิดมาตรการรักษาความปลอดภัยที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุมขององค์กร

ข้อกำหนดให้ผบ.ตร

(2) องค์กรต้องจัดให้มีการเข้าถึงหรือสำเนาบันทึกแก่คณะกรรมาธิการเมื่อได้รับการร้องขอ (2558, ค. 32, น. 10)[91]

จากการศึกษาข้อมูลข้างต้น และพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พบว่าในต่างประเทศมีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล โดยสามารถสรุปข้อมูลได้ดังต่อไปนี้

1) สหภาพยุโรป

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (EU: European Union) หรือ General data Protection Regulation (GDPR) ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยการแจ้งในกรณีที่มีการละเมิดข้อมูลส่วน

(a) the disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and

(b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

[90] Disclosure without consent

(4) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3).

[91] Records

10.3 (1) An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

Provision to Commissioner

(2) An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.

บุคคลต้องแจ้งต่อหน่วยงานที่มีหน้าที่กำกับดูแลภายใต้อำนาจตามมาตรา 55 เว้นแต่การละเมิดข้อมูลส่วนบุคคลจะไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ในกรณีที่การแจ้งเตือนไปยังหน่วยงานที่มีหน้าที่กำกับดูแล ไม่ได้ดำเนินการภายใน 72 ชั่วโมงจะต้องมีให้เหตุผลสำหรับเหตุที่เกิดความล่าช้า และหน่วยงานประมวลผลข้อมูลจะต้องแจ้งให้ผู้ตรวจสอบทราบโดยไม่ชักช้าหลังจากรับเหตุการละเมิดข้อมูลส่วนบุคคล

อย่างไรก็ดี ตามหลักการที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR มีการขยายความชัดเจนในเรื่องนี้ออกไปอีกโดยผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ช่วงระยะเวลาไม่นานในการตรวจสอบข้อเท็จจริงและทำการยืนยันว่าเหตุละเมิดข้อมูลส่วนบุคคลที่พบหรือรับแจ้งนั้น ได้เกิดขึ้นจริงหรือไม่ และภายในช่วงระยะเวลาไม่นานนั้นยังถือไม่ได้ว่าบริษัทฯได้ “รับทราบ” การละเมิดข้อมูลส่วนบุคคลแล้ว

2) สาธารณรัฐสิงคโปร์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ Personal Data Protection Act: PDPA โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสิงคโปร์หรือไม่ ถือว่าอยู่ภายใต้กฎหมายดังกล่าว ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลต้องได้รับความยินยอม จากเจ้าของข้อมูลก่อนทำการเก็บบันทึก การใช้ และการเปิดเผยข้อมูลส่วนบุคคล และจะต้องใช้ข้อมูลนั้น เพื่อวัตถุประสงค์ตามที่แจ้งเท่านั้น รวมถึงจะต้องจัดให้เจ้าของข้อมูลเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลได้ และจะต้องยุติหรือหยุดการจัดเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็น ทั้งนี้ กรณีของสาธารณรัฐสิงคโปร์ในหลักของความยินยอม กฎหมายกำหนดให้การทำความยินยอมควรจะทำ เป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ และเจ้าของข้อมูลสามารถถอนหรือยกเลิกการให้ ความยินยอมในการใช้ข้อมูลเมื่อใดก็ได้ด้วยการแจ้งต่อองค์กรที่จัดเก็บข้อมูลประกอบเหตุผลในการถอน ความยินยอม

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลจะต้องมีการจัดการเพื่อรักษาความปลอดภัยอย่างเหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคล และเพื่อป้องกัน การเข้าถึง การจัดเก็บ การใช้การเปิดเผย การคัดลอก การแก้ไข การลบข้อมูลหรือความเสี่ยงอื่นในทำนอง เดียวกัน ซึ่งกระทำโดยมิชอบด้วยกฎหมาย ในส่วนของ สิทธิใน

การร้องเรียนต่อคณะกรรมการด้านข้อมูลส่วนบุคคลเป็นมาตรการเยียวยาเจ้าของข้อมูล จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย

3) ประเทศญี่ปุ่น

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น หรือ Act on the Protection of Personal Information: APPI โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูล ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงการละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์ ทั้งนี้ ต้องแจ้งโดยไม่ชักช้าตามวิธีการที่คณะรัฐมนตรีกำหนด และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PPC) มีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษาอีกด้วย

4) ประเทศแคนาดา

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) โดยอ้างอิงหลักการมาจาก GDPR แต่ว่าไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการ ถึงการละเมิดมาตรการรักษาความปลอดภัยใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้การควบคุม หากมีเหตุอันสมควรในสถานการณ์ที่เชื่อได้ว่าการละเมิดนั้นก่อให้เกิดความเสี่ยงจริง ๆ ที่จะก่อให้เกิดอันตรายร้ายแรงต่อบุคคล โดยการละเมิดจะต้องเกิดขึ้นโดยเร็วที่สุดหลังจากที่องค์กรพิจารณาว่ามีการละเมิดเกิดขึ้นภายใต้ PIPEDA องค์กรต่างๆ จะต้องเก็บรักษาบันทึกการละเมิดข้อมูลทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ตารางที่ 2 ตารางการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของกฎหมายต่างประเทศ

ประเทศ	การแจ้งเหตุละเมิด
สหภาพยุโรป	แจ้งเหตุเมื่อพบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
สาธารณรัฐสิงคโปร์	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งบังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสิงคโปร์ หรือมีถิ่นที่อยู่ในสิงคโปร์หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้
ประเทศญี่ปุ่น	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เพียงแต่กำหนดหลักเกณฑ์ไว้ว่า จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่
ประเทศแคนาดา	ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

ทั้งนี้ จากการศึกษากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของประเทศไทย และต่างประเทศ ในส่วนบทบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศนั้น มีหลักการที่สำคัญที่ยังคงยังคงประสบปัญหากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเป็นปัญหาการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงปัญหาบทลงโทษทางอาญา จึงจำเป็นต้องมีการแก้ไขเพิ่มเติมกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อไป

บทที่ 4

วิเคราะห์ปัญหากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

จากการที่ผู้วิจัยได้ดำเนินการค้นคว้าวิจัยถึงแนวทางของกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลในบทที่ 1 บทที่ 2 และ บทที่ 3 พร้อมทั้ง ศึกษากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของประเทศไทยและต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา พบว่าประเทศไทยนั้น ยังคงประสบปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ว่าจะเป็นปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สคส.) รวมถึงปัญหาบทลงโทษทางอาญา ซึ่งพบว่าในต่างประเทศมีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นแนวทางปฏิบัติ หลักเกณฑ์ หรือ บทลงโทษต่างๆ โดยมีการอ้างอิงหลักการพื้นฐานมาจากสหภาพยุโรป เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ในส่วนของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลยังไม่เหมาะสมต่อการบังคับใช้กับบริบทของประเทศไทย ผู้วิจัยจึงวิเคราะห์สภาพประเด็นปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ดังต่อไปนี้

4.1 ปัญหาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

ปัจจุบันประเทศไทยได้ให้ความสำคัญกับการคุ้มครองสิทธิความเป็นส่วนตัวในด้านข้อมูลส่วนบุคคลมากยิ่งขึ้น เพื่อไม่ให้ประชาชนตกอยู่ในสภาวะที่ไม่ปลอดภัยต่อการดำรงชีพซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นอยู่ส่วนตัวนั้น ย่อมหมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นถือได้ว่าเป็นความส่วนตัวเกี่ยวกับข้อมูล โดยสิทธิความเป็นส่วนตัวมีการรับรองไว้อย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนข้อ 12 ที่กล่าวว่าบุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการ

สื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น

เช่นเดียวกับแนวคิดของโทมัส ฮอบส์ (Thomas Hobbs) ที่กล่าวในหนังสือ Leviathan ไว้ว่า “ในสภาวะที่ยังไม่มีสังคมมนุษย์มีชีวิตอยู่ในธรรมชาติด้วยความหวาดกลัว เห็นแก่ตัวและชอบใช้ความรุนแรงเป็นสภาวะของอนาธิปไตย ด้วยความจำเป็นเพื่อหลีกหนีจากสภาวะอันเลวร้าย มนุษย์จึงรวมตัวกันขึ้นเป็นสังคม และทำความตกลงมอบสิทธิตามธรรมชาติของตนบางส่วนให้กับรัฐควบคุมดูแล เพื่อไม่ให้เกิดสภาวะที่เป็นอนาธิปไตยได้อีก เช่นเดียวกับแนวคิดของจอห์น ล็อก (John Locke) ที่กล่าวไว้ในหนังสือ The Second Treaties of Government ว่า “มนุษย์ ในสภาวะธรรมชาตินั้นเป็นสภาวะแห่งสันติสุขต่างช่วยเหลือเกื้อกูลกัน มีความเสมอภาคและเป็นอิสระมีสิทธิที่สำคัญ 3 ประการ คือ สิทธิในชีวิต อิสรภาพ และทรัพย์สิน ภายใต้การควบคุมของกฎแห่งธรรมชาติ การล่วงละเมิดสิทธิที่มนุษย์มีอยู่ตามธรรมชาติจะถูกลงโทษโดยการแก้แค้นทดแทนจากผู้เสียหายหรือญาติมิตรของผู้เสียหาย

รวมถึงแนวคิดของซามูเอล ดี วอร์เรนที่ 2 (Samuel D. Warren) และหลุยส์ แบรน (Louis D. Brandeis) นักกฎหมายชาวอเมริกันและรองผู้พิพากษาในศาลฎีกาของสหรัฐอเมริกาที่กล่าวว่าความก้าวหน้าดังกล่าวนี้ทำให้มีความจำเป็นต้องให้ความคุ้มครองแก่บุคคล เพราะพัฒนาการของเทคโนโลยีดังกล่าวทำให้เกิดการคุกคามสิทธิประโยชน์ของบุคคลอย่างน่ากลัว จึงมีแนวความคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นแนวความคิดที่มีพัฒนาการมาจากการคุ้มครองสิทธิในความเป็นส่วนตัว (Privacy Right) มีพัฒนาการมาเป็นระยะเวลายาวนานแล้วโดยในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องความเป็นส่วนตัวยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง ในเขตแดนเสมือนเป็นที่พักที่บุคคลไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาส่วนตัว เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องจากคนอื่น แนวความคิดในการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจนและได้รับการยอมรับมากที่สุดเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” หรือ “สิทธิในความเป็นส่วนตัว”

เนื่องจากปัจจุบันประชาชนมีการนำเทคโนโลยีมาประยุกต์ใช้กับชีวิตประจำวันมากกว่าเมื่อก่อน ไม่ว่าจะเป็นการเก็บ รวบรวม และการเปิดเผยข้อมูลส่วนบุคคลที่สามารถกระทำได้ง่ายผ่านช่องทางอิเล็กทรอนิกส์ จึงอาจส่งผลให้มีการละเมิดข้อมูลส่วนบุคคลขึ้น และอาจสร้างความเสียหาย เดือดร้อนให้กับเจ้าของข้อมูลส่วนบุคคลได้ และเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้นจะต้องมีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลในลำดับต่อมา ซึ่งแม้ว่าประเทศไทยนั้นจะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น และมีผลบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน 2565 แล้วก็ตาม แต่กฎหมายดังกล่าวยังไม่ได้ครอบคลุมถึงกรณีการแจ้งเหตุละเมิด

ข้อมูลส่วนบุคคลที่ชัดเจนมากพอ จึงทำให้เกิดปัญหาในการบังคับใช้กฎหมายขึ้น และทำให้การบังคับใช้กฎหมายไม่สามารถบรรลุผลในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้อย่างครบถ้วนหลายประการ และก่อให้เกิดปัญหาหรือช่องว่างทางกฎหมาย

จากการศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด” จากบทบัญญัติดังกล่าว พบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดความชัดเจน เนื่องจากไม่มีการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลส่วนบุคคล รวมถึงไม่มีการกำหนดข้อยกเว้นว่าหากเป็นการเข้าถึง เก็บ ใช้ เปิดเผย คัดลอก หรือแก้ไขข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตภายในองค์กร ไม่ให้ถือว่าเป็นการรั่วไหลที่ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงทำให้องค์กรไม่มีระยะเวลาเพียงพอต่อการประเมินสถานการณ์เหตุละเมิดข้อมูลส่วนบุคคลก่อนที่จะรายงานให้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ ทำให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลไม่ได้รับข้อมูลที่ถูกต้อง และเพียงพอ สำหรับเหตุละเมิดส่วนบุคคลดังกล่าว

อย่างไรก็ตาม หากพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พบว่าในต่างประเทศมีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้อย่างชัดเจน ซึ่งมีความยืดหยุ่น และเหมาะสมต่อการบังคับใช้กฎหมายในปัจจุบัน โดยกฎหมายของของสหภาพยุโรป หรือ General data Protection Regulation (GDPR) ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องมีการการแจ้งกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ ซึ่งหลักเกณฑ์ดังกล่าว ถือเป็นต้นแบบในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย แต่เนื่องจากบริบทของประเทศไทย และสหภาพยุโรปมีความแตกต่างกันอยู่มาก อาทิ ด้านการสื่อสาร ด้านเทคโนโลยี ด้านดิจิทัล เป็นต้น อาจจะทำให้การดำเนินการเพื่อแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ นั้น ส่งผลให้การ

ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นไปยาก โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ Personal Data Protection Act: PDPA ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสาธารณรัฐสิงคโปร์ หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้ข้อมูลแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on the Protection of Personal Information: APPI) ก็มิได้กำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เช่นเดียวกับสาธารณรัฐสิงคโปร์ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงการละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์ เป็นต้น ทั้งนี้ ต้องแจ้งโดยไม่ชักช้าตามวิธีการที่คณะรัฐมนตรีกำหนด และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นมีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษาอีกด้วย อีกทั้ง ในส่วนกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) ก็ไม่ได้กำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า เพียงแต่จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

จะเห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ อาทิ สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา ไม่ได้กำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดข้อมูล

ส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย และของสหภาพยุโรป เพียงแต่ในต่างประเทศมีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า หากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น จะต้องดำเนินการแจ้งเหตุละเมิดนั้นต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น ๆ เท่านั้น ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศมีการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และไม่ได้กำหนดระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่บีบรัดมากเกินไป จึงมีความยืดหยุ่น และเหมาะสมต่อการบังคับใช้กฎหมายในปัจจุบัน มากกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

4.2 ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่างประเทศ พบว่า สหภาพยุโรปได้นำ Directive95/46/EC ขึ้นมาบังคับใช้ในกลุ่มประเทศสมาชิกของสหภาพยุโรป โดยเป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล ต่อมาในปี พ.ศ. 2559 ซึ่งรัฐสภาแห่งยุโรปได้ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ คือ EU General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้แล้วเมื่อปี พ.ศ. 2561 โดยเป็นกฎหมายที่มีสาระสำคัญเกี่ยวกับการคุ้มครองสิทธิของประชาชนในกลุ่มประเทศสมาชิกสหภาพยุโรปเกี่ยวกับข้อมูลส่วนบุคคลและความเป็นส่วนตัวโดยมีหลักเกณฑ์เกี่ยวกับการใช้อำนาจนอกอาณาเขต คือ ให้ความคุ้มครองต่อข้อมูลส่วนบุคคลของประชาชนในกลุ่มประเทศสหภาพยุโรปไม่ว่าข้อมูลนั้นจะถูกรวบรวมหรือประมวลผลในพื้นที่ใดในโลก และมีการกำหนดบทลงโทษแก่ผู้ที่ก่อให้เกิดความเสียหายหรือทำให้ข้อมูลส่วนบุคคลรั่วไหล โดยต้องโทษปรับ 20 ล้านยูโร หรือปรับไม่เกินร้อยละ 4 ของรายได้ทั่วโลกของกิจการนั้น ขึ้นอยู่กับว่าจำนวนใดมากกว่า ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนี้ ถือเป็นแม่แบบในการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศทั่วโลก

ตามที่ผู้วิจัยได้ศึกษาหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สคส.) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการ

ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด” จากบทบัญญัติมาตรานี้ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ด 72 ชั่วโมงนับแต่ทราบเหตุละเมิดเท่าที่จะสามารถกระทำได้ ผู้วิจัยเห็นควรให้เริ่มนับระยะเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นแล้วว่าเป็นกรณีที่ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และ/หรือ เจ้าของข้อมูลส่วนบุคคลหรือไม่ หากกรณีที่การรั่วไหลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่เกิดประโยชน์ทั้งกับเจ้าของข้อมูลส่วนบุคคลและผู้ประกอบธุรกิจ นอกจากนี้ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจต้องให้ความสำคัญกับการรวบรวมข้อเท็จจริง จัดการแก้ไขปัญหาเบื้องต้น และระงับเหตุเป็นอันดับแรก การกำหนดให้ผู้ประกอบธุรกิจต้องแจ้งเหตุละเมิดดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง จะทำให้เป็นอุปสรรคต่อการดำเนินการข้างต้น

อีกทั้ง เมื่อพิจารณาร่วมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ได้ศึกษาค้นคว้าข้อมูลไว้ในบทที่ 3 นั้น พบว่าในต่างประเทศมีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ชัดเจน และไม่ได้กำหนดระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่บีบรัดมากเกินไป อาทิ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์นั้น ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งบังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสิงคโปร์ หรือมีถิ่นที่อยู่ในสิงคโปร์หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ เช่นเดียวกันกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เพียงแต่กำหนดหลักเกณฑ์ไว้ว่าจะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ก็มิได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมาธิการคุ้มครองข้อมูลส่วนบุคคลเพียงเท่านั้น เป็นต้น

ในประเด็นนี้ พบว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ ได้กำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดไว้ต่างหากจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ของประเทศไทยอย่างชัดเจน ซึ่งหากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ อันได้แก่ สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งเหตุละเมิดนั้นต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น ๆ แต่การกำหนดหลักเกณฑ์ดังกล่าวมิได้ระบุระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเหมือนดังเช่นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ของประเทศไทยจึงทำให้การดำเนินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามกฎหมายของต่างประเทศข้างต้น สามารถกระทำการได้อย่างสะดวก รวดเร็ว และเหมาะสมกับการปฏิบัติตามกฎหมายมากกว่าบริบทของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

ดังนั้น ผู้วิจัยจึงเห็นควรให้มีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา37(4) ในส่วนของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สคส.) เนื่องจากหากเป็นกรณีที่การรั่วไหลของข้อมูลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และควรให้เริ่มนับระยะเวลาที่ต้องแจ้งเหตุการละเมิดเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นเรียบร้อยแล้วเท่านั้น เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) เป็นไปตามหลักการให้การออกประกาศใช้พระราชบัญญัติฉบับนี้ คือ ป้องกันการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป และเพื่อให้มีความเหมาะสมกับสภาพการบังคับใช้ภายในประเทศไทย และเพื่อให้เกิดประสิทธิภาพของกฎหมายอย่างแท้จริง

4.3 ปัญหาบทลงโทษทางอาญา

จากการศึกษาวิจัยพบว่าบทลงโทษทางอาญาสำหรับผู้กระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ในส่วนที่ 1 โทษอาญา (มาตรา 77 - มาตรา 79) การกำหนดโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 79 กำหนดไว้ว่าหากผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืน โดยประเด็นที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ และในมาตรา 80 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับนั้น

หากพิจารณาโทษทางอาญาในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวมีลักษณะเป็นการกระทำผิดในทางแพ่งมากกว่าการก่ออาชญากรรมที่ต้องมีโทษทางอาญา ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น มีความรุนแรงเกินความจำเป็น เนื่องจากการที่ลงโทษทางอาญานั้น เป็นการลงโทษที่มีผลกระทบต่อสิทธิและเสรีภาพในชีวิต ร่างกาย และทรัพย์สินของบุคคล จึงถือเป็นที่ยอมรับโดยทั่วกันว่า โทษทางอาญาควรบังคับใช้กับการกระทำที่มีผลกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงเท่านั้น และตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการกำหนดบทลงโทษไว้สำหรับผู้ฝ่าฝืนกฎหมาย ซึ่งมีความรับผิดโทษทางอาญา เป็นกรณีการบังคับโทษสำหรับความผิดที่เกิดขึ้นจากการฝ่าฝืน หรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนด บทลงโทษทางปกครองจึงเป็นมาตรการลงโทษรูปแบบหนึ่งที่มีวัตถุประสงค์เพื่อลงโทษผู้กระทำผิด เนื่องจากฝ่าฝืน หรือไม่ปฏิบัติตามกฎเกณฑ์ของกฎหมายที่มีลักษณะคล้ายคลึงกับโทษทางอาญาด้วย การกระทำความผิดที่มีลักษณะเป็นการละเมิดหน้าที่ตามกฎหมายที่บุคคลต้องกระทำ หรือละเว้นการกระทำเพื่อประโยชน์แห่งการจัดทำบริการสาธารณะ ซึ่งลักษณะความผิดดังกล่าว ไม่มีลักษณะเป็นความชั่วร้ายหรือกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดี

ผู้วิจัยพบว่าโทษทางอาญาในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวมีลักษณะเป็นการกระทำผิดในทางแพ่งมากกว่าการก่ออาชญากรรมที่ต้องมีโทษทางอาญา ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น มีความรุนแรงเกินความจำเป็น เนื่องจากการที่ลงโทษทางอาญานั้น เป็นการลงโทษที่มีผลกระทบต่อสิทธิและเสรีภาพในชีวิต ร่างกาย และทรัพย์สินของบุคคล จึงถือเป็นที่ยอมรับโดยทั่วกันว่า โทษทางอาญาควรบังคับใช้กับการกระทำที่มีผลกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงเท่านั้น และจากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on the Protection of Personal Information: APPI) พบว่ามีการกำหนดโทษกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดโทษบุคคลผู้กระทำผิด จากเดิมโทษจำคุกสูงสุดไม่เกิน 6 เดือน หรือโทษปรับสูงสุดไม่เกินสามล้านเยน และกำหนดโทษสำหรับนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ประมาณยี่สิบเจ็ดล้านห้าแสนบาทไทย) หรือในกรณีที่มีการส่งข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ก็มีการเปลี่ยนโทษปรับในส่วนของนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินห้าล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน จะเห็นได้ว่าแนวทางการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น แม้จะมีการกำหนดโทษทางอาญาในกรณีมีการดำเนินการกับข้อมูลที่ไม่ถูกต้องตามกฎหมาย และสร้างกฎเกณฑ์ที่เข้มงวดมากขึ้นเพื่อให้องค์กรต่าง ๆ ซึ่งมีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่นต้องปฏิบัติตาม แต่ประเทศญี่ปุ่นมีการกำหนดโดยเน้นเฉพาะโทษปรับมากกว่าโทษทางอาญา ซึ่งต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยอย่างสิ้นเชิง

ทั้งนี้ ลักษณะของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวไม่ใช่การก่ออาชญากรรมที่ต้องมีโทษทางอาญา การกำหนดโทษทางอาญาไว้ในพระราชบัญญัติฯ นี้ โดยเฉพาะโทษจำคุกนั้น จึงมีความรุนแรงเกินความจำเป็น อีกทั้ง อาจถูกใช้เป็นช่องทางหรือเครื่องมือของผู้แสวงหาผลประโยชน์ได้ จึงควรยกเลิกโทษอาญา และกำหนดเป็นโทษปรับเป็นพินัยแทนบทลงโทษทางอาญา เนื่องจากปัจจุบันประเทศไทยได้มีการ

ตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ขึ้นบังคับใช้ซึ่งมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก ด้วยเหตุกรณีนี้เป็นเพียงการฝ่าฝืนไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมกว่าในการบังคับใช้กฎหมายมากกว่า ซึ่งปัจจุบันนานาประเทศได้เริ่มปรับเปลี่ยนบทลงโทษจากความผิดอาญาเป็นมาตรการอื่นที่มิใช่โทษอาญามากขึ้น รวมทั้งการใช้มาตรการอื่นแทนการลงโทษทางอาญา เช่น การคุมประพฤติกรณีจึงสมควรที่ประเทศไทย จะพัฒนากฎหมายไทยให้สอดคล้องกับนานาประเทศ และเกิดประโยชน์แก่ประชาชนยิ่งขึ้น โดยปรับเปลี่ยน โทษอาญาบางประการที่มุ่งต่อการปรับเป็นเงินตามบัญชีท้ายพระราชบัญญัติเปลี่ยนเป็นมาตรการปรับเป็นพินัย ที่สร้างขึ้นใหม่ไม่ให้มีสภาพเป็นโทษอาญา โดยกำหนดหลักเกณฑ์ให้ใช้ดุลพินิจกำหนดค่าปรับที่ต้องชำระให้เหมาะสมกับสภาพความร้ายแรงแห่งการกระทำและฐานะทางเศรษฐกิจของผู้กระทำความผิดให้สอดคล้องกัน และในกรณีที่ผู้กระทำความผิดไม่มีเงินชำระค่าปรับ อาจขอทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนการชำระค่าปรับได้ โดยไม่มีการกักขังแทนค่าปรับดังเช่นที่เป็นอยู่ในคดีอาญา การเปลี่ยนสภาพบังคับไม่ให้เป็นโทษอาญาโดยกำหนดวิธีการดำเนินการขึ้นใหม่เป็นการเฉพาะนี้ ย่อมจะช่วยทำให้ประชาชนที่ถูกกล่าวหาว่ากระทำความผิดไม่ต้องเข้าสู่กระบวนการทางอาญา และไม่มีประวัติอาชญากรรมติดตัวอีกต่อไป การเปลี่ยนแปลงเช่นนี้จะเป็นกลไกทางกฎหมายเพื่อสร้างความเป็นธรรมและขจัดความเหลื่อมล้ำทางสังคม และส่งเสริมการบังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น ดังนั้น จึงควรยกเลิกโทษอาญา และให้กำหนดเป็นโทษปรับเป็นพินัยตามพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 แทนบทลงโทษทางอาญา ย่อมมีความเหมาะสมมากกว่า ซึ่งประกอบด้วยเหตุผลดังต่อไปนี้

1) ควรกำหนดมาตรการในการลงโทษตามการจำแนกประเภทของข้อมูลอย่างเหมาะสมโดยเฉพาะอย่างยิ่งข้อมูลที่มีความละเอียดอ่อนให้รับการคุ้มครองข้อมูลส่วนบุคคลพิเศษเฉพาะเพื่อมุ่งเน้นมาตรการด้านการรักษาความมั่นคงปลอดภัยและมีประสิทธิภาพยิ่งขึ้น รวมทั้งความระมัดระวังในการประมวลผล การเก็บ รวบรวมเปิดเผย ใช้ ลบ หรือ ทำลายซึ่งเป็นข้อมูลส่วนบุคคลที่สามารถบ่งชื่ออัตลักษณ์เฉพาะของบุคคลได้นั้น ซึ่งมีความแตกต่างจากข้อมูลทั่วไป เพื่อให้มีความสอดคล้องกับเศรษฐกิจหรือวิธีปฏิบัติตามกรอบมาตรฐานของสากลยอมรับเท่าที่จะเป็นไปได้ โดยหากเป็นข้อมูลส่วนบุคคลที่มีผลกระทบต่อเศรษฐกิจและสังคมส่วนรวมควรเป็นโทษเด็ดขาด กล่าวคือ นำโทษทางอาญามาปรับใช้โดยให้มีเฉพาะโทษปรับ

2) แม้บทลงโทษทางอาญา จำคุกไม่เกิน 1 ปีและปรับ แต่อย่างไรก็ดี ประเทศไทยยังไม่มีการกำหนดฐานความผิดในกรณีที่มีการล่วงละเมิดข้อมูลส่วนบุคคลอันมีพฤติการณ์

ประกอบการกระทำในลักษณะการขัดขวางการลงทุนหรือการพัฒนาสังคมและเศรษฐกิจ เพื่อให้การลงโทษมีประสิทธิภาพ

3) แม้มีบทลงโทษในการละเมิดต่อผู้อื่นซึ่งเป็นบทลงโทษทางแพ่ง แต่ไม่สอดคล้องกับหลัก GDPR ตาม Article 83 ของ Regulation (EU) 2018/1725 ซึ่งควรมีบทลงโทษที่หนักสำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลให้สูงกว่าความรับผิดของบุคคลธรรมดาโดยนำโทษปรับมาใช้ มิใช่เพียงเฉพาะในกรณีที่มีความเสียหายเกิดขึ้นเท่านั้นแต่จำนวนความรับผิดตามโทษปรับควรมีจำนวนที่เพิ่มขึ้นตามการกระทำนั้นว่าเป็นการกระทำในระดับโทษรุนแรง หรือระดับโทษรุนแรงมาก โดยพิจารณาถึงความจงใจหรือประมาทสำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล

4) เมื่อเปรียบเทียบกับกฎหมาย GDPR พบว่า มาตรการลงโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เฉพาะโทษจำคุกอาจจะเป็นการผลักให้ผู้ประกอบการธุรกิจต้องตกอยู่ภายใต้ความเสี่ยงที่จะรับโทษอาญาซึ่งไม่สอดคล้องกับยุคดิจิทัลที่ผู้ประกอบการธุรกิจมีอยู่ทั่วโลก จึงควรเน้นให้มีการกำหนดบทลงโทษทางปกครองแก่การกระทำความผิดตามพระราชบัญญัตินี้เพิ่มขึ้นแทนโทษทางอาญา

5) การเก็บ การใช้หรือการเปิดเผยลับหรือทำลายข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน โดยมีการแจ้งวัตถุประสงค์ในการเก็บ ใช้ เปิดเผยอย่างชัดเจน และต้องทำาเท่าที่จำเป็นที่ให้ความยินยอมไว้ โดยมีการกำหนดหน้าที่ของผู้ควบคุมและประมวลผล ข้อมูลส่วนบุคคลในการจัดมาตรการรักษาความปลอดภัยและบันทึกข้อมูลส่วนบุคคลโดยการกำหนดมาตรฐานในการโอนย้ายข้อมูลไปต่างประเทศ รวมถึงการเพิ่มสิทธิของเจ้าของข้อมูลส่วนบุคคลในการโต้แย้งระงับการใช้ข้อมูลหากฝ่าฝืนจะต้องมีโทษทางอาญาซึ่งกำหนดเฉพาะโทษปรับเท่านั้น

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จากที่ได้ทำการศึกษาวิจัยปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของไทยนั้น ในตัวบทกฎหมายยังคงมีส่วนที่ยังไม่ได้ระบุให้ชัดเจน อาจทำให้เกิดช่องทางที่ทำให้ข้อมูลส่วนบุคคลถูกละเมิดได้ อีกทั้ง ประเทศไทยยังคงประสบปัญหากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเป็นปัญหาการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงปัญหาบทลงโทษทางอาญา ผู้วิจัยสามารถอธิบายสรุปประเด็นปัญหาได้ ดังต่อไปนี้

1) ปัญหาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) เนื่องจากปัจจุบันการละเมิดข้อมูลส่วนบุคคลสามารถกระทำการได้ง่าย และเมื่อมีการละเมิดข้อมูลส่วนบุคคลขึ้นย่อมส่งผลทำให้เกิดความเสียหายต่อบุคคลผู้ถูกละเมิดข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคล แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไว้ก็ตาม แต่ในส่วนนี้ยังขาดความชัดเจนอยู่มาก ทำให้ยากต่อการปฏิบัติตามได้อย่างครอบคลุม และครบถ้วน

2) ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งแม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีการกำหนดหลักเกณฑ์การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า หากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้นจะต้องดำเนินการแจ้งเหตุละเมิดนั้นต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น ๆ แต่การกำหนดหลักเกณฑ์ดังกล่าวมิได้ระบุระยะเวลาในการแจ้งเหมือนกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย จึงทำให้การดำเนินการตามกฎหมายของต่างประเทศสามารถกระทำการได้สะดวกรวดเร็ว และเหมาะสมกับการปฏิบัติตามกฎหมายมากกว่าบริบทของประเทศไทย

3) ปัญหาบทลงโทษทางอาญา เมื่อพิจารณาโทษทางอาญาในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น จึงมีความรุนแรงเกินความจำเป็น อีกทั้งอาจถูกใช้เป็นช่องทางหรือเครื่องมือของผู้แสวงหาผลประโยชน์ได้ จึงควรยกเลิกโทษอาญา เนื่องจากปัจจุบันประเทศไทยได้มีการตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ซึ่งมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก เนื่องจากกรณีนี้เป็นเพียงการฝ่าฝืน ไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมกว่าในการบังคับใช้กฎหมายมากกว่า

ดังนั้น จึงควรมีการแก้ไขกฎหมายดังกล่าว จากประเด็นปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ข้างต้น เพื่อให้กฎหมายดังกล่าวมีมาตรฐานที่สามารถปฏิบติตามได้อย่างไม่ขัดข้อง และง่ายต่อการปฏิบัติตามหลักเกณฑ์ของกฎหมายดังกล่าว ไม่ว่าจะเป็นภาคประชาชน หรือภาคธุรกิจก็ตาม

5.2 ข้อเสนอแนะ

เมื่อพิจารณาถึงประเด็นปัญหาในการการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย เปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ อาทิ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา จะได้เห็นว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศมีการบังคับใช้ได้อย่างเหมาะสมกับสภาพแวดล้อมของประเทศนั้น ๆ แตกต่างกับประเทศไทยอย่างสิ้นเชิง ซึ่งจากการที่ได้ศึกษามานั้น มีข้อเสนอแนะดังต่อไปนี้

5.2.1 เสนอให้กำหนดกรณีผู้ประกอบการไม่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4) ยังขาดความชัดเจน และไม่มีการกำหนดไว้อย่างชัดเจนว่ากรณี

ใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลส่วนบุคคล รวมถึงไม่มีการกำหนดข้อยกเว้นว่าหากเป็นการเข้าถึง เก็บ ใช้ เปิดเผย คัดลอก หรือแก้ไขข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตภายในองค์กร ไม่ให้ถือว่าเป็นการรั่วไหลที่ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจึงทำให้องค์กรไม่มีระยะเวลาเพียงพอต่อการประเมินสถานการณ์เหตุละเมิดข้อมูลส่วนบุคคลก่อนที่จะรายงานให้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ เช่น กรณีเป็นการรั่วไหลภายในองค์กร หรือผู้ควบคุมข้อมูลส่วนบุคคล สามารถควบคุมเหตุการณ์รั่วไหลได้ หรือเป็นกรณีที่มีผลกระทบกับเจ้าของข้อมูลส่วนบุคคลน้อยมาก เป็นต้น

5.2.2 เสนอให้แก้ไขจุดเริ่มต้นการนับระยะเวลา 72 ชั่วโมง ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาตรา 37 (4)

โดยควรให้เริ่มนับเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นแล้วว่าเป็นกรณีที่ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และ/หรือ เจ้าของข้อมูลส่วนบุคคล ซึ่งจะเหมาะสมกับการบังคับใช้กฎหมายมากกว่า หากกรณีที่เกิดการรั่วไหลของข้อมูลนั้น ไม่ร้ายแรง หรือ ไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่เกิดประโยชน์ทั้งกับเจ้าของข้อมูลส่วนบุคคล และผู้ประกอบธุรกิจ นอกจากนี้ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจต้องให้ความสำคัญกับการรวบรวมข้อเท็จจริง จัดการแก้ไขปัญหาเบื้องต้น และระงับเหตุเป็นอันดับแรก การกำหนดให้ผู้ประกอบธุรกิจต้องแจ้งเหตุละเมิดดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง จะทำให้เป็นอุปสรรคต่อการดำเนินการข้างต้น

ตามที่ผู้ศึกษาได้ศึกษาเปรียบเทียบไว้ในบทที่ 4 ได้กำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล พร้อมทั้ง กำหนดข้อยกเว้นว่าหากเป็นการเข้าถึง เก็บ ใช้ เปิดเผย คัดลอก หรือแก้ไขข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตภายในองค์กร ไม่ถือว่าเป็นการรั่วไหลที่ต้องแจ้งคณะกรรมการฯ เมื่อองค์กรได้ทำการประเมินสถานการณ์เหตุรั่วไหลเรียบร้อยอีกแล้วด้วย ผู้วิจัยได้ข้อสรุปว่า ประเทศไทยนั้น ควรบังคับใช้กฎหมายอย่างค่อยเป็นค่อยไป เนื่องจากที่ผ่านมายังขาดความชัดเจนในเรื่องกฎหมายลำดับรอง และแนวปฏิบัติที่ชัดเจนจากหน่วยงานผู้กำกับดูแล ทำให้ภาคเอกชนเกิดอุปสรรคในการดำเนินการ และด้วยกฎหมายนำต้นแบบมาจาก GDPR การบังคับใช้โดยอาศัยหลักการแบบ GDPR อาจไม่เหมาะสมกับบริบทของการดำเนินธุรกิจของประเทศไทย และควรติดตามการออกกฎหมายลำดับรอง และแนวปฏิบัติที่มีความชัดเจน โดยเร็ว และหน่วยงานกำกับดูแลต้องสื่อสารให้ภาคธุรกิจและประชาชนได้รับรู้ทั่วกันอย่างเป็นรูปธรรม

5.2.3 เสนอให้ใช้โทษปรับเป็นพินัย แทนบทลงโทษทางอาญา

จากการวิเคราะห์เปรียบเทียบในบทที่ 4 ผู้วิจัยเสนอให้กำหนดบทลงโทษสำหรับผู้กระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวมีลักษณะเป็นการกระทำผิดที่ไม่ใช่การก่ออาชญากรรมที่ต้องมีโทษทางอาญา ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น มีความรุนแรงเกินความจำเป็น เนื่องจากการที่ลงโทษทางอาญานั้น เป็นการลงโทษที่มีผลกระทบต่อสิทธิและเสรีภาพในชีวิต ร่างกาย และทรัพย์สินของบุคคล จึงถือเป็นที่ยอมรับโดยทั่วกันว่า โทษทางอาญาควรบังคับใช้กับการกระทำที่มีผลกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงเท่านั้น

ผู้วิจัยจึงเสนอให้ยกเลิกโทษอาญา และกำหนดเป็นโทษปรับเป็นพินัยแทนบทลงโทษทางอาญา ซึ่งปัจจุบันประเทศไทยได้มีการตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ขึ้นบังคับใช้ โดยมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก ด้วยเหตุกรณีนี้เป็นเพียงการฝ่าฝืน ไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมกว่าในการบังคับใช้กฎหมายมากกว่า ซึ่งปัจจุบันนานาประเทศได้เริ่มปรับเปลี่ยนบทลงโทษจากความผิดอาญาเป็นมาตรการอื่นที่มิใช่โทษอาญามากขึ้น รวมทั้งการใช้มาตรการอื่นแทนการลงโทษทางอาญา เช่น การคุมประพฤติกรณีจึงสมควรที่ประเทศไทย จะพัฒนากฎหมายไทยให้สอดคล้องกับนานาประเทศ และเกิดประโยชน์แก่ประชาชนยิ่งขึ้น โดยปรับเปลี่ยน โทษอาญาบางประการที่มุ่งต่อการปรับเป็นเงินตามบัญชีท้ายพระราชบัญญัติ เปลี่ยนเป็นมาตรการปรับเป็นพินัย ที่สร้างขึ้นใหม่ไม่ให้มีสภาพเป็นโทษอาญา โดยกำหนดหลักเกณฑ์ให้ใช้ดุลพินิจกำหนดค่าปรับที่ต้องชำระให้เหมาะสมกับสภาพความร้ายแรงแห่งการกระทำและฐานะทางเศรษฐกิจของผู้กระทำความผิดให้สอดคล้องกัน และในกรณีที่ผู้กระทำความผิดไม่มีเงินชำระค่าปรับ อาจขอทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนการชำระค่าปรับได้โดยไม่มีการกักขังแทนค่าปรับดังเช่นที่เป็นอยู่ในคดีอาญา การเปลี่ยนสภาพบังคับ ไม่ให้เป็นโทษอาญาโดยกำหนดวิธีการดำเนินการขึ้นใหม่เป็นการเฉพาะนี้ ย่อมจะช่วยทำให้ประชาชนที่ถูกกล่าวหาว่า

กระทำความผิดไม่ต้องเข้าสู่กระบวนการทางอาญา และไม่มีประวัติอาชญากรรมติดตัวอีกต่อไป การเปลี่ยนแปลงเช่นนี้จะเป็นกลไกทางกฎหมายเพื่อสร้างความเป็นธรรมและขจัดความเหลื่อมล้ำทางสังคม และส่งเสริมการบังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น ดังนั้น จึงควรยกเลิกโทษอาญา และให้กำหนดเป็นโทษปรับเป็นพินัยตามพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 แทนบทลงโทษทางอาญา ย่อมมีความเหมาะสมมากกว่า และเป็นไปตามมาตรา 77 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ได้บัญญัติให้รัฐพึงกำหนดโทษอาญาเฉพาะความผิดร้ายแรง โดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติว่ารัฐพึงกำหนดโทษอาญาเฉพาะความผิด ร้ายแรง กรณีจึงเป็นการสมควรกำหนดให้การกระทำความผิดในลักษณะที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติ ตามกฎหมายในกรณีที่ไม่ใช่ความผิดร้ายแรง และโดยสภาพไม่กระทบต่อความสงบเรียบร้อยหรือศีลธรรม อันดีของประชาชนอย่างร้ายแรง หรือไม่มีผลกระทบต่อส่วนรวมอย่างกว้างขวางเป็นความผิดทางพินัย โดยไม่ถือเป็นความผิดอาญา และให้กำหนดค่าปรับเป็นพินัยสำหรับผู้ฝ่าฝืนหรือไม่ปฏิบัติตาม โดยไม่ถือ เป็นโทษอาญา ประกอบกับแผนการปฏิรูปประเทศด้านกฎหมายได้กำหนดให้มีการปรับปรุงกฎหมายในการกำหนดโทษอาญาให้เหมาะสมกับสภาพความผิดหรือกำหนดมาตรการลงโทษให้เหมาะสมกับการกระทำความผิด และฐานะของผู้กระทำความผิดเพื่อมิให้บุคคลต้องรับโทษหนักเกินสมควร หรือต้องรับภาระในการรับโทษที่แตกต่างกันอันเนื่องมาจากฐานะทางเศรษฐกิจที่แตกต่างกัน เนื่องจากกรณีที่กฎหมายกำหนดโทษปรับผู้มีฐานะทางเศรษฐกิจดีย่อมสามารถชำระค่าปรับได้ แต่ผู้มีฐานะยากจนและไม่อยู่ในฐานะที่จะชำระค่าปรับได้จะถูกกักขังแทน ค่าปรับอันกระทบต่อศักดิ์ศรีความเป็นมนุษย์ อย่างรุนแรง ประกอบกับเมื่อคำนึงถึงข้อห้ามหรือ ข้อบังคับที่กฎหมายกำหนดให้ประชาชนต้องปฏิบัติหรือไม่ปฏิบัติแล้ว จะพบว่ามีข้อห้ามหรือข้อบังคับจำนวนมากอาจรุกล้ำเข้าไปในสิทธิพื้นฐานหรือสร้างภาระอันเกินสมควรแก่ประชาชน และนับวันจะมีกฎหมายตราออกมากำหนดการกระทำให้เป็นความผิดมากขึ้น หลายกรณีทำให้ประชาชนกลายเป็นผู้กระทำความผิดเพราะรู้เท่าไม่ถึงการณ์ บางกรณีกระทำไปเพราะความยากจนเหลือทนทาน และเมื่อได้กระทำความผิดแล้ว ก็ต้องถูกนำตัวเข้าสู่กระบวนการยุติธรรมทางอาญา เช่น ถูกจับกุม คุมขัง พิมพ์ลายนิ้วมือ และลงบันทึกประวัติอาชญากรเป็นประวัติติดตัวตลอดไป และในที่สุดไม่ว่าผู้นั้นจะเป็นผู้กระทำความผิดหรือไม่ กระบวนการที่กล่าวมาย่อมสร้างรอยด่างให้เกิดแก่ศักดิ์ศรีความเป็นมนุษย์อย่างหลีกเลี่ยงไม่ได้ ถ้ามีทางใดที่จะป้องกันมิให้ประชาชนจะต้องตกเข้าสู่กระบวนการนั้นได้ จะเป็นประโยชน์แก่ประชาชนและขจัดความเหลื่อมล้ำในสังคมลงได้ตามสมควร แม้ว่าการกำหนดมาตรการอันเป็นโทษที่ผู้กระทำการอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายเป็นสิ่งจำเป็นที่จะต้องมีเพื่อให้กฎหมายมีสภาพบังคับ แต่โทษนั้นก็ไม่จำเป็นต้องใช้โทษอาญาเสมอไป ซึ่งนานา

ประเทศได้เริ่มปรับเปลี่ยนบทลงโทษจากความผิดอาญาเป็นมาตรการอื่นที่มิใช่โทษอาญามากขึ้น รวมทั้งการใช้มาตรการอื่นแทนการลงโทษทางอาญา เช่น การคุมประพฤติกรณีจึงสมควรที่ประเทศไทยจะพัฒนากฎหมายไทยให้สอดคล้องกับนานาประเทศ และเกิดประโยชน์แก่ประชาชนยิ่งขึ้น

ข้อเสนอแนะที่ผู้วิจัยได้ทำการศึกษาวิจัยปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พร้อมทั้งวิเคราะห์ประเด็นปัญหากฎหมายทั้งสามประการ อันได้แก่ ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สคส.) และปัญหาบทลงโทษทางอาญา พร้อมทั้งได้สรุปผลการศึกษาวิจัยในแต่ละประเด็นปัญหา และหาแนวทางเสนอแนะเพื่อแก้ไขปัญหากฎหมายฯ ดังกล่าว ซึ่งจากการดำเนินการที่เกี่ยวข้องทั้งหมดข้างต้น สารนิพนธ์ฉบับนี้จะก่อให้เกิดประโยชน์ต่อการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาพรวม และก่อให้เกิดประสิทธิภาพในการบังคับใช้กฎหมายให้มีความครบถ้วนสมบูรณ์ ต่อการบังคับใช้ของหน่วยงาน องค์กร รวมถึงภาคประชาชนมากยิ่งขึ้น และส่งผลให้การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความยืดหยุ่นและมีความเหมาะสมกับบริบทของประเทศไทย

บรรณานุกรม

กฎหมาย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550

ประมวลกฎหมายแพ่งและพาณิชย์

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565

พระราชบัญญัติว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ พ.ศ. 2539

กฎหมายต่างประเทศ

Data Privacy Act of 2012

Personal Data Protection Act 2012

Personal Data Protection Act 2010

หนังสือ

สมาคมประกันวินาศภัยไทย. (2566). ***แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.*** กรุงเทพฯ: สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย.

วิทยานิพนธ์ สารนิพนธ์

จันทร์ทิพย์ แสงแปง. (2559). ***ปัญหาการคุ้มครองข้อมูลส่วนบุคคลศึกษากรณี การจัดเก็บข้อมูลส่วนบุคคลใน หน่วยงานเอกชน.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ธวัชชัย งามเลิศ. (2563). ***แนวทางป้องปรามผู้ประกอบวิชาชีพสื่อมวลชนในการละเมิดสิทธิส่วนบุคคล***. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา, คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม.

ปัทมา มัญชุนากร. (2564). ***ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษา กรณีผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

อธิพร สิทธิธีรรัตน์.(2558). ***ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.*** วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาการค้าระหว่างประเทศ, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

รายงานการวิจัย

ชวิน อุ่นภัทร, ปิยะบุตร บุญอร่ามเรือง. (2564). ***แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.*** รายงานการวิจัย. กรุงเทพฯ: ศูนย์วิจัยกฎหมายและการพัฒนาคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

วารสาร บทความ

คณาธิป ทองรวีวงศ์. (2564). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพ ยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารรัชต์ภาคย์,*** 15(38).

จีระศักดิ์ เสมมีสุข. (2564). การประกันภัยความรับผิดทางไซเบอร์: ศึกษาความคุ้มครองกรณีการละเมิด ข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 14(3).

ฉัตรสุมน พฤฒิภิญโญ. (2565). PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล. ***วารสารกฎหมายและนโยบายสาธารณสุข,*** 8(1).

ตวงพร ปิยวิทย์. (2564). กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศ***ไทย. วารสารวิชาการ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏนครราชสีมา***, 1(1).

ทัชชภร มหาแถลง. (2563). การคุ้มครองชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ***, 11(2).

นพดล นิ่มหนู. (2565). หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. ***วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม***, 41(3).

บรรเจิด ภาคาพันธุ์. (2563). ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในธุรกิจประกันชีวิต. ***วารสารบัณฑิตศึกษานิติศาสตร์,*** 13(1).

พงษ์เทพ สันติกุล. (2562). สิทธิมนุษยชน สิทธิพลเมือง และสิทธิทางสังคม. ***วารสารการเมือง การบริหาร และ กฎหมาย***, 11(1).

สมชาย ธรรมสุทธิวัฒน์และคณะ. (2563). รูปแบบความ ร่วมมือและยกระดับการป้องกันการทุจริตในประเทศไทย โดยศึกษาประสบการณ์ประเทศญี่ปุ่น และเกาหลีใต้. ***วารสารวิชาการธรรมทรรศน์***, 20(1).

สุขวสา ถมังรักษ์สัตว์. (2562). การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์. ***วารสารเกษมบัณฑิต,*** 20(1).

อมรรัตน์ อริยะชัยประดิษฐ์. (2565). การศึกษาเปรียบเทียบโทษทางอาญากับโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ. ศ. 2562. ***วารสารมนุษยศาสตร์ และสังคมศาสตร์ มหาวิทยาลัย มหาสารคาม,*** 41(4).

เอกณัท สุชาติพันธุ์, ประพันธ์พงษ์ ขาอ่อน. (2562). การคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจธนาคาร. ***การประชุมนำเสนอผลงานวิจัยบัณฑิตศึกษาระดับชาติ ครั้งที่ 14 ปีการศึกษาที่ 2562.***

ฐานข้อมูลออนไลน์

กรมยุโรป กระทรวงการต่างประเทศ. (2561). ***สหภาพยุโรป (The European Union - EU).*** (ออนไลน์). เข้าถึงได้จาก: https://europetouch.mfa.go.th/th/content/89715%E0%B8%AA%E0%B8%AB%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%A2%E0%B8%B8%E0%B9%82%E0%B8%A3%E0%B8%9B-the-european-nioneu?page=5d6ac39e15e39c3f300018dd&menu=5dc144e7e76fc740ee44d222

กองกฎหมาย กรมทรัพยากรทางทะเลและชายฝั่ง. ***หลักการกระทำละเมิด ประมวลกฎหมายแพ่งและพาณิชย์.*** (ออนไลน์). เข้าถึงได้จาก: https://dmcrth.dmcr.go.th/lag/detail/1110/

กรุงเทพธุรกิจ. (2564). ***การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/blogs/columnist/127256

แคทรียา มาลาศรี. (2566). ***สรุปข้อมูลสำคัญที่ Data Controller ต้องรู้ ประกาศใหม่จาก PDPC หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ 2565***. (ออนไลน์). เข้าถึงได้จาก: https://t-reg.co/blog/news/guideline-for-data-breach-report-pdpa-law/.

ฉิชนันท์ คุปตานนท์. (2565). ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแก้ไขของญี่ปุ่น.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/999304

เดต้า ว้าว. (2564). ***บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย.*** (ออนไลน์). เข้าถึงได้จาก:https://dporuler.com/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9pdpa/

เดต้า ว้าว. (2565). ***เปรียบเทียบกฎหมาย PDPA ของ 3 ประเทศในเอเชีย แต่ละประเทศมีข้อกำหนดแตกต่างกันอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpacore.com/blogs/get-to-know-the-difference-between-PDPA-of-countriesinasia?utm_source=facebook&utm_medium=social&utm_content=PDPA-comparison-fromcountries&utm_campaign=2 0 2 2 0 6 0 8 _ PDPACore_JUN_1 stInfographicPost&fbclid=IwAR0 rzFh2 Bt6 a_xFBX3 kOoNJOrehXK EBMSMcAGuZAIveX427riipjnt2UkCE

บทความสาระ. (2564). ***PDPA คืออะไร? – สรุป PDPA เกี่ยวกับธุรกิจที่คุณควรรู้! ฉบับเข้าใจง่าย ?.*** (ออนไลน์). เข้าถึงได้จาก: https://easypdpa.com/article/easypdpa-summary-what-is-pdpa

พงษ์มนัส ดีอด และคณะ. (2566). ***รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐ ภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/article/article-4/

มหาวิทยาลัยมหิดล วิทยาลัยนานาชาติ . (2565). ***ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller).*** (ออนไลน์). เข้าถึงได้จาก:https://muic.mahidol.ac.th/thai/%E0%B8%9C%E0%B8%B9%E0%B9%89%E0%B8%84%E0%B8%A7%E0%B8%9A%E0%B8%84%E0%B8%B8%E0%B8%A1%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84/

ลัฐกา เนตรทัศน์. (2566). ***สรุปภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย สิงคโปร์ และฟิลิปปินส์.*** (ออนไลน์). เข้าถึงได้จาก: https://lawforasean.krisdika.go.th/File/files/dataprotectionoverview.pdf

วารุณี เอื้อไตรรัตน์. (2564). ***พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) หากไม่ปฏิบัติตามจะมีผลอย่างไร.*** (ออนไลน์). เข้าถึงได้จาก: https://www.cyfence.com/article/what-are-the-consequences-of-not-being-compliant-with-pdpa/

วันพิชิต ชินตระกูลชัย. (2564). ***ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว คืออะไร มีกี่ประเภท มีอะไรบ้าง*** ?. (ออนไลน์). เข้าถึงได้จาก: https://openpdpa.org/personal-data-type/.

ศุภวัชร์ มาลานนท์. (2565).***การเริ่มนับระยะเวลา แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล.*** (ออนไลน์). เข้าถึงได้จาก: https://www.bangkokbiznews.com/columnist/992923

สุธาทิพย์ อุปสุข. (2566). ***'เท่าที่เราจะอนุญาต' ชวนสำรวจ PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยและต่างแดน.*** (ออนไลน์). เข้าถึงได้จาก: https://creativetalklive.com/global-gpda-privacy-law/

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ***คู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0.*** (ออนไลน์). เข้าถึงได้จาก: https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf.

Howard Poston. (2019) . ***Lessons learned: The Capital One breach***. (Online). Available: https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/

Pakin Phuhinkong. (2017). ***Git คือ Version Control แบบ Distributed ตัวหนึ่ง เป็นระบบที่ใช้จัดเก็บและควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ชนิดใดก็ได้ ไม่ว่าจะเป็น Text File หรือ Binary File***. (ออนไลน์). เข้าถึงได้จาก: https://medium.com/@pakin/git-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-git-is-your-friend-c609c5f8efea

pornpilast. (2565). ***หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Letter) คืออะไรต้องเขียนอย่างไรบ้าง ?***.(ออนไลน์). เข้าถึงได้จาก: https://pdpathailand.com/news-article/data-breach-letter/ pornpilast. (2565).

ประวัติผู้เขียน

ชื่อ - สกุล	นางสาวกนกพร เหลือสาคร
วันเดือนปีเกิด	12 เมษายน 2536
สถานที่เกิด	จังหวัดนครสวรรค์
สถานที่อยู่ปัจจุบัน	95/641 Elio Del Ray อาคาร D
	แขวงบางจาก เขตพระโขนง กรุงเทพมหานคร 10260
ประวัติการศึกษา	
พ.ศ. 2543	ประถมศึกษา โรงเรียนชุมชนบ้านน้ำวิ่ง
พ.ศ. 2549	มัธยมศึกษาตอนต้น โรงเรียนสตรีนครสวรรค์
พ.ศ. 2552	มัธยมศึกษาตอนปลาย โรงเรียนสตรีนครสวรรค์
พ.ศ. 2555	นิติศาสตรบัณฑิต มหาวิทยาลัยแม่ฟ้าหลวง
ประวัติการทำงาน	
ปัจจุบัน	เจ้าหน้าที่อาวุโส ฝ่ายวิชาการทั่วไป
	สมาคมประกันวินาศภัยไทย